CONSULTATION

COMPUTER OUTPUT AS EVIDENCE
CONSULTATION PAPER

TECHNOLOGY LAW DEVELOPMENT GROUP
SINGAPORE ACADEMY OF LAW
SEPTEMBER 2003

About the Consultation Paper

This consultation paper, completed in September 2003, is circulated for comment and review. The paper reflects the authors' current thinking on the researched area of law and does not represent the official position of Singapore Academy of Law or any governmental agency. The paper has no regulatory effect and does not confer any rights or remedies.

Comments and feedback on this consultation paper should be received before 30 November 2003. All correspondence should be addressed to:

Technology Law Development Group
Singapore Academy of Law
3 St Andrew's Road
Third Level, City Hall
Singapore 178958
Email: tldg@sal.org.sg
Fax: (65) 6336 6143

Electronic editions of this paper are available for download from the Singapore Academy of Law website at http://www.sal.org.sg and from the Attorney-General's Chambers website under the "Publications" option of Law Reform and Revision Division, at http://www.agc.gov.sg/index3.htm.

Authors:

Daniel Seng

Director of Research, Singapore Academy of Law &
Visiting Associate Professor, Faculty of Law, National University of Singapore

Sriram Chakravarthi

Legal Researcher, Singapore Academy of Law

ISBN 981-04-9653-2

About the Technology Law Development Group

The Technology Law Development Group ('TLDG') is a think tank established by the Singapore Academy of Law to engage in technology law research and reform with a view to assessing the adequacy of existing laws and formulating broad solutions on these issues. The think tank aims to address the need to ensure that Singapore's laws remain relevant and conducive to the development of technological innovations and businesses.

The think tank is chaired by The Honourable Second Solicitor-General Lee Seiu Kin and headed by the Academy's Director of Research Associate Professor Daniel Seng. Its advisory group comprises representatives from the legal sector, information technology industry, financial services industry and government.

About the Authors

Daniel Seng is a Visiting Associate Professor with the Faculty of Law, National University of Singapore, and concurrently, Director of Research, Singapore Academy of Law.

A law graduate of the National University of Singapore in 1992 from which he obtained a first class, Associate Professor Seng obtained the degree of Bachelor of Civil Laws from Oxford University in 1994, where he also obtained a first class and was the recipient of the Rupert Cross prize for that year. As a member of the Faculty of Law at National University of Singapore, Associate Professor Seng teaches information technology law, infocommunications law and the law of evidence and procedure. He has presented papers at various regional and international conferences and published numerous articles on information technology law and evidence.

Associate Professor Seng has also served as a member of various governmental committees responsible for legislative reforms in the area of information technology law in Singapore. He is presently a member of the Technology Law Development Group and also a member of the National Internet Advisory Committee Legal Sub-Committee.

Sriram Chakravarthi is a legal researcher at the Singapore Academy of Law.

A commerce graduate of the University of Madras, India in 1996 and a law graduate of Bangalore University, India in 1999, Sriram obtained his Master of Laws degree from Tulane University, USA in 2000.

Upon completing his LL.M, Sriram worked for a year in California with an IT consulting firm before joining the Faculty of Law, National University of Singapore to pursue his Ph.D. During his stint at NUS, he was awarded the NUS Graduate Scholarship and the 2002-03 President's Graduate Fellowship.

Sriram's areas of research interest include technology law and intellectual property law.

Foreword

In 1996, significant amendments were made to sections 35 and 36 of the Singapore Evidence Act to provide for the admissibility and weight of computer output as evidence in both civil and criminal proceedings. As I noted in the recent case of *Lim Mong Hong v Public Prosecutor* [2003] 3 SLR 88, the pervasive role played by computers in today's society and the increase in computerisation of records will no doubt lead to more and more computer output being presented in evidence.

Since the turn of the century, there have been rapid advancements in hardware and software technologies and widespread usage of the Internet. All of these can and will raise complex issues relating to the reliability, authenticity and weight of electronic evidence. Any court assessing such evidence must not merely direct its mind to the manner of its production in evidence but also to the accuracy and authentication of the evidence.

In this regard, we must ensure that our laws of evidence are constantly revised and adapted to the realities of modern business practices.

The Technology Law Development Group ('TLDG') is a think tank established by the Singapore Academy of Law to engage in research and reform of technology law. At the request of the Law Reform & Revision Division of the Attorney-General's Chambers, the TLDG has prepared this research paper entitled "Computer Output as Evidence". This paper seeks to assess the current relevance and adequacy of Singapore's laws and analyse in particular sections 35 and 36 of the Evidence Act. It contains a comparative analysis of computer-related evidentiary

provisions in other select jurisdictions and also outlines several options for possible law reform.

This research paper has been released as a public consultation paper for discussion and feedback. I hope that the paper achieves its purpose and provokes constructive debate on these issues.

Yong Pung How
Chief Justice
Republic of Singapore
September 2003

Introduction

In March 2003 the Law Reform & Revision Division ('LRRD') of the Attorney-General's Chambers requested the Technology Law Development Group, Singapore Academy of Law ('TLDG') to review the provisions of the Singapore Evidence Act that deal with the admissibility of computer output as evidence. The TLDG was also asked to make appropriate recommendations arising from this review, including possible changes to the sections 35 and 36 of the Evidence Act.

We welcomed this reference as we are conscious that the existing legal framework relating to the admissibility of computer output is in need of review. Since the passage of the 1996 amendments to the Evidence Act and the passage of the Electronic Transactions Act in 1998, rapid advancements in information technology have posed new challenges to the legal community. The rules of evidence are not immune from such pressures. At the same time, we are also aware that the legislative framework and the policies that underpin the existing computer output provisions have been carefully considered when they were revised in 1996. The development of policies to regulate the admission of electronic evidence requires in-depth legal research and comprehension of the relevant technologies and their evolution.

This is where the TLDG comes in. The TLDG is a think tank established by the Singapore Academy of Law to engage in technology law research and reform with a view to assessing the adequacy of existing laws and formulating broad solutions on these issues.

To further this end, the TLDG undertook a review of the computer output admissibility provisions in selected juris-

dictions. In addition to Singapore's laws, the other jurisdictions reviewed were Canada, United States, United Kingdom, Australia, South Africa, India and Malaysia.

Our review revealed that the United Kingdom and Canada have extensively revised their laws in relation to electronic evidence. Three broad reasons were advanced for these changes. Firstly, with the prevalence of computer output in our work and home environments, onerous computer-specific rules that govern its admissibility of electronic evidence may have to be simplified. Secondly, computer output is no longer confined to computer printouts and scanned documents but extends to electronic records generated and stored by an increasing multitude of data processing, storing and transmission devices such as mobile phones, electronic organisers and digital cameras. Technology-centric evidentiary provisions are viewed as somewhat dated. Thirdly, with greater systems and process integrity, not all computer output is considered suspect and computer output provisions designed to check issues of system unreliability seem to better serve the electronic evidence of yesteryears.

After a careful review and analysis of our Evidence Act provisions, we are of the view that rather than continuing with the existing sections 35 and 36, it may be more prudent to adopt a technology-neutral non-computer specific approach to admit electronic evidence. In conjunction with the use of presumptions to facilitate the admission of electronic evidence, this approach and its advantages are detailed as Option 2 in Part IV of this Consultation Paper.

We are pleased to release this Paper to set out our review, analysis and conclusions for public consultation. Part I of this Paper describes Singapore's existing evidentiary provisions relating to computer output. Part II outlines the statutory provisions relating to admissibility of computer evidence in Canada, United States, United Kingdom, Australia, South Africa, India and Malaysia. Part III analyses Singapore's approach by setting out the major

considerations underlying its current provisions and identifying existing inadequacies and limitations in our laws. Part IV suggests several options that may be considered for reforming Singapore's current approach towards electronic evidence.

We welcome any feedback and comments concerning this Consultation Paper before 30 November 2003. These will be consolidated and forwarded to the Law Reform & Revision Division of the Attorney-General's Chambers.

Daniel Seng & Sriram Chakravarthi
Technology Law Development Group
Singapore Academy of Law
September 2003

Part I. The Admissibility of Computer Evidence under the Singapore Evidence Act

1.1. The Evidence (Amendment) Act 1996[1] introduced new provisions to the Evidence Act to "facilitate the use of information technology" and to "provide for the admissibility and weight of computer output produced by any computer or network as evidence in both criminal and civil proceedings"[2]. These amendments repealed the then existing provisions regarding admissibility of statements produced by computers that were loosely based on certain provisions of the UK Civil Evidence Act 1968 and the UK Police and Criminal Evidence Act 1984.[3] In its place, a comprehensive set of computer related provisions was inserted.[4] This part of the paper discusses these provisions in the Evidence Act that deal with the admissibility of computer output.

What is "Computer Output"?

1.2. Before computer output can be admitted in evidence "for any purpose whatsoever", it must first be relevant or admissible under the Evidence Act or any other written law. It must in addition satisfy one of the three modes of admissibility set out in sections 35 and 36 of the Evidence Act.[5] "Computer output" is a term that has received a statutory definition under the 1996 amendments. Section 3(1) of the Evidence Act defines "computer output" or "output" as follows:

---

1 Evidence (Amendment) Act 1996 (No 8 of 1996).

2 Explanatory Statement to the Evidence (Amendment) Bill ('Explanatory Statement'), (No 45 of 1995).

3 The original ss 35 and 36 of the Evidence Act were inserted into the Evidence Act in 1969. They were taken from s 5 of the UK Civil Evidence Act 1968 (1968, c 64).

4 Ss 3(1), 35, 36, 36A, 62A and 68A, Evidence Act.

5 *Lim Mong Hong v PP* [2003] 3 SLR 88.

> "computer output" or "output" means a statement or representation (whether in audio, visual, graphical, multi-media, printed, pictorial, written or any other form) —
>
> (a) produced by a computer; or
>
> (b) accurately translated from a statement or representation so produced;

1.3. This is a very broad and general definition, and confirms that "computer output" is not limited to computer print-outs. Such computer output may take many possible forms: audio, visual, graphical, multimedia, printed, pictorial or written. The breadth of this definition is coupled with an equally expansive definition of a "computer", which is set out as follows:

> "computer" means 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;
>
> (d) such other device as the Minister may by notification prescribe;[6]

1.4. The exceptions aside, a "computer" is very broadly defined to mean a: (i) data processing device, (ii) group of interconnected data processing devices, (iii) data storage facilities "directly related to or operating in conjunction with" data processing device or group of such devices, and (iv) communications facility "directly related to or operating in conjunction with" data processing facility or group of such devices. The exceptions are automated typewriters, portable hand held calculators and similar non-

---

6 S 3(1), Evidence Act.

programmable devices that do not have any data storage facility. To date, no devices have been prescribed by the Minister to exclude them from the ambit of this definition. The breadth of this definition means that in addition to documents generated by computers such as personal computers and mainframes, "computer output" will include any "statements or representations" "produced by a computer" that are as varied as digital sound and video recordings, electronic art and dial and meter readings from electronic devices.

How is Computer Output Admitted?

1.5. Under the 1996 amended provisions to section 35, computer output is received in evidence under one of three alternative modes of admissibility: by way of an express agreement between the parties to the proceedings ("express agreement"),[7] by way of output produced via an approved process ("approved process"),[8] and by proof of the proper operation of the computer and the corresponding accuracy of the computer printout ("proof of proper operation and accuracy").[9] If the proponent of the computer output fails to satisfy any of these preconditions to one of the three modes of admissibility, it will be ruled inadmissible, even though it is otherwise admissible by some other rule of evidence.[10] This is clear on the face of the wording of section 35(1).

1.6. Under the "express agreement" avenue, parties to the proceedings can at any stage of the proceedings expressly agree not to dispute the authenticity and the accuracy of the contents of the computer output.[11] Section 35 does not prescribe the form required for this express agreement.

---

7 S 35(1)(a), Evidence Act.

8 S 35(1)(b), Evidence Act.

9 S 35(1)(c), Evidence Act.

10 *Lim Mong Hong v PP*, *supra,* note 5.

