ISBN 978-967-11350-4-4

CHALLENGES IN ADMITTING AND AUTHENTICATING EMAILS

Gita Radhakrishna
Faculty of Law, Multimedia University
Email: gita@mmu.edu.mu

ABSTRACT

In the electronic communication era, emails are increasingly becoming the normal mode of communication in both the business as well as the personal sphere. Evidence therefore progressively takes on an electronic format. The main problem with electronic evidence is not its possession but its admissibility and authentication. The ease, with which electronic evidence can be created, altered, and manipulated gives rise to allegations of tampering or damage between the time they were created and adduced in court, the reliability of the computer program, the identity of the author or even the compliance with certain processes. The main challenge to admissibility is the rule against hearsay. Although the rule against hearsay has undergone a great deal of relaxation over time with the introduction of various exceptions such as the 'business records' exception, it is not an automatic right to admissibility. Further admissibility is not synonymous with authenticity. Authentication refers to whether the data is what it purports to be. This requires establishing its reliability and integrity by proving its authenticity, completeness and accuracy. This paper undertakes a comparative study of the legal challenges to the admissibility and authentication of emails in Malaysia, the United States of America, England and Singapore by reviewing the statutory provisions and cases in the respective jurisdictions. The objective is to establish certain guidelines to overcoming the evidentiary challenges in dealing with emails which could be equally useful for other types of electronic evidence.

Keywords: email, admissibility, authenticity

ISBN 978-967-11350-4-4

1. INTRODUCTION

Information technology has today permeated all spheres of both personal and public life, changing the way we communicate. Businesses are increasingly, creating, storing and communicating electronically. Studies show that 70% of paper business records are wholly computer generated, and that 95% of business documents are produced on word-processors. Approximately 30% of the data stored on computers is not printed meaning that 30% of potentially relevant evidence remains in information systems (Marcella, 2002). Such electronic data especially electronic mail (email), is now being increasingly used in litigation. Email is the telecommunication of messages from one computer to another (Benjamin, 19950. Although emails may be admitted into evidence there is a great deal of misunderstanding about their admissibility (Mason, 2010). The fear of easy alteration and manipulated without detection poses challenges to their admissibility. This paper undertakes a comparative study of the legal challenges to the admissibility and authentication of emails in Malaysia, the United States of America (USA), England and Wales (EW), and Singapore by reviewing the statutory provisions and cases in the respective jurisdictions. The objective is to establish certain guidelines to overcoming the evidentiary challenges in dealing with emails.

2. CHARACTERISTICS OF EMAIL

Emails are generally treated as a casual and convenient form of communication often containing careless unguarded comments. This is where the proverbial 'smoking gun' evidence may lie. Unlike paper records, emails are hard to delete as even 'deleted' emails are discoverable by computer forensic experts. 'Deleting' merely means that the computer entry in the disk directory is changed to a 'not used' status permitting the computer to 'write over' the 'deleted' data. Until the 'deleted' data, is 'written over' it may be recovered (Friedrich W. Seitz). Further, as emails are generally stored in various locations and distributed to numerous people, the task of finding and deleting all copies and traces of a document can be almost impossible. The other evidentiary worry is that emails are susceptible to after-the-fact alteration. Most email systems allow forwarding mail to be modified which would be indiscernible to the recipient (Michele C.S. Lange, 2004) However this would pose challenges to the integrity and reliability of the emails.

3. CHALLENGES TO THE ADMISSIBILITY OF EMAIL EVIDENCE

According to Cross and Tapper, 'all evidence that is sufficiently relevant to an issue before the court is admissible and all that is irrelevant or insufficiently relevant should be excluded' (Collin Tapper,2004). However relevancy is not necessarily synonymous with admissibility. Relevant evidence could be excluded on grounds that its prejudicial value outweighs it probative value (Collin Tapper, 2004). Judge Grimm, in *Lorraine v Markel* (2010) indicated that relevance is the first thing to be established for any potential piece of evidence, including an electronic document. This is largely established through content and origin of the document (*Lorraine*). Once relevance has been established the next step is to establish the authenticity of the document in question (*Lorraine*). Email chains and attachments to emails also create the problem of 'hearsay within hearsay'. Authentication and hearsay issues are closely connected. Each and every email and attachment would need to be individually authenticated to satisfy the rule against hearsay or qualify as one of the recognised statutory exceptions if it is to be admitted into evidence and offered for its truth (Gregory P. Joseph). The statutory provisions in the USA, EW, Singapore and Malaysia will now be studied to identify useful guidelines for overcoming the evidentiary challenges in dealing with emails which could be equally useful for other types of electronic evidence.

