Volume: 4 Issues: 15 [June, 2019] pp.121-129]
International Journal of Law, Government and Communication
eISSN: 0128-1763
Journal website: www.ijlgc.com

ADMISSIBILITY AND AUTHENTICITY OF ELECTRONIC EVIDENCE IN THE COURTS OF MALAYSIA AND UNITED KINGDOM

Ani Munirah Mohamad
School of Law, Universiti Utara Malaysia (UUM), Malaysia
(Email: animunirah@uum.edu.my)

***Accepted date**: 24-02-2019*
***Published date**: 11-07-2019*

To cite this document: Mohamad, A. M. (2019). Admissibility and Authenticity of Electronic Evidence in the Courts of Malaysia and United Kingdom. *International Journal of Law, Government and Communication*, 4(15), 121-129.
DOI: 10.35631/ijlgc.4150013

Abstract: *This concept paper elaborates on two main aspects of electronic evidence (1) the admissibility of such evidence in the courts of law, and (2) its authenticity as an evidence for the consideration of the courts. In both aspects, the scope of discussion would be the laws in Malaysia and in United Kingdom (UK). In essence, the relevant rules providing for electronic evidence in Malaysia is the Evidence Act 1950, meanwhile for the case of the UK, the Civil Evidence Act 1995 and Police and Criminal Evidence Act 1984 which provide for electronic evidence in civil and criminal matters respectively. Engaging in comparative legal research methods, and purely library-based, the relevant legal provisions for each jurisdiction are elaborated, and numerous cases are discussed in this paper to illustrate the application of such sections in admitting and authenticating electronic evidence in the Courts of Malaysia and the UK. Hopefully, this paper would become a contribution to the body of knowledge and contribute towards more in-depth research in the area of law of evidence.*

Keywords: *Electronic Evidence, Admissibility of Evidence, Authentication of Evidence, Malaysian Legal System, UK Legal System*

Introduction

Electronic evidence essentially denotes the type of evidence generated electronically, and very often, created by a computer or machine. Electronic or digital evidence is admissible in the courts of Malaysia, by virtue of sections 90A, 90B and 90C of the Evidence Act 1950. In the said sections, the term "computer" is used repeatedly and significantly.

First, before embarking on a more serious note of how electronic evidence is treated by the Malaysian courts, it is wise to define the term "computer" itself. The term "computer" is defined in Section 3 of the Evidence Act 1950 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; 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 single computer.*

In essence, the functions of a computer falling within the ambit of the Evidence Act 1950 are any one or more of the following:

- Recording information
- Storing information
- Processing information
- Retrieving information
- Producing information

Therefore, any information or document generated by such defined "computer" would be taken as "electronic evidence" by virtue of the Evidence Act 1950. Henceforth, this paper examines two main aspects of electronic evidence (1) the admissibility of such evidence in the courts of law in Malaysia, and (2) its authenticity as an evidence for the consideration of the courts.

As for the case of United Kingdom (UK), the law of evidence in the UK has recognised three types of computer-generated documentary evidence. The first type is 'real evidence', such as calculations or analyses generated by the computer itself through the running of software and the receipt of information from other devices, for example, built-in clocks and remote sensors. Real evidence is admissible as direct evidence. In this respect, Smith (1981) wrote on computer evidence, and developed the ideas put forward in *The Statue of Liberty [1968] 1 WLR 739* and crafted a rule which was later accepted by the courts.

> *Where information is recorded by mechanical means without the intervention of a human mind, the record made by the machine is admissible in evidence, provided of course, it is accepted that the machine is reliable.*

Secondly, there are documents and records produced by the computer which are copies of information supplied to the computer by human beings. This evidence is treated as hearsay (Chissick & Kelman, 1999). The third category of digital evidence is derived evidence which is information that combines real evidence with the information supplied by human beings to form a composite record. An example is the figure in the daily balance column of a bank statement, since this is derived from 'real evidence' (automatically generated bank charges) and individual cheque and paying-in entries (supplied by human beings). This is also treated as hearsay evidence (Chissick & Kelman, 1999).

Admissibility of Electronic Evidence

The primary issue with regards to electronic evidence is its admissibility in the courts of law. This part elaborates on the relevant legal provisions governing the admissibility of electronic evidence and the decided cases pertaining to the legal provisions.