11 S 35(1)(a), Evidence Act.

Thus such an agreement need not be in writing and may even be made orally, subject of course only to questions of proof.[12] However, for the prosecution to admit computer output as evidence in criminal proceedings, the agreement must be made with a legally represented accused.[13] In addition, an agreement that is obtained "by means of fraud, duress, mistake or misrepresentation" is vitiated and ineffective to admit the computer output.[14]

1.7. The "approved process" avenue is intended primarily to facilitate the admissibility as evidence of documents and records stored in electronic format. An approved process is a process which has been approved by a certifying authority pursuant to the Evidence (Computer Output) Regulations 1996 ('Evidence Regulations').[15] Currently, by the Evidence Regulations, the approved process only applies to document imaging systems.[16] In other words, physical documents that are digitally captured via a certified document imaging system may be proved by way of electronic records of the document. A certified document imaging system must provide an accurate reproduction of the contents of a document, verifiable by way of an integrity check of the physical process and the imaging system in relation to the capture, committal and output of the document images. The certification process involves a comprehensive audit of all relevant aspects of

---

12 S 35 is also silent as to whether in multi-party proceedings, an agreement is required to be obtained between every party to the proceedings or only as between the proponent and the opponent of the evidence concerned (or any party whose interest will be affected by its admission). It has been submitted that the latter is the correct interpretation. See Seng D, "Computer Output as Evidence" [1997] SJLS 130 at 147.

13 S 35(2)(a), Evidence Act.

14 S 35(2)(b), Evidence Act.

15 Evidence (Computer Output) Regulations 1996 (1997 Rev Ed RG1 G.N. No S 93/96) ('Evidence Regulations') which were made by the Minister pursuant to s 35(5) Evidence Act.

16 First Schedule: Compliance Criteria for Image Systems, Evidence Regulations, *ibid*.

the imaging process and its surrounding procedures,[17] conducted by an approved "certifying authority" appointed under the Evidence Regulations.[18]

1.8. To tender the computer output of an imaged document, the output must be supported by proof that the output is obtained from an approved process and that it accurately reproduces the contents of the original document. This may be satisfied by way of the production of two certificates: a certificate signed by a person holding a responsible position in relation to the operation and management of the certifying authority to certify that the process has been approved,[19] and a certificate by a person holding a responsible position in relation to the operation or management of the approved process, to certify that the computer output is obtained from the approved process.[20] Where this is done, the computer output is presumed to accurately reproduce the contents of the original document unless the contrary is proved.[21]

1.9. In some document imaging systems, the system or process may cause certain features of the original document *e.g.* boxes, lines or patterns to be removed from the reproduction. Also, some of the features of the original document such as shades, colours or graphics may be reproduced inaccurately.[22] An evidential concession is made in this regard. Section 35(10) provides that where notwithstanding these imperfections in the reproduction, if the

---

17 *Ibid.*

18 *Ibid.* Evidence (Computer Output) Regulations 1996 - Appointment of Certifying Authorities (S 273/2001 dated 16 May 2001) where the Minister of Law appointed the following organisations as certifying authorities: KPMG Consulting Pte Ltd (until 16 May 2002), Ernst and Young (until 24 September 2003) and PriceWaterhouse Coopers (until 20 March 2004). The Auditor General is deemed to be the certifying authority under Regulation 4 of the Evidence Regulations.

19 S 35(3), Evidence Act.

20 S 35(4), Evidence Act.

21 *Ibid.*

22 Explanatory Statement, *supra*, note 2.

accuracy of the relevant contents is not affected, the output will not be rendered inadmissible. However if the accuracy of the contents is compromised, these reproduction imperfections may vitiate the admissibility of the output.

1.10. The "proof of proper operation and accuracy" avenue is the residual avenue for admission of computer output that fails to be admitted pursuant to an express agreement or is not produced pursuant to an approved process. A party tendering such output under section 35(1)(c) must satisfy two conditions. The first condition, a negative condition, requires the proponent to show that "there is no reasonable ground for believing that the output is inaccurate because of the improper use of the computer, and that no reason exists to doubt or suspect the truth or reliability of the output" (the "not unreliable output" condition).[23] The second condition, a positive condition, is that "there is reasonable ground to believe that at all material times the computer was operating properly" (the "proper operation of computer" condition).[24]

1.11. Compliance with both conditions can be shown by a certificate.[25] Such a certificate must be signed by a person, generally the designated "systems operator" or the "information systems manager", holding a responsible position in relation to the operation and management of the relevant computer system. Section 35(6) further provides that such a certificate must, in addition to dealing with both conditions as set out above:

- identify the output and describe the manner in which it was produced; and

---

23 S 35(1)(c)(i), Evidence Act.

24 S 35(1)(c)(ii), Evidence Act.

25 It has been held that proof of both the s 35(1)(c) conditions by a certificate pursuant to s 35(6) is not to the exclusion of other modes of establishing proof. See *Lim Mong Hong v PP*, *supra*, note 5.

- give particulars of any device involved in the processing and storage of such output.

1.12. The Evidence Act recognises the fact that for stand-alone computers and small local area networks, an organization may not have a dedicated systems operator or information systems manager. Furthermore, for wide area networks or large systems, one person alone may not have sufficient knowledge of the relevant computer output.[26] Therefore, section 35(7) provides that where a person who occupies "a responsible position in relation to the operation or management of the computer did not have control or access over any relevant records and facts" to permit this person to make the requisite section 35(6) certification, a supplementary certificate may be signed by another person who had such control or access to the computer system. Such a person may be a part time or contract systems operator or manager, or one of the joint managers of a system for which no one person alone has the exclusive access or knowledge. Section 35(7) therefore envisages the production of two certificates in evidence to support the admissibility of the computer output.

1.13. In the absence of a systems operator or manager,[27] or where the primary certifier or supplementary certifier refuses or is unable for any reason to make the requisite certification, for instance, because he is dead or un-available, under section 35(8), a certificate signed by a person such as an expert "who had obtained or been given control or access to the relevant records and facts" may be tendered instead.

1.14. In all the above instances where a certificate is tendered, it is sufficient for the certifier to state the relevant matter to the best of his knowledge and belief.[28] However, to prevent this process from being abused and to preserve the

---

26 Explanatory Statement, *supra*, note 2.

27 *Ibid.*

28 S 35(9), Evidence Act.

sanctity of the certification process, especially where a certificate is used as a tool to admit false evidence, a person who knowingly makes a false or untrue statement in a certificate is guilty of an offence, which is punishable upon conviction by a fine or imprisonment of up to two years, or both.[29]

Secondary Evidence

1.15. Once computer output is admitted pursuant to one of the three modes of admissibility outlined above, section 35(10)(b) provides that it shall not be inadmissible merely on the ground that it is secondary evidence. In other words, there is no requirement to produce the "original document".[30]

Weight of Computer Output

1.16. Even though the court may have admitted the computer output as evidence pursuant to section 35, it may still have doubts as to whether the computer output "accurately reproduces the relevant contents of the original document".[31] Thus the provisions under section 36 reserve for the court a discretion to call for further evidence, presumably to either prove or disprove its doubts. Section 36 allows for such further evidence to be required by way of affidavit from the certifiers whose certificates were tendered to support the admission of the computer output under section 36.[32] The court may even appoint or accept

---

29 S 35(11), Evidence Act.

30 S 35(10), Evidence Act. See also Part III, para 3.134.

31 S 36(1), Evidence Act.

32 S 36(2), Evidence Act. The reference to a person (a) "occupying a responsible position in relation to the operation or management of the certifying authority" is a reference to a s 35(3) certificate, (b) who occupies "a responsible position in relation to the operation of the computer at the relevant time" is a reference to either a s 35(4) or a 35(6) certificate, (c) who "had control or access over any relevant records and facts in relation to the production of the computer output" is a reference to a s 35(6) or a s 35(7)

an independent expert who can contribute his evidence by way of affidavit for consideration by the court.[33] In addition, the court may require oral evidence to be given "of any matters concerning the accuracy of the computer output", and may require a certifier or the deponent of the affidavit to testify.[34]

1.17. The issue of the probative value of the admitted computer output is addressed in section 36(4). The section provides that the court in estimating the weight of computer output shall have regard for "all the circumstances from which any inference can be reasonably drawn as to the accuracy or otherwise" of the computer output. Additionally the court must also give consideration as to whether the information reproduced in the computer output was supplied or recorded contemporaneously with the occurrence or existence of the facts dealt with in the information,[35] and as to whether any information supplier or processor had any incentive or motive to conceal or misrepresent the information so supplied.[36] Section 36(4) was applied by the Singapore High Court in *Lim Mong Hong v PP* to accord little weight to computer output in the form of a computer printout previously admitted under section 35(1)(c) of the Evidence Act.[37]

Other Technology-specific Provisions

1.18. The 1996 amendments to the Evidence Act amendments also enabled the Rules Committee constituted under the Supreme Court Judicature Act (Cap 322, 1999 Rev Ed) to make rules for the filing, receiving and recording of evidence and documents in court by using information

---

certificate, (d) who "had obtained or been given control or access over any relevant records and facts" is a reference to a s 35(8) certificate.

33 S 36(2)(e), Evidence Act.

34 S 36(3), Evidence Act.

35 S 36(4)(a), Evidence Act.

36 S 36(4)(b), Evidence Act.

37 *Lim Mong Hong v PP*, *supra,* note 5.

technology.[38] Pursuant to section 36A, the Rules Committee has promulgated Order 63A of the Rules of Court on Electronic Filing and Service.[39]

1.19. The Act also provides two other provisions that encourage the greater usage of information technology in the courts. Section 62A enables the use of live video or live televisions links in court for the purpose of giving evidence. The other provision, section 68A, facilitates the usage of charts, summaries, computer output and multi-media technology in the courtroom for the presentation of complex or voluminous evidence. To prevent such evidence from being used as a substitute for supporting evidence, section 68A requires that any relationship among facts or opinions asserted in the presentation materials must be proven by relevant and admissible evidence.[40]

1.20. Section 35(1) has made provision for its admissibility rules to be overridden by written law. Such provisions exist in several other laws such as the Companies Act[41], the Land Titles Act[42] and the Business Registration Act[43]. For instance, section 12A of the Companies Act states that notwithstanding the provisions of any other written law, copies of electronically filed documents are admissible in evidence as of equal validity with the original document and certificates in respect of such electronically filed documents are admissible in evidence as true extracts of the original document. Similarly, section 164(3) of the Land Titles Act states that notwithstanding section 35 of

---

38 S 36A, Evidence Act.

39 Supreme Court Judicature Act (Cap 322, 1999 Rev Ed), Rules of Court, O.63A.

40 S 68A(2), Evidence Act.

41 S 12A(2)-(4), Companies Act (Cap 50).

42 S 164(3), Land Titles Act (Cap 157).

43 S 16B(4)-(6), Business Registration Act (Cap 32, 2001 Rev Ed) provides a similar provision as found in the Companies Act for copies of electronically filed documents and certificates in respect of such electronically filed documents to be admissible in evidence.

the Evidence Act, a printout of any information (other than computer folios) stored in a computer in the Land Titles Registry issued by the Registrar and bearing a facsimile of the Registrar's seal shall be received in evidence in any court as prima facie proof of all the matters contained in or entered on any instrument filed in the Land Titles Registry. An extract of the provisions is provided in Appendix II of this Paper.

1.21. Our research also revealed various other provisions in other laws containing technology-specific provisions that exist not to provide for the admissibility of electronic evidence but to facilitate the use of information technology. Most of these provisions simply state that statutory registers that are needed to be maintained in law can also be maintained in an 'electronic form' and that such documents so maintained are admissible as evidence of the contents thereof.[44] An extract of these provisions is provided in Appendix II of this Paper.

---

44 For example, ss 66(3), 66(4), 68(2), Trade Marks Act (Cap 332, 1999 Rev Ed), ss 7(2), 7(4), 7(5), Trade Unions Act (Cap 333, 1985 Rev Ed), s 42(4), Patents Act (Cap 221, 2002 Rev Ed), ss 42, 43, Goods and Services Tax Act (Cap 117 A, 2001 Rev Ed), ss 71A (5), 71A(6), 71A(7), 71A(8), Income Tax Act (Cap 134, 2001 Rev Ed), s 4(3), National Registration Act (Cap 201, 1992 Rev Ed).