4. UNITED STATES OF AMERICA

In the USA the Federal Rules of Evidence (FRE) govern all evidentiary matters. FRE 101(b)(6) provides that a reference to any kind of written material or any other medium includes electronically stored information (ESI) (*Doali-Miller v. SuperValu, Inc.*,2012). ESI includes emails, text messages, chats, information from websites etc. Nevertheless basic evidentiary rules established under the FRE would have to be satisfied before electronic evidence can be admitted (Michael R. Arkfeld). These issues were discussed at great length by Judge Paul Grim in *Jack R. Lorraine and Beverly Mack, Plaintiffs v. Markel American Insurance Company (Lorraine),* and identified as relevance, authenticity, hearsay, original writing and unfair prejudice. This paper focuses on authenticity and hearsay which often overlap.

ISBN 978-967-11350-4-4

In *Lorraine*, the plaintiff sought to recover the damage to his boat that had been struck by lightning under his insurance policy. The defendants paid out the initial claim. However later there was a second claim when further damage was discovered to the hull of the boat. Parties sought to rely on various emails. Judge Paul W Grimm scrutinised and analysed the "evidentiary hurdles" before electronically store information (ESI) could be admitted into evidence. The relevant provisions of the Federal Rules of Evidence (FRE) for consideration were Rules 104, 401, 403, 901and 902, 801 and 1001-1008. The first rule for admissibility is that evidence should be relevant(Rule 401). Then he went on to consider the foundation for authenticity(104) and the available methods for authentication ranging from oral testimony of a witness, comparison of previous specimens, circumstantial evidence, public records, as well evidence from an accurate process or system (Rule 901). The FRE also provides for self authentication through official publication, inscriptions, and regularly conducted business (Rule 902). Once evidence is relevant and authentic it must also overcome any hearsay objections (Rule 801).

4.1 AUTHENTICITY

This is a complex issue and is dealt with by FRE Rules 901(a) and (b), as well as FRE Rule 902 which provide instructive guidance. FRE Rule 901(a) contains the substantive requirement for authentication while Rule 901(b) provides for extrinsic methods of authenticating. Rule 902 on the other hand provides for self-authenticating features in ESI. As a rule, evidence must be authenticated or identified before it may be admitted i.e. authenticity is a precondition to admissibility. Generally, to authenticate or identify an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is. FRE Rule 901 (b) provides ten non-exclusive ways by which extrinsic evidence may authenticate ESI. These include the testimony of a witness with knowledge, expert and non- expert opinion, distinctive characteristics, witness identification, circumstantial evidence, evidence that a document is a public record or ancient documents more than 20 years old, evidence showing that a process or system was used to produce a result and that the process or system produces an accurate result (Rule 901).
FRE Rule 901(b) (4) provides for authentication by way of circumstantial evidence by 'the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances'. This is frequently used to authenticate email and other ESI records such as dates, nicknames, screen names, email addresses and web addresses. Conversational references to the content have been found to be sufficient authentication under this rule. Emails contain certain self- authenticating features in their 'header' and 'body'. The header lists the user name and address of the sender and the recipient, the date and time of the transmission and the subject matter of the mail. The body of the emails contains the text of the mail (Gregory P. Joseph, 2012). Authenticity of the email may be established by these identifying markers that appear in the email itself as well as by a witness as his personal communication as in *Ussery v. State.* Further, an absence of a challenge by an opposing party disputing the authenticity of the emails may be deemed sufficient evidence of the emails' authenticity (Gregory P. Joseph, 2012). In *Lemme v County of Yuma*, the Court overruled objections as to the authenticity of documents which the Plaintiff and her counsel had not specifically challenged. However where an unsolicited email is received ostensibly from a sender whom the recipient has no previous history of contact with, more than mere oral testimony from the recipient may be required to link the email to the alleged sender (*Jimena v. UBS AG Bank, Inc.*, 2011). *United States v. Safavian (2006)*, set out guidelines on the circumstantial evidence required under the US Federal Rules of Evidence 901(b)(4) to establish the authenticity of an email identifying the sender or receiver, being confirmation that:

(i) a witness or entity received the email;
(ii) the email bore the customary information in the header of the email;
(iii) the address of the recipient was consistent with the email address on other emails sent by the same sender.
(iv) the email contained the electronic signature of the sender.
(v) the email stated matters known only to the alleged sender;
(vi) the email was in fact sent as a reply to the sender;
(vii) following receipt of the email, the recipient communicated with the alleged sender and the conversation reflected the sender's knowledge of the contents of the email.

However in contrast in *Jimena v. UBS AG Bank, Inc*.(2011), a case alleging fraud against Chief Financial Officer at UBS AG Bank, the court found that there was inadequate foundational evidence in the emails linking the Chief Financial Officer as the author of the emails. The emails that were allegedly sent to plaintiff were unsolicited, contained only publicly available, self-serving information, with no substantive or unique information that supported authenticity.

ISBN 978-967-11350-4-4

In *Suni Munshani v. Signal Lake Venture Fund II, LP, et al*.(2004). Mr. Munshani sued the Signal Lake, a venture-capital based company for $25 million because its CEO, had allegedly promised him warrants with which to purchase stocks at very favourable pricing. The authenticity of an e-mail that had allegedly been sent from Signal Lake's CEO to Mr. Munshani was in issue. The court-appointed computer forensics expert found that the email had been forged. The e-mail header data sent from an earlier e-mail had been used to send the alleged offer. The investigation revealed inconsistencies with the e-mail's message ID and the alleged time stamp as well as in the received, sent, create, and last modified dates embedded within the e-mail message as saved on the plaintiff's personal computer. The key to the forgery was the discovery of an ESMTP ID number, that was the same in both the original e-mail and the forged e-mail sent by Mr. Munshani. The finding resulted in Mr. Munshani being indicted for criminal attempt of fraud and obstruction of justice.

Problems may also arise where the authorship and receipt of the email is disputed as in *Clement v California Department of Corrections* (2008). In such circumstances, it would be necessary to call technical expertise to trace the transmission by identifying the Internet Protocol address (IP address) in the header of the email. The IP address would enable the email recipient to identify the sender with the assistance of the service provider. It is important for counsel to establish a proper foundation to authenticate the evidence as it will otherwise be rejected as in(Gita Radhakrishna, 2013).

4.2 HEARSAY

FRE Rule 801 provides definitions for certain key terms when dealing with hearsay. Rule 801(c) defines 'hearsay as a statement that:
(1) the declarant does not make while testifying at the current trial or hearing; and
(2) a party offers in evidence to prove the truth of the matter asserted in the statement.

'Hearsay' is therefore an out of court statement, by someone other than the declarant while testifying at the trial or hearing, offered to prove the truth of the matter asserted. The 'statement' could be either an oral or written assertion or even a nonverbal conduct intended as an assertion. (Jonathan D. Frieden) The Court in *Lorraine* advocated a five step analysis to deal with hearsay issues, (Paul W**.** Grimm et al, 2009).
There are five separate questions that must be answered:
(1) does the evidence constitute a statement, as defined by Rule 801(a);
(2) was the statement made by a "declarant," as defined by Rule 801(b);
(3) is the statement being offered to prove the truth of its contents, as provided by Rule 801(c); (4) is the statement excluded from the definition of hearsay by rule 801(d); and
(5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807.