The Malaysian Position

Sections 90A, 90B and 90C provides for the admissibility of electronic evidence in the Malaysian courts of law. Section 90A provides that 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 (Radhakrishna, 2012). Several cases have questioned the admissibility of computer evidence within the meaning of this section.

In this regard, the courts have admitted three different terms that would imply the meaning of computer evidence. These can be seen in cases such as *PP v Lee Kim Seng [2013] 7 MLJ 844* (computer printout), *PP v Ong Cheng Heong [1998] 6 MLJ 678* (computer output) and *Ahmad Najib b Aris v PP [2007] 2 MLJ 505* (computer evidence). In the case of *PP v Lee Kim Seng*, one of the evidences in question was the photographs taken with a digital camera. Meanwhile, in the case of *PP v Ong Cheng Heong*, the evidence was in the forms of the computer print-out on the particulars and ownership of a vehicle produced by a computer belonging to the Royal Malaysian police. Similarly, in *Ahmad Najib b Aris v. PP*, it was a chemist report produced by a computer.

In respect of the rule of hearsay, a statement which is not uttered by the person making the statement is not admissible in the court of law for being a hearsay statement in line with the best evidence rule (Sethia, 2016). However, sections 90A, 90B and 90C are regarded as exceptions to the hearsay rule because the computer-generated documents are admissible in the courts without having to call the original maker of the documents to testify as to the contents of the documents. Section 90A is an exception to the hearsay rule and provides that a document produced by a computer or a statement contained in such document shall be admissible as evidence of any fact stated therein whether or not the person tendering the same is the maker of such document or statement. This section applies to both criminal and civil proceedings (Mohamed, 2010).

Meanwhile, section 90B provides for the weight to be attached to the relevant computer evidence, whereby the court 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. This includes the manner and purpose of the document's creation or its accuracy. The court should also have regard to the following:

(a) vide Section 90B(b)(i) of the Evidence Act 1950 - 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

(b) vide Section 90B(b)(ii) of the Evidence Act 1950 - 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.

Nevertheless, section 90C provides that sections 90A and 90B shall prevail and have full force and effect notwithstanding anything inconsistent therewith, or contrary thereto, contained in any other provision of this Act, or in the Bankers' Books (Evidence) Act 1949, or in any provision of any written law relating to certification, production or extraction of documents or in any rule of law or practice relating to production, admission, or proof, of evidence in any criminal or civil proceeding.

The UK Position

In the UK, electronic evidence is accepted at both civil and criminal trials. For civil cases, the Civil Evidence Act 1995 was passed to provide for the admissibility of electronic evidence, the proof of certain documentary evidence and the admissibility and proof of official actuarial tables in civil proceedings. Computer records are admissible as evidence in the UK courts by virtue of Section 3 of the Act. Additionally, by virtue of section 8 of the Act, proof of statements

in documents may be made by the production of such document or a copy thereof before the court. On this note, such documents include plans, photographs and models pursuant to Rule 33.6 of Part 33 of Miscellaneous Rules about Evidence of the Civil Evidence Act 1995.

Meanwhile, for criminal cases, the Police and Criminal Evidence Act 1984 defined electronic evidence as 'all information contained in a computer' and therefore admissible as evidence in the courts of law. In the case of *Castlev. Cross [1985] 1 All ER 87* wherein the prosecution sought to rely on a print out from a computerised breath-testing device. The Court held that the print-out was admissible evidence. The position of law was further clarified in the leading case of *R v. Shephard (1988) 86 Cr App R 47*. In this case, records from till rolls linked to a central computer in a shop were produced to prove that items in possession of the accused had not been billed and had thus been stolen by the accused. The issue was whether a document produced by a computer can be produced as evidence. The Court held that so long as it could be shown that the computer was functioning properly and was not misused, a computer record can be admitted as evidence.

The same principle was applied in *R v. Spiby [1991) Crim. L.R. 199 (C.A.Cr.D.),* the Court of Appeal held that printouts from an automatic telephone call logging computer installed in a hotel were admissible as they constituted real evidence. The Court concluded that in the absence of evidence to the contrary, the machine had been in working order at the material time. In another case of *Camden London Borough Council v. Hobson, The Independent, January 28, 1992, 24 (Clerkenwell Magistrate's Court),* it was stated that computer-generated evidence constituted real evidence if the statement originated in the computer. It would then be admissible as the record of a mechanical operation in which human information had played no part; however, a statement originating from a human mind and subsequently processed by a computer would be inadmissible as hearsay.