Part II. The Admissibility of Computer Evidence in Other Jurisdictions

Canada

2.1. In 1997, the Uniform Law Conference of Canada ('ULCC'), a law reform body founded to harmonize the laws of the provinces and the territories of Canada,[1] proposed a draft Uniform Electronic Evidence Act ('UEEA') for adoption in Canada.[2] The ULCC explained that "[a]s more and more activities are carried out by electronic means, it becomes more and more important that evidence of these activities be available to demonstrate the legal rights that flow from them."[3] The assessment of the ULCC is that while most electronic records in practice have been admitted in evidence, Canadian courts have struggled with the traditional rules of evidence such as authentication, best evidence, hearsay and weight with inconsistent results.[4] Records managers and their legal advisors were similarly not confident that modern information systems would produce records suitable for use in court.[5] Various provinces in Canada had legislated on electronic evidence, and various government departments had adopted different standards to authorize the use of records from their own computer systems.[6] The ULCC

---

1 See http://www.ulcc.ca/en/home/ (visited 6 June 2003).

2 See Uniform Electronic Evidence Act and Comments (1997) at http://www.ulcc.ca/en/poam2/index.cfm?sec=1997&sub=1997hk (visited 31 March 2003), Uniform Electronic Evidence Act - Consultation Paper (1997) ('ULCC Consultation Paper') at http://www.ulcc.ca/en/poam2/index.cfm?sec=1997&sub=1997hka (visited 31 March 2003) and the Uniform Electronic Evidence Act (1998) ('ULCC Act and Comments') at http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2 (visited 6 June 2003).

3 ULCC Consultation Paper, *ibid*, para 2.

4 *Ibid*, para 3.

5 *Ibid*, para 4.

6 *Ibid*, paras 5-6.

felt that harmonization of the laws will avoid these inconsistencies in laws as well as incompatibilities of information systems.[7] The UEEA is a product of this law reform and consultative exercise that spanned three years.

2.2. The UEEA departs significantly from other jurisdictions by using the term "electronic record"[8] instead of the usual terms "computer evidence" or "computer output".

> **Definitions**
>
> 1. In this Act,
>
> (a) "data" means representations, in any form, of information or concepts.
>
> (b) "electronic record" means data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data, other than a printout referred to in sub-section 4(2).
>
> (c) "electronic records system" includes the computer system or other similar device by or in which data is recorded or preserved, and any procedures related to the recording and preservation of electronic records.[9]

2.3. Careful thought has been given by the ULCC to these terms. The term "data" is used and defined to apply to "any form of information in an electronic record, whether figures, facts or ideas."[10] The term "electronic" is used because a record may be made or preserved in or by a computer system or similar device.[11] So an "electronic record" applies to data on magnetic strips on cards, in smart cards, computer-generated faxes, voice mail and video records made or preserved through computer

---

7 *Ibid*, para 7.

8 In some jurisdictions, the term "electronic document" is used instead. See the Canadian Evidence Act, s 31.8 and the Manitoba Evidence Act 2000, s 51.

9 The version of the UEEA is the version dated September 1998 from the ULCC Act and Comments.

10 S 1(a), ULCC Act and Comments, *supra*, note 2.

11 *Ibid*, s 1(b), UEEA.

systems.[12] The ULCC observed that the current definition of "electronic record" will not include information on paper recorded by a typewriter, but if that same paper record is captured by electronic imaging technology, the imaged form will constitute an electronic record.[13] However, the UEEA excludes from its ambit electronic information that is neither "recorded nor preserved", for instance, digital telephone conversations, since such electronic information is only transmitted by or in a computer system or similar device.[14] This is a deliberate decision on the part of the ULCC to focus the UEEA on electronic record keeping systems.[15]

2.4. The ULCC envisages the enactment of the UEEA rules as rules of evidence to supplement the existing hearsay rules[16] and its exceptions such as the business records rule[17] or the bank records rule[18]. Consequently, the only rules of evidence that are revised under the UEEA are rules dealing with the authentication of electronic record (section 3, UEEA) and the best evidence rule (section 4, UEEA).

2.5. Section 3 requires a proponent seeking to introduce an electronic record into evidence to discharge "the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be." The ULCC states that section 3 merely codifies the common law rule on authentication which applies equally to paper records and follows the formulation as set out in the US Federal Rules of

---

12 *Ibid.*

13 *Ibid.*

14 *Ibid.*

15 *Ibid.* The focus on "electronic record systems" which store "electronic records" is best illustrated by a consideration of ss 4 and 5, UEEA.

16 *Ibid*, s 2, UEEA.

17 S 30, Canada Evidence Act 1997 at http://laws.justice.gc.ca/en/C-5/15124.html (visited 31 March 2003).

18 S 31, Canada Evidence Act 1997 at http://laws.justice.gc.ca/en/C-5/15124.html (visited 31 March 2003).

Evidence.[19] However, the concept of "authentication" that is adopted by the ULCC is a very narrow one, as it stressed that although logically, authentication subjects an electronic record to "attacks on its integrity or reliability … [t]hat question is reserved for the new 'best evidence' rule [under the UEAA]."[20] Therefore, under the UEEA the proponent need only to bring evidence that "the record is what the proponent claims it is". But any evidence adduced as to authenticity and as to accuracy or integrity of the electronic record may facilitate the admissibility of the record.[21] Thus the UEEA acknowledges that the requirements of the business records exception to the hearsay rule and the authentication requirements of electronic records may coincide and overlap.

2.6. Section 4(1) deals with the application of the "best evidence rule" to electronic records. The "best evidence rule" exists to ensure the integrity of the record, since alterations are more likely to be detectable on the original.[22] The ULCC's approach is that electronic records are especially vulnerable to undetectable change,[23] and to this end, the "best evidence rule" serves a useful function to test the accuracy and integrity of electronic records.[24] However, the notion of an "original" record as inherited from the origins of the "best evidence rule" is not easily applicable to electronic records.[25] To this end, a modified "best evidence rule" is developed for electronic records

---

19 This is the position taken by the Canadian Supreme Court in *USA v Shephard* (1976) 30 C.C.C. (2d) 424, per Ritchie J for the majority of the court.

20 S 3, ULCC Act and Comments, *supra*, note 2.

21 S 2(2), UEEA.

22 S 4(1), ULCC Act and Comments, *supra*, note 2.

23 Paras 11, 13, ULCC Consultation Paper, *supra*, note 2.

24 The best evidence rule does not automatically apply to all electronic records: s 4(1), UEEA uses the formulation "where the best evidence rule is applicable in respect of an electronic record", a formulation that is to be found only in the latest (1998) revision to the UEEA.

25 S 4(1), ULCC Act and Comments, *supra*, note 2.

which is satisfied "on proof of the integrity of the electronic records system in or by which the data was recorded or stored".

2.7. The ULCC took this approach because "it will usually be impossible to provide direct evidence of the integrity of the individual record to be admitted. System reliability is a substitute for record reliability."[26] Thus in section 4(1), the focus of the "best evidence" rule shifts away from the "electronic record" to the "electronic record system". Proving the integrity of the system would thereby prove the integrity of the record in whatever form it might be presented. Section 4(2) additionally provides that a printout of an electronic record satisfies the best evidence rule if it "has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout." The intention here is to provide for the admission in evidence physical copies of electronic records where "the reliability of the computer system is not at issue" and where "the record 'lives its life' on paper." Examples of these include business correspondence produced using a computer with word processing software.[27]

2.8. Proving the integrity of the electronic records system is not a straightforward exercise. The ULCC sought to make provisions for this exercise by setting out, in section 5, some presumptions of the integrity of electronic record systems. This rebuttable presumption arises in one of three ways.

2.9. The first presumption is based on evidence that at all material times, "the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic records system."[28] This first presumption as to the integrity of the electronic records system is based on

---

26 *Ibid.*

27 S 4(2), ULCC Act and Comments, *supra*, note 2.

28 S 5(a), UEEA.

evidence of the proper operation of both the computer system that produced the record (hardware) and the record-keeping system in which it operates (software).[29] While the ULCC does not preclude the possibility of admitting business records maintained by a small business on its computer with off-the-shelf software, the ULCC notes that such a record-keeping system could be exposed to more successful attack in court than a sophisticated record-keeping system.[30] However, when this presumption was designed, the ULCC was concerned not to make the process of routinely admitting electronic records more difficult, or not to introduce new grounds for frivolous but possibly expensive attacks on otherwise acceptable records.

2.10. The second presumption arises in relation to electronic records recorded or stored by an adverse party to the proceedings.[31] An adverse party is a party "who is adverse in interest to the party seeking to [introduce the electronic record]."[32] The record is presumed reliable because if it were not, "the other person has the opportunity to show the unreliability and rebut the presumption, since that person knows his or her or its own record-keeping system better than anyone else."[33] The ULCC however is clear that this presumption applies only to records maintained by the adverse party. Records maintained by a friendly third party must be brought within the first presumption in section 5, UEAA, and not the second presumption.[34]

2.11. Records maintained by a neutral third party, "a person who is not a party to the proceedings and who did not record or store [the electronic record] under the control of the party seeking to introduce the record", may be admitted

---

29 S 5(a), ULCC Act and Comments, *supra*, note 2.

30 *Ibid.*

31 S 5(b), UEEA.

32 *Ibid.*

33 S 5(b), ULCC Act and Comments, *supra*, note 2.

34 *Ibid.*

pursuant to the third presumption.[35] This is where the record was "recorded or stored in the usual and ordinary course of business" by the neutral third party. Where the proponent has such control, for instance, because it has contracted out its data processing or record management responsibilities, such records are records controlled by the proponent and the first, and not the third, presumption applies.[36]

2.12. The focus of the UEEA on the electronic record system was premised on the assumption, identified by the ULCC itself, that "it will usually be impossible to provide direct evidence of the integrity of the individual record to be admitted."[37] However, technology has since moved on and it is now possible to have secure electronic records and use secure electronic signatures to verify the integrity of these individual records. Since the release of the UEEA, the Canadian government has recognized this, and in the 2000 amendments to the Canadian Evidence Act, it has been provided that the "best evidence" rule in respect of an electronic record[38] may be satisfied by way of government-prescribed "evidentiary presumptions in relation to electronic documents signed with secure electronic signatures" to associate the secure electronic signatures with persons, and the integrity of information contained in electronic documents signed with secure electronic signatures.[39] It may also be for this reason that in the

---

35 S 5(c), UEEA.

36 *Ibid.*

37 S 4(1), ULCC Act and Comments, *supra*, note 2.

38 S 31.8, Canadian Evidence Act. The formulation "electronic document" is used instead of "electronic record". The definitions are otherwise identical, except for the reference to computer printouts which are not treated as electronic records.

39 S 31.4, Canadian Evidence Act. "Secure electronic signature" is in turn defined in s 31(1) of the Personal Information Protection and Electronic Documents Act 2000 as "an electronic signature that results from the application of a technology or process prescribed by regulations made under s 48(1)." Alberta, Manitoba and Ontario have followed suit with similar provisions in their respective versions of their Evidence Act where

Canadian Evidence Act, the "presumptions" under the UEEA of the integrity of the electronic records system are not enacted as "presumptions",[40] since only the use of secure electronic signatures can be said to give rise to strong presumptions in favour of the integrity of electronic records.

2.13. The UEEA requires the court to consider the reliability of the record-keeping system, and in this regard, section 6 requires the court to consider whether the record-keeping system has adhered to any particular "standard, procedure, usage or practice" in recording and storing the electronic records. Furthermore, this adherence to a particular standard is considered in light of the nature and purpose of the record sought to be admitted, and the type of business which used, recorded or stored the record. By not prescribing any particular standard or practice, section 6 gives records managers broad discretion as to whether to establish and follow their own inter-organisation record-keeping standards, or to follow other external standards which have been established or endorsed for a particular industry.[41] The ULCC cites as an example, the "Electronic Imaging and Microfilm as Documentary Evidence" standard developed by the Canadian General Standards Board.[42] The ULCC also acknowledged the development of standards for storing of electronic records by the International Standards Organization ('ISO'). While compliance with such standards is not obligatory to get the records admitted, such standards are relevant to the question of admissibility of the records. By expressly

---

these technologies are referred to as "secure electronic signatures", "electronic signatures" and "reliable encryption techniques". See s 41.4(2), Alberta Evidence Act (revised 2001), s 51.5, Manitoba Evidence Act (revised 2000) and s 34.1, Ontario Evidence Act (revised 1999).

40 S 31.3, Canadian Evidence Act. A similar formulation is found in the Alberta Evidence Act, the Manitoba Evidence Act and the Saskatchewan Evidence Act.