With respect to emails, the 'business records' exception under FRE rule 803 (6), is an important, frequently used exception. It requires five conditions to be met to qualify as records of a regularly conducted activity. The records should have been regularly compiled at the material time by someone with knowledge as part of a course of a regularly conducted activity of the establishment, whether for profit or otherwise. This can be testified to by either the record custodian or another qualified witness, or by a certification that complies with FRE Rule 902(11) or (12) or any other statute permitting certification. Importantly, the source of information or the method or circumstances of preparation should also be shown to be trustworthy. In *State of New York v. Microsoft Corp*.(2002), the Court paid stringent attention to the business policies and practices of the organisation. Emails were rejected because there was a complete lack of information regarding the practice of composition and maintenance of the emails. The Court clarified that for an employee's e-mail to qualify as a business record it had to be proved that it was the regular practice of the employer to require the employee to make and maintain the e-mail for business purposes. Further for e-mail chains, it was again necessary to establish that each participant in the email chain was acting in the regular course of the business in contributing to the e-mail chain. Similarly in *Canatxx Gas Storage Ltd. v. Silverhawk Capital Partners (2008)*, the Court emphasised that neither a paper document, nor ESI could automatically qualify within the business-records exception by virtue of it being a business matter. It had to be established that the records were regularly made in furtherance of the employer's needs and the employer imposed a business duty to make and maintain such a record as opposed to the personal practices of the employee who made them. FRE Rule 805 permits hearsay within hearsay or multiple hearsay subject to conditions. The statements could be admitted if each part of the combined statements

ISBN 978-967-11350-4-4

conforms with an exception to the rule. In *State of New York v. Microsoft Corp*.(2002), it was held that both the source and the recorder of the information, as well as every other participant in the chain producing the record, should be acting in the regular course of business, to qualify under the Rule 803(6) exception. Where any single participant in the chain falls outside the rule then it must qualify under any other exception to be admitted. In *Trade Finance Partners, LLC v. AAR Corp*.(2008), it was specifically held that the 'catch all' provision of FRE Rule 807 would not apply.

It may be summarised that the FRE provides detailed guidelines on issues pertaining to admissibility, authenticity and hearsay statements. Emails would generally be admitted under the exception to business records if it can be shown that the record keeping was part of the administrative policy of the organisation. Hearsay and authenticity issues are in practice treated together as there is an overlap in the proof of record keeping practices and authenticating emails.

5. ENGLAND & WALES

The relevant statutes here are the Civil Evidence Act 1995 (CEA 1995) and the Criminal Justice Act 2003 (CJA 2003). The section 1 CEA 1995 provides that, in civil proceedings, evidence shall not be excluded on the ground that it is hearsay. The thrust has now been shifted from admissibility to weight.

5.1 AUTHENTICITY

Electronically produced documents are admissible under sections 8 and 9 CEA 1995. Section 13 CEA 1995 defines 'documents' in the widest possible sense and includes 'copies'.[1] Section 8 facilitates the authentication of documents, by producing the original or a copy, irrespective of whether the document is a paper or an electronic document. It has to satisfy the court that it has an efficient and reliable 'Electronic Records Management System'(EDRM) following the guidelines set in The British Standards Institute's BS 10008:2008 (Evidential weight and legal admissibility of electronic information Specification). This provides five criteria:

(i) Representation of Information (i.e. an information management policy) - Recognition and understanding all types of information within the organization;
(ii). A Duty of Care -Understanding all legal issues and execution of appropriate „duty of care" responsibilities;
(iii). Business Procedures and Processes;
(iv). Enabling Technologies including document management, content management and records management systems and
(v). Audit Trails

Section 9 CEA 1993 facilitates the admissibility and authentication of business records through the certification signed either by an officer of the business or authority to which the records belong. Electronic copies of documents may be admitted so long as their integrity can be shown. In *Villalba v Merrill Lynch & Co. Inc*.(2004), an employment case, emails were admitted to show unlawful discrimination and unfair dismissal.

In criminal proceedings section 133 CJA 2003 provides that where a statement in a document is admissible as evidence in criminal proceedings the statement may be proved either by the document or (whether or not the document exists) a copy of the document or the material part of it, authenticated in whatever way the court may approve. In *R v Mawji* (2003), the appellant was convicted of threatening to kill his estranged wife. Among the evidence produced was an email dated 31 July 2002 that he allegedly sent the victim. Evidence was tendered on how an email could be sent appearing to come from a third party's account. One of the grounds of appeal was that the print out of the email was secondary evidence and it was necessary to provide an audit trail of the email to show the authenticity of the document. This was rejected by the Court of Appeal as the content of the email demonstrated its authenticity on the face of the totality of the evidence and linked to the other evidence produced at the trial which showed that it was written and sent by the appellant.