In a more recent case of *Intercity Telecom Limited & Anor v. Sanjay Solanki [2015] 2 Costs LR 315, [2015] EWHC B3 (Mercantile),* the court was satisfied that the evidence in the forms of laptop, *iPad* and three universal serial bus (USB) pen drives which contained confidential information belonging to the company was admissible as evidence in the court of law. Similarly, in the case of *Atkins v The Lord Chancellor [2014] EWHC 1387 (QB),* the case involved murder trials, in which part of the evidence used in the proceeding was closed circuit television (CCTV) system and footages captured at the railway station showing what, how and when things took place at the railway station. The court admitted the CCTV system and footage for the purpose of the proceeding.

In another case involving income tax assessment, in the case of *Glenn Whittle v The Commissioner for Her Majesty's Revenue & Customs [2014] UKFTT 254 (TC),* the evidence gathered and tendered during prosecution was in the forms of computer print outs of the appellant's bank account statement, taxi fare metered records and other computerised records kept and saved by the appellant for the purpose of preparing tax returns. All these computerised documents were tendered as evidence and admitted by the court as computerised evidence.

On this note, it is provided that a video recording may be admitted as evidence in chief, specifically if the evidence was taken from vulnerable witnesses, such as pursuant to Youth Justice and Criminal Evidence Act 1999. Where a video recording is to be adduced during proceedings before the Court, it should be produced and proved by the interviewer, or any other person present in the interview with the witness during which the recording was made, as required pursuant to Para 27B.3 of the Practice Criminal Directions 2013. Audio and video

recorded interviews may also be admitted as evidence pursuant to Para 27C of the same Directions.

Based on the above discussion, it could be concluded that in both jurisdictional settings of Malaysia and the UK, electronic evidence is admitted in the courts of law by virtue of the relevant legal provisions aforementioned. Consequently, the next issue to be discussed would be the authenticity of such electronic evidence, and the legal provisions thereto.

Authenticity of Electronic Evidence

The common issue raised on computer output is with regards to its authenticity. The issue generally revolves around whether the plaintiff or defendant has complied with the requirements provided by the legal provisions.

The Malaysian Position

On the issue of authentication of electronic evidence, section 90A (2) of the Evidence Act 1950 requires the production of certificate from the person responsible for the work of the computer. Failure to produce the certificate in cases of computer-generated evidence being tendered into court will render the evidence inadmissible for failure of authenticity. For instance, in the case of *Bank Bumiputra Malaysia Berhad v Emas Bestari Sdn Bhd & Anor [2014] 1 CLJ 316*, the computer-generated document in question was an exhibit of a bank statement showing that the respondent had been paying instalments for the financing facility since its disbursement. The court ruled that the statement was inadmissible because it was not accompanied by a certificate from the bank officer who prepared the statement.

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. For instance, in the case of *Gnasegaran a/l Pararajasingam v Public Prosecutor [1997] 3 MLJ 1*, which involved criminal breach of trust by a firm of lawyers to their client, the computer-generated documents in question were bank statements of the firm maintained at the bank. The court held that despite the requirement of such accompanying certificate by section 90A (2) of the Act, the testimony by one of the witnesses, the bank officer in charge of the account, was sufficient to prove the elements of section 90A, i.e., that the statements were generated by computer in its ordinary course of business. Therefore, the court dispensed with the requirement of the certificate because the maker of the statements was present during the hearing of the case. It is noteworthy that no certificate was ever tendered in this case. However, the witness who gave evidence was able to give evidence as to whether the document was produced in the course of its ordinary use.

Nevertheless, in some situations, the requirement of a certificate may be dispensed with. For example, in the case of *Standard Chartered v Mukah Singh [1996] 3 MLJ 240*, it was held that it was only if the admissibility of the evidence was challenged, then it would be necessary to produce a certificate under section 90A (2) of the Act, that is, the documents were produced by a computer in the course of its ordinary use. There was no necessity for the certificate as the documents were unchallenged.