41 S 6, ULCC Act and Comments, *supra*, note 2.

42 *Ibid.*

recognizing this in section 6, UEEA, the ULCC felt that record managers may take comfort from their compliance with such standards.[43]

2.14. To prove the authenticity of electronic records, and the integrity of electronic record systems, evidence may be given by way of an affidavit given by a deponent, who only needs to attest to such facts as to the best of his knowledge or belief.[44] While the requirement for oral evidence is dispensed with, "[i]f doubt is cast on the reliability of the affidavit, then the person presenting the electronic record may have to provide more detailed support of the record-keeping system."[45] Furthermore, the deponent of the affidavit may be cross-examined as of right by the opponent to the electronic record.[46]

2.15. In summary, the approach taken in Canada is to recognize the need to subject electronic records to closer judicial scrutiny, by requiring such records to be authenticated, and by requiring proof of the integrity of the corresponding record keeping systems. Proof of the latter may be achieved by way of one of three presumptions. The originality introduced by the Canadian approach is to be more favourably disposed towards electronic evidence originating from neutral third parties, but to require proof of the reliability (and refutation of its unreliability) from the proponent (and opponent) of the electronic record. However, no specific legislative provisions were enacted to deal with electronic records as computer-generated records or as real evidence: these are presumably dealt with the usual way under the general rules of evidence.

---

43 *Ibid.*

44 S 7, UEEA.

45 S 7, ULCC Act and Comments, *supra*, note 2.

46 S 8, ULCC Act and Comments, *supra*, note 2. The only exception will be a deponent of a neutral third party who makes an affidavit in support of the admission of an electronic record under s 5(c), UEEA, where leave of the court is required. This is because ULCC does not want the deponent from a non-party to be frivolously disturbed.

United States

2.16. In the United States ('US'), computer records are routinely admitted pursuant to the Federal Rules of Evidence, which are applicable to both civil and criminal proceedings. This is so despite the fact with one notable exception, there are no specific provisions in the Federal Rules of Evidence for admitting computer evidence.[47]

2.17. As such, the US Federal Courts have applied the traditional rules of hearsay, the best evidence rule and the authentication rule to computer evidence. When admitting computer evidence, most Federal Courts have focused on the application of the hearsay rule to these records, and drawn the distinction between computer-generated records and computer-stored records.[48] Whereas computer-generated records are output of computer programs untouched by human hands, computer-stored records contain the writings of some person and happen to be in electronic form. To admit computer-stored records to prove the truth of the matter they assert, the proponent of the records must show circumstances indicating that the human statements contained in the record are reliable and trustworthy (a question of hearsay rule) and that the records are authentic (a question of authentication). However, to admit computer-generated records, while the proponent no longer needs to show that a human's out-of-court statement was truthful and accurate (since no question of hearsay arises), the proponent must show that the computer and the computer program that generated the record were functioning properly (a question of authentication).[49]

---

47 The only exception is Rule 1001(3), which deals with the admissibility of electronic records as "originals" under the best evidence rule.

48 See Orin S. Kerr, "Computer Records and the Federal Rules of Evidence", March 2001 at http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm (visited 30 April 2003).

49 *Ibid*, at 143.

2.18. Thus, computerized business records have been admitted under the business records exception in the Federal Rules of Evidence. Adopting a technology-neutral approach, as early as 1969, the US courts have said that "it is immaterial that the business record is maintained in a computer rather than in company books."[50] The courts have undoubtedly been helped by the language of Rule 803(6), Federal Rules of Evidence, which reads:

> **Rule 803. Hearsay Exceptions; Availability of Declarant Immaterial**
>
> The following are not excluded by the hearsay rule, even though the declarant is available as a witness:
>
> (6) Records of regularly conducted activity.—A memorandum, report, *record, or data compilation, in any form*, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit. [our emphasis]

2.19. As the US Federal Court in *United States v Catabran* said, the business records exception in the Federal Rules of Evidence "specifically allows for the admission of a 'data compilation, in any form,' which meets the requirements of the rule."[51] In *Catabran*, the accused were charged with concealing the assets of the bankrupt company while they

---

50 *United States v De Georgia* 420 F.2d 889, 893 (9th Cir. 1969), *United States v Russo* 480 F.2d 1228, 1239-40 (6th Cir. 1973), *United States v Fendley* 522 F.2d 181, 187 (5th Cir. 1975), *United States v Miller* 771 F.2d 1219, 1237 (9th Cir. 1985), *United States v Cestnik* 36 F.3d 904 (10th Cir. 1994), *Dyno Construction v McWane, Inc.* 198 F.3d 567, 576 (6th Cir. 1999), *United States v Briscoe* 896 F.2d 1476, 1494 (7th Cir. 1990).

51 *United States v Catabran* 836 F.2d 453, 457 (9th Cir. 1988).

were directors. The prosecution sought to admit in evidence general ledger computer printouts that listed inventory, payroll and other accounting data put into the computer by the bookkeepers of the company. The court heard evidence from one of the bookkeepers that the sales, inventory, payroll and tax information were kept current in the computer and printouts were produced as a regular practice each month. Before the information was entered into the computer, the information had been manually checked for accuracy. The Federal Court found that prosecution had laid the necessary foundation, concluded that any inaccuracies in the printouts resulting from incorrect data entry or operation of the computer program went only to weight, and admitted the printout in evidence.[52] Similarly, in *United States v Salgado*, the prosecution sought to admit in evidence telephone toll records of telephone subscriptions of the accused.[53] The Federal Court admitted them as business records in evidence, after hearing testimony from the security manager of the telephone company that these toll records were accurate and were relied upon for billing purposes. The US courts were so routinely admitting computer records as business records that by 1990, the Federal Court in *United States v Briscoe* described this exception as "well established".[54]

2.20. In addition, the proponent who seeks to admit either a computer-generated or a computer-stored record must show that it is authentic. Rule 901(a) of the Federal Rules of Evidence reads:

> **Rule 901. Requirement of Authentication or Identification**
>
> (a) General provision.—The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

---

52 *Ibid*, at 458.

53 *United States v Salgado* 250 F.3d 438 (6th. Cir. 2001).

54 *Supra*, note 50, at 1494.

> (b) Illustrations.—By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
>
> …
>
> (7) Public records or reports.—Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.
>
> …
>
> (9) Process or system.—Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

2.21. As computer records can be altered easily, opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created.[55] And unauthenticated evidence is irrelevant unless the proponent of the evidence can show that the evidence is what its proponent claims.[56]Such challenges are met by the proponent through the laying of a proper foundation for the computer records and providing witnesses who handled the evidence to testify as to their authenticity. In *United States v Whitaker*,[57] a FBI agent testified, from his personal knowledge and participation, as to how the accused's computer was seized and how the records were subsequently retrieved. The Federal Court accepted his testimony, and rejected allegations of record tampering by the accused as speculative.[58] Alternatively, authentication may be established if the computer records are taken from a public office where they form part of a public record,[59] or where there is evidence as to the process or system of keeping the information indicated on

---

55 *Supra*, note 48, at 145.

56 *United States v Hernandez-Herrera* 952 F.2d 342, 343 (10th Cir. 1991).

57 127 F.3d 595 (7th Cir. 1997).

58 *Ibid*, at 601-602.

59 *United States v Meienberg* 263 F.3d 1177, 1181 (10th Cir. 2001), applying Rule 901(b)(7), Federal Rules of Evidence

the record and that the process or system produces an accurate result.[60]

2.22. In addition to considerations of hearsay and authentication, US courts have on occasion considered the application of the "best evidence" rule to electronic records. The concern that a printout of a computer-stored electronic file may not be an "original" for the purpose of the best evidence rule is expressly dealt with in the Federal Rules of Evidence:

> **Rule 1001. Definitions**
>
> **For purposes of this article the following definitions are applicable:**
>
> (3) Original.—An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. *If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".*
>
> **Rule 1003. Admissibility of Duplicates**
>
> A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

2.23. Thus if it is shown that a printout accurately reflects the data, it will be held to satisfy the best evidence rule as an "original" document. According to the Advisory Committee Notes on the Federal Rules of Evidence, "practicality and usage confer the status of original upon any computer printout."[61] An accurate printout of computer data always satisfies the best evidence rule.[62] In *United States v Edgemon*, the printouts of the call records from the

---

60 *United States v Edgemon* 1997 U.S. Dist. LEXIS 23828, at 20, applying Rule 901(b)(9).

61 Advisory Committee Notes, Proposed Federal Rules of Evidence, Rule 1001(3) (1972).

62 *Doe v United States* 805 F. Supp. 1513, 1517 (D.Haw. 1992), *Laughner v State* 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002).

telephone company were held to be "original" for listing those calls that were in fact made by the accused. Even if the printout was held not to be an original, it was held to be admissible as a "duplicate" since no genuine questions have been raised as to its authenticity.[63]

2.24. In summary, computer evidence does not pose a serious evidential hurdle to its proponent in US courts. By accepting the distinction between computer-generated and computer-stored records and developing a heightened awareness of the accuracy, reliability and integrity of electronic evidence within the broad general rules of the Federal Rules of Evidence, US jurisprudence has acknowledged the continued relevance of the hearsay, authentication and best evidence rules to electronic evidence and admitted such evidence without the need to introduce computer-specific provisions into its laws.

United Kingdom

2.25. In the United Kingdom, ('UK') unlike the codified rules of evidence that exist in the United States and Canada, the admissibility of computer evidence is governed by a mixture of statutory provisions and common law rules. The statutory provisions governing the admissibility and proof of documentary evidence in the Civil Evidence Act 1995 ('CEA 1995')[64] and in the Criminal Justice Act 1988 ('CJA 1988')[65] are designed to apply to documents containing computer-stored information. This has been accomplished by providing broad identical definitions in both the CEA 1995[66] for civil proceedings and the CJA 1988[67] for criminal proceedings to the term "document" to mean "anything in which information of any description is

63 *Supra*, note 60, at 21-22.

64 Civil Evidence Act 1995 (1995 c 38).

65 Criminal Justice Act 1988 (1988 c 33).

66 S 13, CEA 1995.

67 S 28(5)(1) Schedule 2, CJA 1988.

recorded". This definition is widely worded to include a computer as well as the computer printout from it.[68] Apart from the statutory provisions, at common law computer-generated evidence obtained from computers may also be admissible as real evidence.[69]

2.26. The most common objection to the admissibility of evidence obtained from computers has been that such evidence amounts to hearsay. Over the past decade however, substantial efforts have been made by the UK Law Commission ('Law Commission'), to reform the hearsay rule in civil[70] and criminal proceedings[71], which have in effect eased the admissibility and proof of computer evidence in both civil and criminal proceedings.

2.27. In civil proceedings, following explicit recommendations made by the Law Commission, the CEA 1995 repealed the whole of Part I of the Civil Evidence Act 1968 ('CEA 1968')[72] that dealt with hearsay evidence. Part I included the erstwhile section 5 which, until its repeal, laid down conditions for the admissibility of documents produced by computers.[73] These conditions were specified in section 5(2) of the CEA 1968 and they required the proponent seeking to admit computer-stored documents to prove:

> (a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any

---

68 UK Law Commission Report No 216, *The Hearsay Rule in Civil Proceedings* (1993) ('UK Law Commission Report No 216'). The Law Commission proposed a wide definition for the term "document" to cover documents in any form and in particular to be wide enough to cover computer-generated information.

69 See for example *Re Statute of Liberty* [1968] 2 All ER 195, *R v Wood* (1982) 76 Cr App Rep 23, [1982] Crim LR 667, *Castle v Cross* [1984] 1 WLR 1372, QBD.

70 UK Law Commission Report No 216, *supra*, note 68.

71 UK Law Commission Report No 245, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (1997) ('UK Law Commission Report No 245').

72 Civil Evidence Act 1968 (1968 c 64).

73 CEA 1995, Schedule 2.

> activities regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by any individual;
>
> (b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;
>
> (c) that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and
>
> (d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

2.28. In calling for the repeal of section 5 of the CEA 1968 without any replacement,[74] the Law Commission took note of the technological changes that intervened in the span of time between the enactment of CEA 1968 and its subsequent reconsideration.