5.2 HEARSAY

In civil cases section 1 CEA 1995 effectively states evidence shall not be excluded by reason of it being hearsay. As a safeguard, section 2(1) requires a party proposing to adduce hearsay evidence to give notice to all other parties identifying the hearsay statement, proposal to rely on such statement at trial and reason why the witness cannot be

 ISBN 978-967-11350-4-4

called. Where any other party wishes to challenge such statement section 3 CEA 1995 allows that other party with leave of court, to call the maker of the statement for cross examination. Section 4 CEA provides guidelines to the court on the weight to be given to such hearsay evidence in that regard shall be had to:
(i) whether it would have been practicable to call the witness;
(ii) whether the original statement was made contemporaneously with the occurance of the matters stated;
(iii) whether multiple hearsay is involved;
(iv) whther there was any motive to conceal r misinterpret matters;
(v) whether the original statement was edited for any particular purpose;
(vi) whether the hearsay statement was adduced to prevent proper evaluation of its weight.

However where business records of a business or public authority are concerned section 9 CEA 1995 provides that such records shall be received in civil proceedings without further proof subject to the requirement of a certificate to that effect from an officer of that business or public authority and notice to all other parties.

In criminal proceedings, section 117 CJA 2003 provides for the admissibility of hearsay statements contained in business and other documents subject to five conditions namely:
(i) oral evidence would be admissible as evidence of the matter stated;
(ii) the document was created or received by a person in the course of a trade, business, profession or other occupation ot as holder of a paid or unpaid office;
(iii) the person who supplied the information may be the same person creator or the receiver of the document or may be reasonably be supposed to have knowledge of the matters dealt with;
(iv) where information is supplied indirectly, then each person through whom it was supplied, received it in the course of a business, profession or other occupation ot as holder of a paid or unpaid office and
(v) where the statement is prepared for the purpose of a criminal proceeding or investigation, the supplier of the information does not give oral evidence for one of the reasons set out in section 116(2) i.e.

- The person is dead (section 116(2)(a));
- The person is unfit to be a witness because of their bodily or mental condition (section 116(2)(b));
- The person is outside the United Kingdom and it is not reasonably practicable to secure his attendance (section 116(2)(c); or
- The person cannot be found although such steps as it is reasonably practicable to take to find him have been taken (section 116(2)(d)).
- There is a limited form of admissibility if the reason for non-availability to give oral evidence is through fear (section 116(2)(e)).

Although admissibility is generally automatic, there is limited discretion given to the court to exclude evidence if satisfied that the statement's reliability is doubtful in view of:

- Its contents;
- The source of the information contained in it;
- The way in which or the circumstances in which the information was supplied or received; or
- The way in which or the circumstances in which the document concerned was created or received (section 117(7)).

This provision is of particular importance to the prosecution as it is the only way of challenging the admissibility of business and other documents tendered by the defence. The test is in favour of admissibility rather than of exclusion.

Thus in England and Wales hearsay is not a bar to admissibility in either civil proceedings or criminal proceedings. The rule has been well diluted albeit with certain safeguards in place.

6. SINGAPORE

Singapore has journeyed from treating computer output as a special category of evidence to subjecting it to the same evidentiary rules as all other types of evidence. The Evidence (Amendment) Bill 2012 passed on 14 February 2012, introduced progressive changes. The term ‘computer output’ was repealed and replaced with the non- computer specific term, ‘electronic record’ defined in section 3 as:

 ISBN 978-967-11350-4-4

‘ “electronic record” means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or transmitted from one information system to another’.

Further subsections to section 116A introduced four rebuttable presumptions relating to electronic records namely:

(1) mechanical devices were in order when they were used ;
(2) reliability of business records of someone who is not a party to proceedings;
(3) reliability where an electronic record is obtained by a proponent from an adverse party and is used against the adverse party ;
(6) accuracy of an electronic record produced by way of an approved process.

Moreover section 64 Explanation 3 provides that an electronic record will be admissible as primary evidence where shown to be consistently relied on failing which it will be treated as secondary evidence.

The effect of these amendments is that electronic evidence will not be treated as a special category but ‘be subject to the same rules of admission as all other types of evidence, such as the hearsay rule and the rules on authentication’(Ministry of Law, 2012). In *Malcolmson Nichols Hugh Bertram & Anor. v Naresh Kumar Mehta (*2001), various emails were admitted into evidence to prove trespass and harassment. In *SM Integrated Transware Pte. Ltd. v Schenker Singapore Pte. Ltd*.(2005) the Court recognised email correspondence to be writing for the purpose of a contract in interests in land.