These cases were adopted and affirmed in a more recent case of *AmFinance Berhad v Ultimate Eight Sdn Bhd & Ors [2014] 3 CLJ 695* in which case involved hire purchase agreements and bank statements which were generated from computers. In this case, the maker of the statements was not called to testify as to the course as to the ordinary use of the computers. During appeal, the appellant argued that the statements should not be admissible for failure to

comply with section 90A (2). The appeal court ruled that it would be unjust to refuse admission of the documents because from the notes of proceedings, it was recorded that when the first time the statements were produced as evidence, lawyers for both the appellant and the respondent did not raise any objections as to its production. It was therefore held that the statements were admissible as evidence.

The UK Position

Admittedly, computer evidence can be easily and potentially modified, overwritten or deleted, thus posing challenges where sources of digital information must be authenticated and verified. The authenticity of computer-generated and computer-stored information is potentially open to security vulnerabilities in operating systems and programs that could give rise to threats to the integrity of the digital information.

The susceptibility of digital information to manipulation has been considered by court in the case of *Re VeeVinhnee, Debtor American Express Travel Related Services Company, Inc v VeeVinhnee, 336 BR 437 (9th Cir BAP, December 16, 2006)*. In that case, it was emphasised that when introducing electronic evidence, with emphasis on 'the need to show the accuracy of the computer in the retention and retrieval of the information at issue.' The admissibility of computer-generated information (such as log file records) detailing the activities on a computer, network, or other device may be open to challenge when the system generating the information does not have robust security controls (Chaikin, 2006).

At this point, it is pertinent to discuss on the issue of hearsay evidence as in traditional evidence as opposed to electronic evidence as part of the best evidence rule. In any case, the court will insist on real evidence which comes out from the original source, for instance, the person making the statement, or the machine which produces the statement, that is, as far as proving the contents of the evidence, and not as to the proving of the statement being made by the person or the machine.

Other than the original source, the court regards the evidence as hearsay, and therefore not admissible as evidence. The case is not similar for electronic evidence. So long there is no issue as to whether the computer was functioning properly or otherwise there was no misuse, electronic evidence is not subject to the hearsay rule. In other words, such electronic evidence is not regarded as hearsay evidence.

As for committal at the trial stage, there is nothing in the legislation or Rules that prevents the service of committal statements electronically. There are, however, procedural requirements concerning the form and content of statements to ensure admissibility when magistrates are inquiring into an offence as examining justices. The primary requirement for admissibility of a written statement for the purposes of committal to the Crown Court is that it purports to be made by the person who made it as provided by section 5B(2)(a) Magistrates' Courts Act 1980. This requirement can be complied with by a digital signature on a document or by a printed copy of the maker's signature.

When a charge is read during committal, and the accused makes a formal admission, a digital form of such admission is acceptable. On this note, Section 10(1) Criminal Justice Act 1967 provides that:

> *…any fact of which oral evidence may be given in any criminal proceedings may be admitted for the purpose of those proceedings…and the admission*

shall as against that party be conclusive evidence in those proceedings of the fact admitted.

The requirements of section 10 include that a formal admission must be in in writing; and purports to be signed by the person making it (unless made on behalf of the defendant by solicitor or counsel). Therefore, it is evident that digital versions of formal admissions are therefore fully compliant with section 10 provided they meet the admissibility criteria. Accordingly, Sections 5A(3) and 5E(1) Magistrates' Courts Act 1980 together permit the admission of documents at committal. It has also been established that documents also include digital or electronic documents.

As for the service of such formal admissions, by virtue of section 134 Criminal Justice Act 2003 a document is 'anything in which information of any description is recorded'. Digital versions of statements are therefore documents admissible to the same extent as paper-based statements, provided the requirements of form and signature are complied with.

Of equal importance is section 9 of the Criminal Justice Act 1967 which emphasises that there must be proof by written statement in criminal proceedings other than committal proceedings. Similar considerations apply to the admissibility of digital versions of formal admissions under section 10 Criminal Justice Act 1967. Where a statement to be tendered in evidence is a scanned copy of a paper statement, the paper version should be necessary only to resolve any issues concerning the authenticity of the paper statement or the copying process. Where the statement has only ever existed in digital format the 'statement' will, in effect, be the digital version of the statement already served to the court.

In order to cater to the specific issue of authenticity of electronic evidence in the courts of the UK, the British Standards Institute has published in 2008 a specific standard called *BS 10008: Evidential weight and legal admissibility of electronic information – Specification*, which was later revised in 2014. The standard sets out the requirements for the implementation and operation of electronic information management systems, including the storage and transfer of information, and addresses issues relating to authenticity and integrity of information.