> Twenty-five years later, technology has developed to an extent where computers and computer-generated documents are relied on in every area of business and have long been accepted in banking and other important record-keeping fields. The conditions have been widely criticized, and it has been said that they are aimed at operations based on the type of mainframe operations common in the mid 1960's, which were primarily intended to process in batches thousands of similar transactions on a daily basis.[75]

2.29. Taking these considerations into effect, the Law Commission concluded that the admissibility requirements of section 5 posed substantial fetters to businesses as to their means of proof, that it remained questionable as to whether these requirements provided any real safeguards in relation to the reliability of the hardware or software concerned and that the provisions provided no protection

---

74 UK Law Commission Report No 216, *supra*, note 70, para 4.43.

75 *Ibid*, para 3.14.

against the inaccurate input of data.[76] Furthermore, the Law Commission opined that in relation to computer records:

> [T]he real issue for concern was authenticity and that this was a matter which was best dealt with by a vigilant attitude that concentrated upon the weight to be attached to the evidence, in the circumstances of the individual case, rather than by reformulating complex and inflexible conditions as to admissibility.[77]

2.30. The Law Commission therefore recommended that:

> 5.13 Documents, *including those stored by a computer*, which form part of the records of a business or public authority should be admissible as hearsay evidence… and the ordinary notice and weighing provisions should apply.
>
> 5.14 The current provisions governing the manner of proof of business records should be replaced by a simpler regime which allows, unless the court otherwise directs, for a document to be taken to form part of the records of a business or public authority, if it is certified as such, and received in evidence without being spoken to in court. *No special provisions should be made in respect of the manner of proof of computerised records.*[78] [emphasis ours]

2.31. Following the repeal of Part I of the CEA 1968, the CEA 1995 now provides for the admissibility of hearsay evidence and no longer distinguishes between traditional physical documents and computer-stored documents.

2.32. In criminal proceedings, the Law Commission in 1997 proposed a similar set of reforms aimed at easing the rules relating to admission of hearsay and the relaxation of proof as had been accomplished by the CEA 1995.[79] In its examination of the hearsay rule, the Law Commission also considered the issues relating to computer evidence in criminal proceedings[80] by specifically considering the situation of statements produced by machines. In cases where statements are not based on human inputs but are

---

76 *Ibid*, para 3.15.

77 *Ibid*, para 3.21.

78 *Ibid*, Part V Recommendations, paras 5.13 and 5.14.

79 UK Law Commission Report No 245, *supra,* note 71.

80 *Ibid,* Part XIII.

produced by machines that automatically record an event or circumstance, the Law Commission stated that such a statement would fall outside the proposed definition of a statement and such evidence would not be hearsay but real evidence.[81] As regards statements produced by machines that are based upon human input, the Law Commission sought to liberalise the admissibility requirements of hearsay by proposing the repeal of section 69 of the Police and Criminal Evidence Act 1984 ('PACE 1984').

2.33. Section 69 of PACE 1984, had until its repeal provided additional conditions for the admissibility in criminal proceedings of records derived from computers.[82] These conditions were:

> (a) there are no reasonable grounds for believing that a statement is inaccurate because of improper use of the computer; and
>
> (b) at all material times the computer was operating properly, or if not, that any respect in which it was not working properly or was out of operation was not such as to effect the production of the document or the accuracy of its contents; and
>
> (c) that any relevant conditions specified in rules of court are satisfied.[83]

2.34. In calling for the repeal, the Law Commission took into consideration the major criticisms of the operation of section 69 of PACE 1984. These criticisms were that:[84]

> (a) section 69 failed to address the major causes of inaccuracy in computer evidence,
>
> (b) advances in computer technology had made it increasingly difficult to prove satisfaction with the examination and certification conditions especially in relation to networked systems,
>
> (c) the recipient of computer output would be especially hard-pressed to prove compliance with the terms of section 69, and
>
> (d) it was anomalous that the computer could be used to provide the basis for an expert report, but not adduced in evidence itself.

---

81 *Ibid*, para 7.44.

82 Police and Criminal Evidence Act 1984, s 69 (since repealed).

83 S 69(1), PACE 1984.

84 UK Law Commission Report No 245, *supra,* note 71, paras 13.6-13.10.

2.35. Furthermore, the Law Commission also seemed to be influenced by its perception that in other jurisdictions such as in Scotland, some Australian states, New Zealand, the United States and Canada where "there were no special rules relating to computer output", there were no special problems as a result.[85] The Law Commission therefore, like their counterparts for the CEA 1995, recommended the repeal of section 69 without specific replacement. The Law Commission was also of the view that in criminal proceedings the common law presumption of the proper functioning of mechanical instruments may operate to cast the evidential burden of rebutting the presumption upon the opponent of the evidence.[86] In conformance with the above recommendations, the Youth Justice and Criminal Evidence Act 1999 has since repealed section 69 of PACE 1984.[87]

2.36. In view of the above changes, the broad statutory framework for the admissibility and assessment of computer records in the United Kingdom is now provided for civil proceedings by the provisions of CEA 1995 and in criminal proceedings by the provisions of Part II of CJA 1988. While some differences exist as to the scope of the admissibility provisions, there exist considerable similarities in the provisions relating to proof, cross-examination and weight of evidence for both civil and criminal proceedings.

2.37. As regards hearsay, while section 1 of CEA 1995 (subject to certain safeguards)[88] provides for the broad admissibility of both first-hand and multiple hearsay evidence, the

---

85 *Ibid,* para 13.12. The Law Commission's view of the approach in Canada has since been overtaken by the Uniform Electronic Evidence Act proposed by the Uniform Law Conference of Canada, the provisions of which have been accepted and incorporated into the Canada Evidence Act as well as the evidence statutes of many Canadian provinces. See Part II, *supra*, paras 2.1 - 2.15 of this Paper for a summary of the Canadian approach.

86 *Ibid,* paras 13.13 - 13.14.

87 Youth Justice and Criminal Evidence Act 1999, Schedule 6.

88 Ss 2-6, CEA 1995.

corresponding provisions under Part II of CJA 1988 only provide for the general admissibility of first hand documentary hearsay[89] and multiple hearsay contained in a business document.[90] Also, the admissibility of such documentary evidence in criminal proceedings is subject to close judicial scrutiny to exclude evidence generally in the interests of justice.[91]

2.38. As regards the proof of admitted documents, section 8 of CEA 1995 and section 27 of CJA 1988 are identical and provide a relatively easy mechanism for their admissibility. A proponent may do so by either the production of the document or by the production of a copy[92] of the document or a material part of the document.

> (1) Where a statement contained in a document is admissible as evidence in civil [or criminal] proceedings, it may be proved—
>
> (a) by the production of that document, or
>
> (b) whether or not that document is still in existence, by the production of a copy of that document or of the material part of it,
>
> authenticated in such manner as the court may approve.
>
> (2) It is immaterial for this purpose how many removes there are between a copy and the original.

2.39. The above provision to facilitate proof modifies the application of the best evidence rule as it allows for the production of a copy of the document as evidence and renders immaterial the number of removes between such a copy and the original.

2.40. In addition to section 8 of CEA 1995, a special provision for admissibility and proof of business documents is provided under section 9 of CEA 1995. As such

---

89 S 23, CJA 1988.

90 S 24, CJA 1988.

91 Ss 25-26, CJA 1988.

92 The term "copy", in relation to a document has been defined to mean "anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly".

documents are considered to be generally reliable the section provides that if a document forms part of the records of a business or public authority it may be received in evidence in civil proceedings without any need to adduce further proof,[93] and a certificate to that effect signed by the officer of the business or authority will be sufficient to authenticate it as such.[94] No such corresponding provision exists in the CJA 1988.

2.41. These provisions are supplemented by provisions of the Electronic Communications Act 2000 ('ECA 2000').[95] The ECA 2000 provides that an electronic signature[96] incorporated within a particular electronic communication or electronic data and the certification of such a signature by any person shall be admissible as evidence of the authenticity and integrity of the communication or data.[97] Certification of an electronic signature may be made by any person who can confirm that the signature, the means of making such a signature and the procedure applied to the signature provide a valid means of authenticating the electronic communication or data.[98]

2.42. As regards estimation of weight, both section 4 of CEA 1995 and Schedule II of CJA 1988 provide a broad discretion to the courts to estimate weight based on the circumstances surrounding the admitted evidence.[99]

---

93 S 9(1), CEA 1995.

94 S 9(2), CEA 1995.

95 Electronic Communications Act 2000 (2000 c 9).

96 S 7(1), ECA 2000 defines an electronic signature to mean "anything in electronic form, which is used to establish authenticity of an electronic communication or data".

97 S 7(1), ECA 2000.

98 S 7(3), ECA 2000.

99 However, while the provision in s 4 of the CEA 1995 stresses that such inference must be drawn on the "reliability" of the evidence, the corresponding provision in Schedule II of the CJA 1988 places emphasis of drawing inference upon the "accuracy" of the admitted evidence.

2.43. In summary, the approach taken in the United Kingdom with regard to both civil and criminal proceedings is not to have computer specific provisions for dealing with documents that contain computer-stored information. Instead such documents are treated on par with traditional physical documents and their admissibility is governed by the general rules of admissibility and proof applicable to documentary evidence. With the abolition of the hearsay rule in civil proceedings and its restricted application in criminal proceedings, documents are more readily admitted under the statutory exceptions but remain subject to scrutiny as to accuracy and reliability. Once such a document is admitted, the statutory provisions allow for the production of either the document or a copy of the document as proof.

Australia

2.44. In Australia, all jurisdictions have enacted laws that have application to the admissibility of computer evidence. These laws while exhibiting a certain degree of uniformity remain largely varied in their approach and application. In South Australia, Queensland and Victoria, explicit statutory provisions have been enacted to cater to the admissibility of computer output. On the other hand, Northern Territory and Western Australia have chosen not to have such explicit computer specific provisions but to admit documents produced by a computer under the statutory provisions governing the admissibility of business records and documents. A third approach is visible in the Commonwealth, New South Wales, Tasmania and the Australian Capital Territory. Under this approach, evidence derived from computers is admissible on the same basis as documentary evidence.

These are now described in turn.

South Australia

2.45. In the South Australia Evidence Act 1929 [100] ('SAEA 1929'), specific provisions[101] exist to cater to the admissibility of computer output. These provisions enacted as early as 1972[102] form Part 6A of the SAEA 1929 dealing with computer evidence. These provisions are applicable to both civil and criminal proceedings.[103]

2.46. Section 59B provides for the general admissibility of "computer output". The term "computer output" has been defined to mean "a statement or representation (whether in written, pictorial, graphical or other form) purporting to be a statement or representation of fact produced by a computer or accurately translated from a statement or representation so produced".[104] The term "computer" has also been statutorily defined to mean "a device that is by electronic, electro-mechanical, mechanical or other means capable of recording and processing data according to mathematical and logical rules and of reproducing that data or mathematical or logical consequences thereof".[105]

2.47. Under the SAEA 1929, computer output is admissible as evidence upon the satisfaction of seven conditions. These conditions specified in section 59B(2) require the proponent to satisfy the court that:

> (a) the computer is correctly programmed and regularly used to produce output of the same kind as that tendered; and
>
> (b) the data from which the output is produced is systematically prepared upon the basis of information that would normally be acceptable in a court of law as evidence of the representations made in it; and

---

100 South Australia Evidence Act 1929 (No 1907 of 1929).

101 Ss 59A – 59C, SAEA 1929.

102 South Australia Evidence Act Amendment Act 1972 (No 53 of 1972).

103 S 59B(1), SAEA 1929.

104 S 59A, SAEA 1929.

105 *Ibid.*

> (c) there is no reasonable cause to suspect any departure from the system or any error in the preparation of the data; and
>
> (d) the computer has not been subject to a malfunction after the data was introduced which might reasonably be expected to affect the accuracy of the output; and
>
> (e) there may have been no alterations to the mechanisms or processes of the computer during that period which might reasonably be expected to affect the accuracy of the output; and
>
> (f) records have been kept by a responsible person in charge of the computer of alterations to the mechanism and processes of the computer during that period; and
>
> (g) there is no reasonable cause to suspect that the accuracy or the validity of the output has been severely affected by the use of any improper process or procedure or by inadequate safeguards in the use of the computer.

2.48. While sections 59B(1) and (2) provide for the admissibility of computer output, they are designed to cater to the output of a single computer and do not specifically cater to networked computers. Section 59B(3) has therefore been designed to provide specifically for the admissibility of computer output in cases where two or more computers have been used either in combination or in succession for recording data or producing output. In such cases, the admissibility threshold prescribed in section 59B(3) is rather high as the court must be satisfied that the seven admissibility conditions are met in relation to each of these computers so far as relevant to the accuracy or validity of the output. The section further requires that the court must be satisfied that the use of more than one computer has not introduced any factor that might adversely affect the accuracy or validity of the output.[106]

2.49. Proof of satisfaction of the admissibility conditions provided under sections 59B(2) is provided by means of a certification mechanism. Section 59B(4) allows either a person having prescribed qualifications in computer system analysis and operation or a person responsible for the management or operation of the computer system to give a

---

[106] S 59B(3), SAEA 1929.

certificate with respect to all or any of the matters relating to the computer output admissibility conditions. This section provides that such a certificate shall be accepted as proof of those matters in the absence of contrary evidence.[107]

2.50. To counterbalance the ease of admissibility of computer output by production of a certificate, section 59B(6) gives a wide discretion to the courts to require oral evidence of any of the matters comprised in the certificate or to require the maker of such a certificate to be cross examined upon any of the matters so stated in the certificate.