6.1 AUTHENTCITY

Sections 116A and section 64 have reduced the burden of establishing the authenticity of electronic records which would include emails. Authenticity of the electronic records and reliability and accuracy of the process can be established by an affidavit deposing to that effect according to the deponents best knowledge and belief (section 116A(7) EA).

6.2 HEARSAY

Generally, computer-generated records which do not contain human information are not subject to the hearsay rule. Computer records may also be admitted in evidence as business records s 32(1)(b). The Business Records Exception was widened to permit the court to admit into evidence all business records produced in the ordinary course of business which appear *prima facie* authentic, including:

(a) any information in market quotations, tabulations, lists, directories or other compilations generally used and relied upon by the public or by persons in particular occupations; and
(b) documents forming (in part or wholly) the records (whether past or present) of a business that are maintained or kept by any person or entity carrying out the business (sections 32A – 32C).

The amendments also carry certain safeguards to prevent abuse. First, the Courts have a discretion to exclude hearsay evidence that does not fall within the statutory exceptions, or where its prejudicial value is greater than it probative value. Secondly, the proponent of such hearsay evidence, has to give notice to all opposing parties of his intention to do so.

Section 116A of the Evidence Act creates a presumption of authenticity and reliability of the electronic record where the proponent of an electronic record can satisfy the Court that it falls within the four presumptions. Further, statutory exceptions to hearsay are set out in section 32 of the Evidence Act. Courts retain the discretion to accord little or no weight to evidence which it deems to have insufficient probative value.

7. MALAYSIA

Section 90A Evidence Act 1950 (EA 1950) with seven subsections, sets out the requirements for admissibility and proof of documents produced by a computer. Section 90B deals with the probative value to be attached to the evidence, while section 90C, stipulates that the provisions of sections 90A and 90B shall prevail over any other provisions in any other statutes.

 ISBN 978-967-11350-4-4

Section 90A(1) EA 1950 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'.

Section 90A(1) relaxes the direct evidence rule or rule against hearsay as provided in section 60 by expressly permitting documents produced by a computer to be admitted albeit with the proviso that it should be produced by the computer ' in the course of its ordinary use'. It is noted that in practice the term 'document produced by a computer' refers to computer printouts or computer generated documents and rarely ever to documents in their 'native' format i.e. copies of the original documents in the format created by the authoring application, like DOC or XLS with the metadata intact (Christine Musil, 2010). The main elements in the subsection would be:

(i) document produced by a computer;
(ii) in the course of its ordinary use;
(iii) whether or not the person tendering it is the maker.

7.1 AUTHENTICITY AND HEARSAY
In *Gnansegaran a/l Pararajasingam v PP*(1997), Mahadev Shankar JCA clarified that :

> 'The effect of s 90A(1) … 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 section 60 of the Act beyond the extent to which its provisions have been diluted by section 32(b) in the case of document made in the ordinary course of business. A situation could thus arise under section 90A(1) where the particular person who keyed in the information may not be individually identifiable, but the document would nevertheless be admissible'.

Thus section 90A EA1950 dilutes the rule against hearsay and recognises the existing 'business records' exception in section 32(b) EA 1950. Further section 62 EA 1950 provides that a document produced by a computer shall be primary evidence. Section 90A therefore prima facie removes any obstacles to the admissibility and authenticity of emails. In *Petroliam Nasional Bhd v Khoo Nee Kiong* (2003), the court accepted that e-mails, instant messages and digital photographs stored in a computer constituted documents produced by a computer. It also acknowledged that an email could be authenticated by "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances". Further circumstantial evidence including the document's own distinctive characteristics and the circumstances surrounding its discovery could also establish its authenticity.

