Electronic Evidence
Singapore's Electronic Transaction Act

Electronic communications are paperless. A paper document is human-readable instead of machine-readable. An electronic record can only be read through software programs that convert machine-readable data into human-readable data. A paper document has only one original and the rest are copies. An electronic record can have many "originals". An electronic record may be stored as many "copies", in different electronic locations.

It is open to challenge as to which copy is the complete version. A stored paper document is not normally vulnerable to alteration or forgery if stored in a secured physical space such as a safe. A stored electronic record is vulnerable to deterioration caused by viruses, the impact of magnetic, electrical or electronic interference, and software bugs. Data in the electronic record may then be deleted.

As a result the integrity of the electronic record can be called into question. Electronic data is easily edited, modified and transferred in seconds worldwide to recipients who will not be able to tell which the original version is. Electronic evidence can therefore be unreliable and be fraudulently altered or misrepresented. Electronic evidence will pose challenges different from that of paper - based evidence.

There are important legal issues on the admissibility of electronic evidence in legal proceedings. These issues have to be addressed if electronic records are to be trusted worldwide in electronic communications and electronic commerce.

S Y N O P S I S

This paper will discuss the provisions of the Singapore Electronic Transactions Act ("ETA") so far as electronic evidence is concerned. The purpose of the ETA is to remove any doubts as to the legal consequences of electronic transactions.

This paper will focus on : what is the effect of recognising electronic records or computer records as evidence for electronic commerce? The paper will discuss how the ETA addresses the legal issues arising from relying on electronic evidence and electronic records, the legal status of electronic contracts and the legal standing of digital signatures. In the process, the paper will review the amendments to the Singapore Evidence Act, and the relevant provisions of the UNCITRAL Model Law on Electronic Commerce, and the UNCITRAL Model Law on Electronic Signatures.

This paper will consider generally the legal issues that may arise in admitting electronic records as evidence. Finally the paper will conclude with observations on the way electronic evidence is changing some of the traditional concepts and rules of evidence.

LEGAL PRESUMPTIONS ON ELECTRONIC RECORDS
THE SINGAPORE ELECTRONIC TRANSACTIONS ACT ("ETA")

The ETA gives legal recognition to electronic records and electronic signatures by way of evidentiary presumptions to ensure these have the same legal effect, validity or enforceability as paper records. Briefly, the presumptions are:

1. *There is no legal difference between electronic records and paper records.*

2. *There is no legal difference between electronic records and paper documents when satisfying the legal requirements of being in writing.*

3. *There is no legal difference between an electronic signature and a hand-written signature when satisfying the legal requirement of a signature.*

4. *There is no legal difference between electronic records and paper records when admitting these as evidence in legal proceedings.*

5. *There is no legal difference between a contract entered into electronically and a paper contract.*

ELECTRONIC EVIDENCE : ISSUES ON THE ADMISSIBILITY OF COMPUTER RECORDS

By reviewing the requirements of the Evidence Act and the ETA on electronic evidence, it is clear there are particular issues to consider on the admissibility of computer records as evidence in court. These issues may be summarised as:

1. **Authentication :** Electronic records, like paper documents, must be authenticated before they can be admitted as evidence in court. This can be done by direct evidence from the creator of the electronic record; by establishing audit trails in the sender's computer systems; by encryption technology; and by transmitting all electronic communications through an intermediary. This issue of authentication has been addressed to a large extent by section 35 and 36 of the Evidence Act. The possible areas for challenge may be the reliability of the computer program that generated the records, and the identity of the author of a computer-stored record.

2. **Identifying the Author of a computer-stored record :** A computer-stored record is a document that contains the writings of a person or persons in an electronic form. As with any evidence containing human statements, a computer-stored record is subject to the hearsay rule on the admissibility of evidence. If this record is offered in evidence, the offeror must show circumstances indicating that the human statements contained in this record are reliable and trustworthy. Before the offeror can do so, he must first prove who is the author of the human statements contained in the computer-stored record. This may be a difficult problem in internet communications where authors remain anonymous. It is less likely to be a problem with

commercial correspondence in electronic form.

3. **Challenging the Reliability of Computer Programs :** This is likely to be an important issue for computer-generated records. A computer-generated record contains the output of computer programs, without any human intervention. Examples include log-in records from internet service providers, acknowledgement of receipts of e-mails, auto-replies in an electronic mail system, ATM receipts for cash withdrawals, etc. The fact that a computer rather than a human has created the record makes it critical to determine whether the computer program that generated the computer output was functioning properly. It is possible that despite the admission of a section 35 certificate under the Singapore Evidence Act, parties may specifically challenge the reliability of a specific computer program if it is relevant to the proceedings.

4. **Computer records that are both computer-generated and computer-stored :** An Excel spreadsheet containing financial figures processed by a person is an example of this type of computer record. The evidentiary issues here are :
   (a) the information contained in the Excel spreadsheet is subject to the hearsay rule; and
   (b) the Excel program itself is subject to challenge as to the reliability of the program.

5. **The Hearsay Rule :** The hearsay rule exists to exclude out-of-court statements (statements made outside the courtroom) when such statements are used to affirm the truth of the facts contained in these statements and the makers of these statements are not witnesses in the court. The makers of these statements must be examined in court to give evidence on the truth of these statements. This paper will not go into the many issues arising on the hearsay rule (particularly in criminal proceedings). It is not always the case that computer records are subject to the hearsay rule. Computer-generated records which do not contain human information are not subject to the hearsay rule. Computer records may be admitted in evidence as business records and official government records.

6. **The Best Evidence Rule** : The *best evidence rule* states that "there is but one general rule of evidence, the best that the nature of the case will admit". This rule has been interpreted in some jurisdictions to mean that no evidence other than the original of a writing is admissible to prove the content of the writing. The UNCITRAL Model Law (EC) pre-empts this by making it clear a data message shall not be denied admissibility as evidence on the ground that it is not in its original form. This is because it is difficult to define an "original" document in an electronic record. For example, it has been said that the original of a photograph may be the negative. Practicality and commonsense require that any print from the negative may be regarded as an original. Computer print-outs, like photographs, may have an infinite number of originals.

CONCLUSION

There are many obstacles and challenges to the admissibility of electronic evidence in court. Electronic evidence challenges the traditional rules on the admissibility of evidence, for example, the best evidence rule. New obstacles are created because of the nature of computer technology itself such that it is necessary to re-examine the application of the hearsay rule, or to make evidentiary presumptions for or against the hearsay rule.

Electronic evidence may sometimes have better evidential weight than paper-based evidence. For example, encryption technology in electronic communications can almost make it fairly certain that electronic records can be attributed to the correct signatory, for example, secured electronic records as defined in the ETA.

Most electronic mail communications can be attributed to the correct signatories through secure passwords and access codes. The storage of electronic evidence, very often in disk files not known to the creator of the electronic evidence, may actually make it easier to rebut or corroborate the evidence. At best, it can make it harder to totally delete unwanted electronic evidence.

Singapore has attempted to keep in step with developments in electronic communications by updating the Evidence Act, and by giving legal authority and evidential weight to electronic records and electronic signatures through the ETA, and through accompanying regulations. Singapore also attempts to harmonise its laws and regulations to keep in line with those of its major trading partners by working with the UNCITRAL Model Laws, the OECD Guidelines, ICC's Guidec, APEC, the WTO and other international organisations.

This is not the full LLM Paper.
Dated: 28 January 2002