2.51. Notwithstanding the wording of Part 6A of SAEA 1929, which suggests that any computer output whatsoever tendered in proceedings, is "subject to" its admissibility requirements,[108] through a process of judicial interpretation, it has been held by the South Australian courts that alternate modes of admission of computer output are permissible under other statutory provisions such as the banking records provisions under section 47 of Part 5 of the SAEA 1929 or at common law. In *Griffiths v ANZ Banking Group Ltd,*[109] it has been held that computerized banking records are admissible as evidence under section 47 of SAEA 1929 without any requirement to satisfy the admissibility conditions specified in section 59B. Furthermore, in *Mehesz v Redman (No 2)*,[110] it has been held that the provisions of section 59B were not intended to restrict the admissibility of computer output, which remains admissible under common law. This holding was followed in *R v Weatherall*,[111] where a computer printout of bankcards has been held to be admissible at common law, independently of section 59B.

---

107 S 59B(4), SAEA 1929.

108 S 59B(1), SAEA 1929.

109 (1990) 53 SASR 256.

110 (1980) 26 SASR 244.

111 (1981) 27 SASR 238.

2.52. No computer-specific provision exists in Part 6A of the SAEA 1929 to deal with the issue of weight of the tendered computer output. However, a generic provision to cater to the weight of tendered evidence is found in section 34D, which states that the court in estimating the weight of any statement must regard all circumstances from which inference can be drawn as to the accuracy or otherwise of the statement and in particular to the contemporaneity of the statement with the existence or occurrence of the facts stated, and the makers incentive to conceal or misrepresent facts.[112]

2.53. The application of the best evidence rule at common law has been modified by the statutory provision in section 45C, which provides for reproductions of the contents of a document to be admissible as evidence. Section 45C(3) specifically states that the provision applies to reproductions made by a process in which the contents of a document are recorded by electronic means and the reproduction is subsequently produced from that record.

2.54. In addition the provisions under Part 6A of SAEA 1929 are supplemented by the provisions of the South Australia Electronic Transactions Act 2000[113] which provide for the production of documents in electronic form and contains presumptions as to the reliability of documents in electronic form and for digital signatures.

2.55. In summary, the South Australian approach has been to formulate an explicit statutory framework for the admissibility of computer output. This framework consists of creating a high threshold limit for admissibility by requiring the proponent to satisfy seven conditions, providing an easy certification mechanism for proof and allowing courts to have a wide discretion as to estimation of weight of admitted evidence. However, despite the statutory framework built specifically for admissibility of

---

112 S 34D, SAEA 1929.

113 South Australia Electronic Transactions Act 2000 (No 72 of 2000).

computer output, it appears that such output can also be admitted under alternate modes of admissibility provided statutorily or under common law.

Queensland and Victoria

2.56. Similar to the South Australian approach, the Queensland Evidence Act 1977 ('QEA 1977')[114] and the Victoria Evidence Act ('VEA 1958')[115] contain provisions that explicitly provide for the "admissibility of statements produced by computers". These provisions are contained in section 55B of the VEA 1958[116] and section 95 of the QEA 1977. They are applicable to both civil and criminal proceedings.[117]

2.57. The general admissibility requirements for statements produced by computers provided by section 55B of the VEA 1958 and section 95 of the QEA 1977 are broadly similar. These provisions state that where direct oral evidence of a fact would be admissible, any statement contained in a document produced by a computer and tending to establish that fact is admissible subject to four conditions being met. These conditions are:

> (a) the document must be produced by the computer during a period in which the computer was being regularly used to store or process information for the purposes of any activities regularly carried on over that period,
>
> (b) during that period, information contained in the statement or so derived must have been regularly supplied to the computer in the ordinary course of those activities,
>
> (c) the computer must have been operating properly during the relevant period or , if not, any deficiency in operation must not have affected the production of the document or the accuracy of its contents, and
>
> (d) the information contained in the document must reproduce any information, or be derived from information, supplied to the

114 Queensland Evidence Act 1977 (No 47 of 1977).

115 Victoria Evidence Act 1958 (No 6246 of 1958).

116 Inserted by the Evidence (Documents) Act 1971 (No 8228 of 1971).

117 S 95(1), QEA 1977, s 55B(1), VEA 1958.

> computer in the ordinary course of the activities being regularly carried on.[118]

2.58. Where a combination of computers is being used to process information at the same time or in tandem, they may be treated as being a single computer.[119]

2.59. The term "computer" been defined in the VEA 1958 to mean "any device for storing or processing information, and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or any other process".[120] The same definition is to be found in the QEA 1977, which however defines a "computer" as any device for "storing *and* processing information".[121]

2.60. Proof of satisfaction of the admissibility preconditions may be provided by way of a certificate, which among other things must identify the document containing the statement and describe the manner of its production, giving particulars of any device involved in the production of the document.[122] This certificate must be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities and to the best of his knowledge and belief.[123]

2.61. As regards the manner of proof of such statements, both the Acts provide that the tendered evidence may be proven by the production of the document or a copy of that document or a material part thereof, authenticated in such manner as the court may approve.[124]

---

118 S 55B(2), VEA 1958, s 95(2), QEA 1977.

119 S 55B(3), VEA 1958, s 95(3), QEA 1977.

120 S 55B(8), VEA 1958.

121 S 95, QEA 1977.

122 S 55B(4), VEA 1958, s 95(4), QEA 1977.

123 *Ibid.*

124 S 55D, VEA 1958, s 97, QEA 1977.

2.62. Where such a copy is admissible in evidence, it shall be admissible to the same extent and for the like purpose as the original.[125]

2.63. Both the Acts provide a similar wide discretion to the courts for the purpose of deciding whether or not such a statement is admissible in evidence.[126] For the purposes of deciding whether to include or exclude such evidence, the court may draw any reasonable inference from the form or contents of the document in which the statement is contained, or from any other circumstance.[127] The court may also in its discretion reject any statement or representation notwithstanding that the requirements of admissibility have been met, if the admissibility of such a statement is inexpedient in the interests of justice.[128]

2.64. In addition the Electronic Transactions (Victoria) Act 2000 supplements the admissibility and proof provisions of the VEA 1958 by providing for the production of documents in electronic form and contains presumptions as to the reliability of documents in electronic form and for the reliability of digital signatures.[129]

2.65. In summary, the approach taken by Queensland and Victoria appears similar to the approach taken by South Australia, which is to provide for a statutory framework that explicitly caters to the admissibility of computer output. While the number of admissibility conditions is fewer under the Queensland and Victorian approach compared to the South Australian approach, they still pose a rather high threshold for admitting computer output. However this high threshold has been balanced by providing a simple mechanism for satisfying the admissi-

---

125 S 46, VEA 1958, s 116, QEA 1977.

126 S 55C, VEA 1958, s 96(1), QEA 1977.

127 *Ibid.*

128 S 55B(7), VEA 1958, s 98, QEA 1977.

129 Ss 9, 10, Electronic Transactions (Victoria) Act 2000 (No 20 of 2000).

bility preconditions and for proof by the production of document or its copy.

Northern Territory

2.66. In the Northern Territory of Australia, the Evidence (Business Records) Interim Arrangements Act ('EBRIAA')[130] provides for the admissibility of business documents. The EBRIAA does not contain any specific provision to cater exclusively to the admissibility of evidence obtained from a computer. Instead, it provides for the general admissibility of business documents[131] the scope of which includes such documents containing statements of information that have been stored or processed by a computer.[132] These provisions are applicable to both civil and criminal proceedings.[133]

2.67. Section 5 of the EBRIAA provides for the admissibility of documents containing a statement of a fact or opinion where the document forms part of a record made in the course of business. Such a statement may be: (i) made by a qualified person or (ii) reproduced or derived from information in statements each made by a qualified person, or reproduced or derived from information obtained from devices.[134] A "qualified person" in relation to a statement has been defined to mean a person who at the time of the making of the statement was associated with the business and has or is expected to have personal knowledge of the facts stated in such a statement.[135] The EBRIAA has also provided a statutory definition to the term "derived" to mean any information "derived, by the use of a computer or otherwise, by calculation, comparison, selection, sorting,

---

130 Northern Territory Evidence (Business Records) Interim Arrangements Act 1984, which was amended in 1990.

131 S 5, EBRIAA.

132 S 14, EBRIAA.

133 S 5(1), EBRIAA.

134 *Ibid.*

135 *Ibid.*

consolidation or by accounting, statistical or logical procedures".[136]

2.68. Furthermore, a statement given in conformance with the above conditions is considered to be admissible notwithstanding the rule against hearsay, the best evidence rule and the rule requiring the right of cross-examination of a person making the statement on a document.[137]

2.69. Proof of the contents of a document may be established by the production of a copy of the document or a material part of the document.[138] In particular, a record of information made by the use of a computer may be proven by the production of a document produced by the use of a computer containing the statement.[139]

2.70. A wide discretion is given to the court as regards the estimation of weight. Tendered evidence may be rejected on the grounds of being insignificant, of being likely to unduly prolong proceedings or of being unfair or misleading to either party.[140] However, in the estimation of weight, the court is mandated to regard all the circumstances from which an inference can reasonably be drawn as to the accuracy or otherwise of the statement.[141] The EBRIAA specifically prescribes that for statements reproduced or derived from devices, the court is required to take into account the reliability of such devices as well as the reliability of the means by which such information was reproduced or derived.[142]

2.71. In summary, the Northern Territory approach has been to expand the scope of provisions catering to the admissibility of business documents to include documents stored or

---

136 S 5(1), EBRIAA.

137 S 5(2), EBRIAA.

138 S 15, EBRIAA.

139 S 14(2)(c), EBRIAA.

140 S 6(2), EBRIAA.

141 S 9, EBRIAA.

142 S 9(b), (c), EBRIAA.

processed by computers. While this approach has negated the need to craft explicit computer-centric admissibility provisions, this approach is restrictive as it does not provide for the admissibility of non-business related documents.

Western Australia

2.72. The Western Australia Evidence Act 1906 ('WAEA 1906')[143] contains provisions similar to the Northern Territory EBRIAA approach. However, unlike the narrower Northern Territory approach that admits only evidence derived from computers as business records, the Western Australian approach is wider as it applies to all documents containing information obtained from computers. These provisions are applicable to both civil and criminal proceedings.[144]

2.73. The general admissibility provision in the WAEA 1906 relating to documents is similar to section 5 of the EBRIAA. Section 79C(1) of the WAEA 1906 provides that any document containing a statement of fact or opinion may on production of the document, be admissible as evidence of that fact or opinion. This is however subject to the condition that such statement was either made by a qualified person or that such statement was reproduced or derived from information in statements made by a qualified person or from information obtained from devices.[145] Under the WAEA 1906, a "qualified person" in relation to a statement means a person who had or might reasonably be supposed to have had personal knowledge of the matters.[146] The term "derived" is identical to the

143 Western Australia Evidence Act 1906.

144 S 79C(1), WAEA 1906.

145 *Ibid.*

146 *Ibid.*

EBRIAA definition.[147] Alternatively, where a document contains a statement reproduced or derived from a business record, it may also be admissible if the court is satisfied that the business record is genuine.[148]

2.74. Neither the rules against hearsay nor the rules against secondary evidence apply to statements admitted under the above provisions.[149]

2.75. A wide discretion is given to the court to ascertain the authenticity of the document. Tendered evidence may be rejected on the grounds of being insignificant, of being likely to unduly prolong proceedings or of being unfair or misleading to either party.[150]

2.76. In estimating the weight to be given to a statement tendered for admission the court is required to have regard for all the circumstances from which an inference can reasonably be drawn as to the accuracy or otherwise of the statement.[151] These circumstances include the contemporaneity of the statement, the motive behind the making of the statement, the accuracy of information and the reliability of the systems.[152]

2.77. In summary, the Western Territory approach is to permit a document containing statements information derived from a computer to be admissible on the same basis as other documentary evidence. This approach is characterized by its low admissibility threshold and easy authentication mechanisms. However while assessing the tendered evidence a number of factors have to be considered by the

---

147 The term derived is defined to mean any information "derived, by the use of a computer or otherwise, by calculation, comparison, selection, sorting, consolidation or by accounting, statistical or logical procedures".