However interesting issues relating to emails arose in the case of *Avnet Azure Sdn Bhd v Eact Technologies Sdn Bhd and Sapura Research Sdn Bhd*.(2011). A server generated email was crucial evidence in a tripartite online contract dispute. Spaura denied having received an email from IBM Singapore. The first question was whether an email was a 'document produced by a computer'. Although a certificate under section 90A(2)EA 1950 was tendered the email was ruled inadmissible. The court was unable to reconcile the meaning of the terms 'document produced by a computer' and 'computer output'. The Court was referred to the then Singapore provision section 35 (1) EA that **'**computer output is admissible in court as primary evidence …..' Nevertheless the court was of the opinion that the two expressions were not in pari materia. Regrettably the court was not referred to the clarification provided in section 2 Computer Crimes Act 1997 (CCA 1997) which specifically equates a 'document produced by a computer' to 'computer output'. The court took the view that a document 'produced by a computer' referred to input of data which would be recorded, stored, analysed or processed through some software programme as 'computer output'. A computer was not just a device to receive messages sent by others. The recipient computer would not have 'produced' the email message. Unfortunately no submissions were made on the scope of the definition of the terms 'computer' and 'document' as given in section 3 EA 1950 or to the definition in section 2 CCA 1997 which specifically includes a 'communication facility'. The crux of the problem was that Sapura categorically denied receipt of the email from IBM Singapore. As proof Avnet tendered a server generated e-mail with the 'Proof of Entitlement' (POE) as attachment sent by IBM Singapore directly to Sapura on 31 March 2009, marked exhibit 'P4'. This was submitted as proof of delivery together with a certificate under section 90A(2)EA 1950. Avnet contended that once this computer evidence was admitted upon production of the certificate, the truth of the contents must be held proven. Avnet's witness P4, also explained the circumstances of the

ISBN 978-967-11350-4-4

contract in detail. Despite the section 90A certificate and oral testimony the court questioned the admissibility and evidential weight of email messages. This was inspite of the fact that the only rebuttal evidence on the part of Sapura was a bare denial without more. The Court held the view that an email without the maker being called was inadmissible. The Court also required Avnet to prove receipt of the email by Sapura. In response Avnet tendered 'ID12' which was a screen shot of the system status at IBM Singapore stating that "message was mailed to: wanzil@Sapura.com.mv' user-type U". However this was also rejected as hearsay on two grounds. First, that it came from IBM Malaysia although it originated from IBM Singapore and secondly it was hearsay as the makers were not called. The result was that the Court found that Avnet had not proved its claim and dismissed its claim.

It is submitted that though section 90A has provided for the admissibility of computer generated documents confusion persists resulting in inconsistencies in findings by the Courts (Gita Radhakrishna).

8. CONCLUSION AND RECOMMENDATIONS

The four jurisdictions under study have established statutory provisions for the admissibility of computer generated or 'electronic' records. Emails qualify under this category and are routinely introduced into evidence. While Malaysia still uses 'computer' specific terminology, the USA, EW and Singapore have opted for the neutral, non- computer specific term of 'electronic' records. All the jurisdictions under study have considerably relaxed the rule against hearsay with safeguards such as the requirement of notice to opposing parties and vesting the discretion with the Courts on the weigh to be given to the evidence. Presumptions on the reliability, accuracy and authenticity of the computer and contents of the document may be established by certification by a person in authority. Additionally the USA and EW have detailed provisions on what amounts to 'business records'. It is submitted that Malaysia could learn from these provisions and establish certain guidelines on the authentication of electronic records in general and emails in particular. The guidelines established in *United States v. Safavian* on authenticating emails would be especially useful. It is important to note that none of the cases considered raised the issue of the requirement of proof of receipt of an email. It is submitted issues such as this could be cleared at the pre-trial case management stage where documents to be relied on would be disclosed and exchanged.

REFERENCES

[2]Benjamin Wright: The Law of Electronic Commerce EDI, Fax, and E-mail: Technology, Proof, and Liability (Boston: Little, Brown & Co., 2nd ed., 1995) at 6.

BIP008 (Code of Practice for Legal Admissibility and Evidential Weight for Information Stored Electronically

Collin Tapper, Cross and Tapper on Evidence (Oxford University Press, 12th. Ed, 2010) 64

Christine Musil**,** The Reality of Native Format, Production and Redaction, EDRM White Paper Series 26 August 2010. <http://www.edrm.net/resources/edrm-white-paper-series/the-reality-of-native-format>

Friedrich W. Seitz and Lynn J. Harris, Document Discovery in the Electronic Age <http://www.thefederation.org/documents/seitz.htm>

Gita Radhakrishna, E-mail Evidence and the Hearsay Rule – Commentary on a recent Malaysian case' Digital Evidence and Electronic Signature Law Review 10[2013] 107