BS 10008 ensures that any electronic information required as evidence of a business transaction is afforded the maximum evidential weight. The process is based on the specification of the requirements for planning, implementing, operating, monitoring and improving the organisation's information management systems. Specific areas covered by the standard are the management of electronic information over long period, including one that has gone through technology changes in which information integrity is a vital business requirement, management of the various risks associated with electronic information, information on how to demonstrate the authenticity of electronic information, management of quality issues related to document scanning processes, as well as the provision of a full life history of an electronic object throughout its life.

The adherence to the Standard is voluntary and would only become binding when incorporated in contract or legislation. To ensure admissibility such electronic evidence, information must be managed by a secure system throughout its lifetime. Where doubt or threats can be placed on the information, the evidential weight may be diminished, potentially harming the legal case, particularly where criminal evidence is concerned (Tolson, 2012).

Conclusion

This paper provides an overview of the issue of admissibility and authenticity of electronic evidence in the Courts of Malaysia and the UK. With the changing legal environment in the era of Industrial Revolution 4.0, various types of computer-generated evidence are increasingly being introduced and tendered as evidence in the courts of law. The Malaysian Evidence Act 1950 particularly section 90A, 90B and 90C provide for the admissibility and authenticity of such evidence in Malaysia, whereas for the UK context, the relevant legal provisions would be the Civil Evidence Act 1995 and Police and Criminal Evidence Act 1984. This paper examined each legal provision by highlighting the application of the respective provisions via decided case laws. Hopefully, this paper would become a contribution to the body of knowledge and contribute towards more in-depth research in the area of law of evidence.

References

Chaikin, D., (2006). Network investigations of cyber-attacks: the limits of digital evidence. *Crime Law Soc Change*, 46: 239

Chissick, M., & Kelman, A. (1999). *Electronic commerce law and practice*: Sweet & Maxwell, Ltd.

Mohamed, D. (2011). Computer evidence: Issues and challenges in the present and in the future. *LNS* (A) lxvii.

Radhakrishna, G. (2012). Digital evidence in Malaysia. Digital Evidence & Elec. *Signature L. Rev*., 9, 31.

Sethia, A. (2016). Rethinking admissibility of electronic evidence. *International Journal of Law and Information Technology*, 24(3), 229-250.

Smith, J. C. (1981) 'The admissibility of Statements by Computer' *Crim LR* 390, at p. 396.

Tolson, S. (2012) Legal issues with electronic evidence, online, available at http://www.building.co.uk/legal-issues-with-electronic-documents/5031357.article accessed on 20 February 2016.

Law Cases

Ahmad Najib b Aris v PP [2007] 2 MLJ 505.

AmFinance Berhad v Ultimate Eight Sdn Bhd & Ors [2014] 3 CLJ 695.

Atkins v The Lord Chancellor [2014] EWHC 1387 (QB).

Bank Bumiputra Malaysia Berhad v Emas Bestari Sdn Bhd & Anor [2014] 1 CLJ 316.

Camden London Borough Council v. Hobson, The Independent, January 28, 1992, 24 (Clerkenwell Magistrate's Court).

Castlev. Cross [1985] 1 All ER 87.

Crime, Law and Social Change, 46(4-5):239256, 249.

Glenn Whittle v The Commissioner for Her Majesty's Revenue & Customs [2014] UKFTT 254 (TC).

Gnasegaran a/l Pararajasingam v PP [1997] 3 MLJ 1.

Intercity Telecom Limited & Anor v. Sanjay Solanki [2015] 2 Costs LR 315, [2015] EWHC B3 (Mercantile).

PP v Lee Kim Seng [2013] 7 MLJ 844.

PP v Ong Cheng Heong [1998] 6 MLJ 678.

R v. Shephard (1988) 86 Cr App R 47.

R v. Spiby [1991) Crim. L.R. 199 (C.A.Cr.D.).

Re VeeVinhnee, Debtor American Express Travel Related Services Company, Inc v VeeVinhnee, 336 BR 437 (9th Cir BAP, December 16, 2006).

RHB Bank Berhad v Lee Kai Shin & Anor (High Court of Sabah & Sarawak at Kuching, July 2008).
Standard Chartered v Mukah Singh [1996] 3 MLJ 240.
The Statue of Liberty [1968] 1 WLR 739.