148 S 79C(2a), WAEA 1906.

149 S 79C(3), WAEA 1906.

150 S 79C(6), WAEA 1906.

151 S 79D(1), WAEA 1906.

152 *Ibid.*

courts in order to determine accuracy of the statements contained in the document.

Commonwealth, Australian Capital Territory, New South Wales and Tasmania

2.78. In the Commonwealth Evidence Act 1995 ('CthEA 1995')[153] evidence derived from computers is admissible on the same basis as other documentary evidence. The same approach is adopted by the New South Wales Evidence Act 1995 ('NSW 1995')[154] and the Tasmania Evidence Act 2001 ('TEA 2001')[155] both of which contain identically numbered provisions to the CthEA 1995. This approach is also followed in the Australian Capital Territory as the CthEA 1995 provisions apply to proceedings in the Australian Capital Territory.[156] These provisions are applicable to both civil and criminal proceedings.

2.79. The CthEA 1995 makes no specific mention of the term "computer" but instead refers to "devices", a term left undefined. The Act however defines the term "document" to mean "any record of information and includes… anything from which sounds, images or writings can be reproduced with or without the aid of anything else…".[157] This definition is sufficiently wide enough to include any record of information that may be obtained from a computer. However, if a computer-stored document contains hearsay, it has to be admitted under a statutory exception to the hearsay rule such as the business records exception.[158] Thus, under the CthEA 1995, a document that is part of a business record may be admitted if the person supplying the information had personal knowledge

153 Commonwealth Evidence Act 1995 (No 2 of 1995).

154 New South Wales Evidence Act 1995 (No 25 of 1995).

155 Tasmania Evidence Act 2001.

156 S 4(1), CthEA 1995, s 4(1), NSW 1995, s 4(1), TEA 2001.

157 S 3, CthEA 1995, s 3, NSW 1995, s 3, TEA 2001.

158 S 59, CthEA 1995, s 59, NSW 1995, s 59, TEA 2001.

of such information.[159] However, the hearsay rule does not apply to information represented in electronic mail between computers concerning the identity of the sender and the receiver and the date and time of sending.[160]

2.80. As regards evidence produced by processes, machines and other devices the CthEA 1995 does not have provisions that afford special treatment for their admission. Instead, the CthEA has presumptions that facilitate their admission in evidence. Section 146 applies to a document or a thing produced wholly or partly by a device or process.

> **146. Evidence produced by processes, machines and other devices**
>
> (1) This section applies to a document or thing:
>
> (a) that is produced wholly or partly by a device or process; and
>
> (b) that is tendered by a party who asserts that, in producing the document or thing, the device or process has produced a particular outcome.
>
> (2) If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or thing on the occasion in question, the device or process produced that outcome.

2.81. Section 147 of the CthEA 1995, on the other hand, applies to documents that are produced by processes, machines and other devices in the course of business.

> **147. Documents produced by processes, machines and other devices in the course of business**
>
> (1) This section applies to a document:
>
> (a) that is produced wholly or partly by a device or process; and
>
> (b) that is tendered by a party who asserts that, in producing the document, the device or process has produced a particular outcome.

---

159 S 69(1), (2), CthEA 1995, s 69(1), (2), NSW 1995, s 69(1), (2), TEA 2001.

160 S 71, CthEA 1995, s 71, NSW 1995, s 71, TEA 2001.

> (2) If:
>
> (a) the document is, or was at the time it was produced, part of the records of, or kept for the purposes of, a business (whether or not the business is still in existence); and
>
> (b) the device or process is or was at that time used for the purposes of the business;
>
> it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document on the occasion in question, the device or process produced that outcome.

2.82. Both sections 146 and 147 raise a similar presumption that a device or process produces an expected outcome. The difference however lies in the preconditions to the presumption. Section 146 requires the proponent to satisfy the court of the accuracy in respect of devices and processes used before the court allows the presumption to operate. As the Australian Law Commission observed:[161]

> **Evidence produced by devices etc-**
>
> Where it is reasonably open to find that a device or process (for example, cheque sorting equipment) is of a kind that, properly used, does what is claimed for it (for example, on the basis of evidence of general reliability and trustworthiness), it should be presumed that the particular device did what the party claimed it did on the occasion in question. Such a presumption should operate both at the stage of admission of evidence and at the conclusion of proceedings.[162]

2.83. In contrast, section 147 provides that in cases where a document is produced by a device or process used for the purpose of a business, there is no requirement for the proponent to adduce proof of the accuracy of the device. As the Australian Law Commission's report states:

> **Business record.**
>
> In the case of documents reproducing or derived from information from a device, it should, prima facie, not be necessary to prove the working accuracy of the device if the court is satisfied,

---

161 Australian Law Reform Commission, *Evidence,* Report No 38 (1987).

162 *Ibid*, para 71, Summary of Recommendations.

> on the balance of probabilities, that the device is used for the purposes of a business.[163]

2.84. Proof of contents of documents may be provided in the manner specified by section 48 of the CthEA 1995. This may be done by tendering a document that is a copy of the document, which has been produced by a device that reproduces the contents of documents.[164] The application of the best evidence rule in common law has been reversed by a statutory provision in section 51, which states that the principles and rules of the common law that relate to the means of proving the contents of documents are abolished.

2.85. As regards weight, the courts have been given a general discretion to reject or limit the use of evidence if its probative value is substantially outweighed by the danger that the evidence might be unfairly prejudicial to a party, be misleading or confusing or cause or result in undue waste of time.[165]

2.86. Apart from the above provisions, the Commonwealth Electronic Transactions Act 1999[166] provides for the production of documents in electronic form and contains presumptions as to the reliability of documents in electronic form and for the reliability of digital signatures. Similar provisions exist in the New South Wales Electronic Transactions Act 2000[167] and the Tasmania Electronic Transactions Act 2000.[168]

2.87. In summary, the Commonwealth approach provides that a document containing hearsay evidence may be admitted under the business records exception. The Act remains technology-neutral by not referring to any specific devices

---

163 *Ibid.*

164 S 48(1)(b), CthEA 1995, s 48 (1)(b), NSW 1995, s 48(1)(b), TEA 2001.

165 Ss 135, 136, CthEA 1995, ss 135, 136, NSW 1995, ss 135, 136, TEA 2001.

166 Commonwealth Electronic Transactions Act 1999 (No 162 of 1999).

167 New South Wales Electronic Transactions Act 2000.

168 Tasmania Electronic Transactions Act 2000 (No 75 of 2000).

but allowing documents produced by processes, machine or other devices to be tendered in evidence. Furthermore the Act retains presumptions of reliability of devices to facilitate proof of evidence of documents produced by such devices.

South Africa

2.88. In 1983, South Africa enacted its Computer Evidence Act[169] ('SACEA 1983') as a separate statute to provide for the admissibility in civil proceedings of evidence generated by computers. The Act was amended in 1992 by the Computer Evidence Amendment Act, which introduced minor changes to the existing provisions.[170]

2.89. The term "computer print-out" has been statutorily defined to mean "the documentary form, in original or in duplicate, in which information is produced by a computer and includes any transcription, translation or interpretation used to convert the information produced by a computer into such documentary form".[171] The term "computer" has been defined to mean "any device or apparatus or a sequence or combination of such device or apparatus, which by various electronic, mechanical or other means, is capable of receiving data input, performing data processing and data storage functions and producing information by processing such data input".[172]

2.90. Section 3 provides that in any civil proceedings, a computer printout that is properly authenticated shall be admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible. To authenticate a computer printout five conditions must be satisfied. Section 2 requires the submission

169 Computer Evidence Act 1983.

170 Computer Evidence Amendment Act 1992.

171 Taken from definition of "computer print-out".

172 Taken from definition of "computer".

of an affidavit as satisfaction of the conditions. Such an affidavit should:

> (a) identify the computer print-out in question and confirm that it is a computer print-out as defined in this Act which has been produced by a computer as likewise defined;
>
> (b) identify such copy, reproduction, transcription, translation or interpretation of information produced by the computer as the computer print-out may comprise or contain, and confirm that it is a true copy, reproduction, transcription, translation or interpretation of such information;
>
> (c) describe in general terms the nature, extent and sources of the data and instructions supplied to the computer, and the purpose and effect of the processing of the data by the computer;
>
> (d) certify that the computer was-
>
> > (i) correctly and completely supplied with data and instructions appropriate to and sufficient for the purpose for which the information recorded in the computer print-out was produced;
> >
> > (ii) unaffected in its operation by any malfunction, interference, disturbance or interruption which might have had a bearing on such information or its reliability;
>
> (e) certify that no reason exists to doubt or suspect the truth or reliability of any information recorded in or result reflected by the computer print-out.

2.91. This affidavit can be given by any person who is qualified to give the testimony contained in it by reason of his knowledge and experience of computers and of the particular system by which the computer in question was operated at all relevant times, and his examination of all relevant records and facts which are to be had concerning the operation of the computer and the data and instructions supplied to it.[173]

2.92. Section 4 provides a wide discretion to the court to estimate the weight of the computer printout by permitting the court to take into account any matter contained in the

---

173 S 3(a), (b), SACEA 1983.

affidavit.[174] Also, on the application of any party to the proceedings, the court may require the deponent to the affidavit or any other person to testify orally on any relevant topic, whether covered by the affidavit or not.[175]

2.93. In March 2002 South Africa enacted the Electronic Communications and Transactions Act[176] ('SAECTA 2002') which came into force in August 2002. The SAECTA 2002 contains provisions that apply to the admissibility of documents containing electronic representations of information in any form. The SAECTA 2002 has repealed the SACEA 1983. The provisions of the SAECTA 2002, based on the UNCITRAL Model Law on E-commerce are applicable to both civil and criminal proceedings[177] and to any electronic transaction or data message[178].

2.94. Section 15(1)(a) of the ECTA 2002 provides that in any legal proceedings, the rules of evidence must not operate to deny the admissibility of data messages on the grounds that it is constituted as such a data message. Section 15(1)(b) provides that the best evidence rule which requires the tendering of original evidence must not operate to deny the admissibility of such a data message. In addition, section 14 provides that where information is required to be presented or retained in its original form, that requirement is met by a data message containing that information if there is integrity of information and that information is capable of being displayed or produced to the person to whom it is presented. Section 15(4) further provides that a data message, its copy or an extract thereof

---

174 S 4(2)(a), SACEA 1983.

175 S 4(2)(b), SACEA 1983.

176 South Africa Electronic Communications and Transactions Act 2002 (No 25 of 2002).

177 S 15(1), SAECTA 2002.

178 S 4(1), SAECTA 2002. The term "data message" is given legal recognition under the SAECTA 2002 and has been defined to mean "data generated, sent, received or stored by electronic means and includes - voice, where the voice is used in an automated transaction; and a stored record".

made by a person in the ordinary course of business is admissible in evidence on its mere production subject to its certification as being correct by an officer of that business.

2.95. As regards weight of the admitted data message, section 15(2) of the SAECTA 2002 states that information in the form of a data message must be given due evidential weightage. However, in assessing the weight of such data message, the court is mandated to regard:
(a) the reliability of the manner in which the data message was generated, stored or communicated,
(b) the reliability of the manner in which the integrity of the data message was maintained,
(c) the manner in which its originator was identified, and
(d) any other relevant factor.[179]

2.96. In summary, the South African approach is a unique attempt to provide for the admissibility of documents that exist in electronic form. The SAECTA 2002 approach is to use the term "data messages" to fix the scope of application of the Act. Data messages, which include electronic representations in any form, are admissible in the ordinary course of a business subject to certification. Where such data messages are to be presented in original form, they are admissible subject to adducing proof that their integrity is not altered. Broad discretion is given to the courts to assess the weight of admitted evidence while taking into account factors such as reliability and integrity of the data messages.

India

2.97. In the Indian Evidence Act 1872 ('IEA 1872'), specific provisions exist to cater to the admissibility of electronic records. These provisions which are applicable to both civil and criminal proceedings, were inserted by the Indian

[179] S 15(3), SAECTA 2002.