Gregory P. Joseph, Internet And Email Evidence (Part 1) The Practical Lawyer February 2012 at p 19 <www.jha.com/us/filemanager/tpl1112_joseph.pdf>

Jonathan D. Frieden and Leigh M. Murray, 'The Admissibility of Electronic Evidence under the Federal Rules of Evidence' Richmond Journal of Law and Technology Vol. XVII, Issue 2, 2011) 23

Marcella, Albert J., Jr Cyber Forensics : A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes. (Auerbach Publishers Incorporated, USA) (2002) xvi <http://site.ebrary.com/lib/mmulibrary/Doc?id=10074940&ppg=17>

Mark Palmer, 'Electronic document admissibility and retention'(2010) <http://www.midrepro.co.uk/upload/casestudies/electronic_document_admissibility_and_retention.pdf>

Michele C.S. Lange & Kristin M. Nimsger: Electronic Evidence and Discovery: What Every Lawyer Should Know(Chicago: ABA 2004) at 7

Michael R. Arkfeld, Arkfeld's Best Practices Guide for Electronic Discovery and Evidence (Law Partner Publishing 2013-14 ed.) 107

ISBN 978-967-11350-4-4

Paul W. Grimm, Michael V. Ziccardi, Alexander W. Major, 'Back To The Future: Lorraine v. Markel American Insurance Co.' 42 Akron Law Review (2009) 357.
Stephen Mason, General Editor with a team of contributors, 'Electronic Evidence' (Second ed.LexisNexis 2010)94

CASES

USA

*Canatxx Gas Storage Ltd. v. Silverhawk Capital Partners LLC, Civ. No. H-06-11330, 2008 U.S. Dist. LEXIS 37803, at *36–37 (S.D. Tex. May 8 .*
*Clement v California Department of Corrections*2002 U.S. Dist. LEXIS 17426 at *32 (N.D. Cal. Sept. 9, 2002)
Civil Action No. PWG-06-1893 District Court of Maryland. 241 F.R.D.,534,(D.Md.2007)
Doali-Miller v. SuperValu, Inc.,2012 U.S. Dist. LEXIS 50841(D. Md. Apr. 11, 2012).
*Jack R. Lorraine and Beverly Mack v. Markel American Insurance Company*241 F.R.D. 534 (D.Md. 4 May 2007)
Jimena v. UBS AG Bank, Inc., 2011 U.S. Dist. LEXIS 68560 (E.D. Cal. June 24, 2011)
[1] 435 F. Supp. 2d 36, 40 (D.D.C. 2006)
*State of New York v. Microsoft Corp*2002 U.S. Dist. LEXIS 7683 at *14 (D.D.C. April 12, 2002)
Suni Munshani v. Signal Lake Venture Fund II, LP, et al., [2004] 60 Mass. App. Ct. 714
< http://masscases.com/cases/app/60/60massappct714.html>
Trade Finance Partners, LLC v. AAR Corp. 2008 U.S. Dist. LEXIS 32512 (N.D. Ill. Mar. 31, 2008

England & Wales

R v Mawji [2003] EWCA Crim 3067, [2003]AER (D) 285(Oct.)
Villalba v Merrill Lynch & Co. Inc ET/2302467/03 & ET/2305203/03, [2004]AER (D) 36 July

Singapore

Malcolmson Nichols Hugh Bertram & Anor. v Naresh Kumar Mehta[2001] 3 SLR(R) 379
SM Integrated Transware Pte. Ltd. v Schenker Singapore Pte. Ltd. [2005] SGHC 58

Malaysia

Avnet Azure Sdn. Bh.d v Eact Technologies Sdn Bhd and Sapura Research Sdn. Bhd.(22nd September 2011) KL HC Com. Div. D-22NCC439-201
Gnansegaran a/l Pararajasingam v PP, [1997] 3 MLJ 1, CA
Petroliam Nasional Bhd v Khoo Nee Kiong, [2003] 4 MLJ 216

Statutes

USA

Federal Rules of Evidence Rules 101, 401, 801, 802,803, 901, 902

England & Wales

Civil Evidence Act
Criminal Justice Act

Singapore

Evidence Act

Malaysia

Evidence Act 1950