Information Technology Act ('IITA 2000')[180] in 2000 and were deemed necessary to facilitate *inter alia* the legal recognition for the use of electronic records in e-commerce transactions.[181]

2.98. The IEA 1872 now provides a comprehensive statutory framework for the admissibility of electronic records. This has been accomplished by expanding the scope of application of the provisions relating to documentary evidence to include such electronic records. The IEA 1872 defines the term "electronic record" as "data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche" but retains the existing definition of the term "document". However, the definition of the term "evidence" has been extended to include "electronic records".

2.99. The IITA has also introduced new definitions to technical terms such as "computer", "computer system", "data", "digital signature", "electronic form", "function" and "information".

---

[180] Indian Information Technology Act 2000 (No 21 of 2000). The IITA broadly follows the Model Law on E-commerce adopted by the United Nations Commission on International Trade Law.

[181] *Ibid.* The Second Schedule: Amendments to the Indian Evidence Act 1872. The IITA amendments substituted the term "electronic record" to the existing s 3 (Interpretation), s 17 (definition of admission), s 34 (entries in books of accounts), s 35 (entry in public record), s 39 (proof of statement), s 59 (proof of facts by oral evidence) and s 131 (production of documents) of the IEA 1872. Furthermore, the amendments also inserted new provisions relating to electronic records in s 22A (relevancy of oral admission as to contents of electronic records), s 47A (relevancy of opinion as to digital signature), s 65A (evidence relating to electronic record), s 65B (admissibility of electronic records), s 67A (proof as to digital signature), s 73A (proof as to verification of digital signature), s 81A (presumption as to gazette in electronic form), s 85A (presumption as to electronic agreements), s 85B (presumption as to electronic records and digital signatures), s 85C (presumption as to digital signature certificates), s 88A (presumption as to electronic messages), and s 90A (presumption as to electronic records five years old).

2.100. Pursuant to these amendments, section 65B of the IEA 1872 now governs the admissibility of electronic records.[182] Section 65B refers to "any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media produced by a computer" as a "computer output". Section 65B(1) provides that such computer output shall be admissible in any proceedings subject to four conditions. These conditions prescribed in section 65B(2) are that:

(a) the computer output containing the information was produced by a computer in the regular course of its operations and carried out by a person having lawful control over the use of that computer,
(b) the computer output containing the information was derived from data that was input in the normal course of its operation,
(c) the computer during the said period was operating properly and that the accuracy of the output was not affected by any interruptions in its normal operations, and
(d) the computer output was reproduced or derived from information fed into the computer in the normal course of its operations.

Section 65B(3) provides that where two or more computers are used in combination or in succession, they shall be treated as constituting a single computer and the conditions of admissibility under section 65B(2) shall apply accordingly.

2.101. Proof of the computer output can be satisfied by means of a certificate signed by a person occupying a responsible position in relation to the operation of the device or the management of the relevant activity, which states the following matters:[183]

---

182 S 65A, IEA 1872 states that contents of electronic records may be proved in accordance with provisions of s 65B, IEA 1872.

183 S 65B(4), IEA 1872.

(a) identify the electronic record containing the statement and describing the manner of its production.
(b) give particulars of any device involved in the production of that electronic record as may be appropriate to show that the electronic record was produced by a computer.
(c) deal with any matter related to the conditions imposed by section 65B(2).[184]

2.102. In recognition of the fact that digital signatures can authenticate electronic records in e-commerce and in e-filing transactions, the IITA 2000 has introduced new provisions in the IEA 1872 for proof of digital signatures.[185] Also, presumptions relating to electronic records, electronic agreements and electronic messages have been introduced.[186]

2.103. The application of the best evidence rule in relation to electronic records has been modified by the statutory provision in section 65B(1) which provides that computer output whether printed or copied shall be admissible without the need to adduce further proof by production of the original document if the conditions mentioned in the section 65B(2) are satisfied in relation to the information and computer in question.

2.104. In summary, the amendments to the IEA 1872 made by the IITA 2000 have provided a comprehensive statutory framework to cater to the admissibility of electronic records. Section 65B of the IEA 1872 now provides for the admissibility of electronic records subject to the satisfaction of certain conditions which are similar to the conditions for admissibility prescribed under the UK Civil Evidence Act 1968. Compliance with these conditions can be proved by means of a certification mechanism. To cater to the expanding use of e-commerce and e-filing

184 S 65B(4)(a), (b), (c), IEA 1872.

185 Ss 67A, 73A, IEA 1872.

186 Ss 85A, 85B, 88A, IEA 1872.

transactions, the UNCITRAL Model Law rules have been incorporated into the IEA 1872 to provide for the proof of digital signatures, electronic messages and electronic agreements. Furthermore the application of the best evidence rule has been modified in relation to the electronic records that are adduced under section 65B.

Malaysia

2.105 In 1993, the Malaysian Evidence (Amendment) Act,[187] introduced two new provisions (sections 90A and 90B) to the Malaysian Evidence Act ('MEA 1950')[188] to provide for the admissibility of documents produced by computers and to assess the weight to be attached to such documents. These provisions apply to both civil and criminal proceedings.

2.106 Section 90A provides for the admissibility of documents produced by computers or statements contained in such documents as evidence of any fact stated therein if they are produced by computers in the course of their ordinary use.[189] Section 3 of the MEA 1950 defines the term "computer" to mean "any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions, by whatever name or description such device is called; and where two or more computers carry out any one or more of those functions in combination or in succession or otherwise howsoever conjointly, they shall be treated as a single computer".

2.107 A statutory definition is also given to the term "document".

> "document" means any matter expressed, described, or howsoever represented, upon any substance, material, thing or

187 Malaysian Evidence (Amendment) Act 1993 (Act A851 of 1993).

188 Malaysian Evidence Act 1950 (Act 56 of 1950), Revised 1971.

189 S 90A(1), MEA 1950.

> 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;[190]

2.108 A proponent tendering such a document as evidence may by means of a certificate prove that the document was produced by a computer in the course of its ordinary use.[191] Such a certificate may be given by any person responsible for the management of the operation of the computer or for the conduct of the computer's activities, to the best of his knowledge and belief.[192] This certificate shall be admissible in evidence as *prima facie* proof of all matters stated therein and shall be deemed to satisfy the presumption that the computer referred to in the certificate was in good working order and was operating properly.[193]

2.109 Section 90A(5) provides that a document will be deemed to have been produced by a computer whether it was produced by it directly or by means of an appropriate equipment, and whether or not there was any direct or indirect human intervention.[194] In *PP v Datuk Hj Sahar*

---

190 S 3, MEA 1950. *Illustration* "A matter recorded, stored, processed, retrieved or produced by a computer is a document".

191 S 90A(2), MEA 1950

192 S 90A(2), (3)(a), MEA 1950.

193 S 90A(3)(b), (4), MEA 1950.

194 S 90A(5), MEA 1950.

Arpan,[195] it was held that bank computer printouts were not hearsay but nonetheless they had to satisfy the conditions of section 90A. It is submitted that the court would have arrived at the same conclusion if it had referred to section 90A(5) in its judgment.

2.110 In estimating the weight of a document or statement admitted by virtue of section 90A, the court may draw any reasonable inference from the circumstances relating to its creation, accuracy or otherwise. However, courts must have regard to 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. The courts also have to check whether any motive exists to conceal or misrepresent all or any of the facts stated in the document or statement.[196]

2.111 Apart from the provisions of the MEA 1950, the Malaysian Digital Signatures Act 1997 ('DSA 1997') contains provisions that provide for a document signed with a digital signature to be legally binding.[197] Furthermore the DSA provides for certain presumptions where a document in which a digital signature appears and where the signature is verified in accordance with the procedures set out in the Act.[198]

2.112 In summary, sections 90A and 90B of the MEA 1950 govern the admissibility and weight of documents produced by computer. Section 90A provides for the admissibility of documents produced by a computer in the course of its ordinary use. This may be proven by a proponent adducing a certificate to that effect, which can

---

195 [1999] 3 CLJ 427.

196 S 90B(b)(i), MEA 1950.

197 S 62(2), DSA 1997.

198 S 67, DSA 1997.

be signed by a person normally responsible for the management or operation of the computer. Section 90B provides courts with a wide discretion to estimate the weight to be attached to documents admitted pursuant to section 90A. The provisions of the MEA 1950 are supplemented by the Malaysian Digital Signatures Act 1997 which sets out presumptions relating to digital signatures incorporated into documents.

Part III. An Analysis of Singapore's Provisions

3.1. Having outlined the evidential provisions of Singapore and the other major jurisdictions that deal with computer-related output, printouts and records, this Part critically assesses the utility and effectiveness of our provisions. It concludes that sections 35 and 36 of our Evidence Act have to be revised and its evidential provisions streamlined to keep them current.

Objectives of Rules of Evidence

3.2. In a court of law, the court receives facts that either prove or disprove some fact in issue. Rules of evidence exist to guide the court in receiving or rejecting these facts – the evidence before the court – and thus facilitating the court in deciding on the facts in issue. And the court is principally guided by two broad principles in its treatment of rules of evidence: relevancy and admissibility.[1]

Relevancy

3.3. Relevancy as a legal construct is largely about the logical connection between the fact and the fact in issue where, in the ordinary course of experience, the existence of the fact will render more probable the existence of the fact in issue.[2] The same formulation is to be found in the Evidence Act 1995 (Commonwealth) of Australia:

> The evidence that is relevant in a proceeding is evidence that, if it were accepted, could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding.[3]

---

1 §§9-10, Wigmore, *Evidence in Trials at Common Law*, Volume I (Tillers Ed, 1983), at 655-674 ('Wigmore').

2 Howard, *et al, Phipson on Evidence*, (15th Ed, 2000), at 106 ('Phipson').

3 S 55(1), Evidence Act 1995 (Commonwealth) of Australia.

3.4. Our Evidence Act adopts in essence the same formulation in its definition of the term "relevant", except that the connection of one fact with another is "referred to in the provisions of [the Evidence Act] relating to the relevancy of facts".[4] These relevancy provisions are found in Part I of the Evidence Act, in particular, sections 5 to 16 of the Act.

Admissibility

3.5. While a fact may be relevant, yet evidence of it may, on grounds of policy, be rendered inadmissible. Admissibility is thus a legal construct that seeks to encapsulate issues of convenience and policy, to exclude evidence which is otherwise relevant and admissible.[5] The majority of rules of evidence are built around this principle, and are exclusionary in nature. As Wigmore puts it, "The true meaning is that everything having a probative value is *ipso facto* entitled to be assumed to be admissible and that therefore any rule of policy that may be valid to exclude it is a superadded and abnormal rule."[6]

3.6. These principles of evidence – relevancy and admissibility – remind us that the primary objective of rules of evidence is to include as evidence facts that are relevant. In both civil and criminal proceedings, if documents produced by computers or computer printouts are relevant, the rules of evidence should principally operate to admit them. Any rules of admissibility of computer evidence operating as exclusionary rules of evidence are exceptions to the principle of relevancy and "must show cause for

---

4 S 3(2), Evidence Act (Cap 97, 1997 Rev Ed) ('Evidence Act'). An argument may be made about the possible distinction between legal relevance and logical relevance, but, as the authors of Phipson noted, the concept of legal relevance confuses the exclusionary rules of evidence with the rules of relevance, since the former are not associated with relevance at all: Phipson, at 106.

5 Phipson, at 106. Tapper, *Cross and Tapper on Evidence* (9th Ed, 1999), at 56 ('Cross and Tapper').

6 §10, Wigmore, Volume I (Tillers Ed, 1983), at 672.

existence",[7] just like the other exclusionary rules of evidence.

3.7. So what are the justifications for these rules of admissibility? Cross and Tapper have highlighted four main classes of exclusionary rules of evidence: hearsay, opinion, character and conduct on other occasions.[8] The rule against hearsay operates to exclude statements, even if highly relevant, on account of their contents, because the circumstances in which they are made may vary greatly. Generally, this rule promotes the use of statements made by the attesting witness in court, because this guarantees the witness's availability for cross-examination.[9] Where out of court statements are admitted, they are admitted because they are made in such circumstances that promote their reliability. The rule against opinion discourages witnesses from informing the court of inferences drawn by them from facts perceived by them, unless they have special qualifications or expertise.[10] This rule preserves the sanctity of the judicial process, by arrogating for the court the primary responsibility for drawing inferences to resolve issues of fact.[11] The rule against character disallows, *inter alia*, the use of an accused person's reputation to draw the inference that he is guilty of the offence with which he is charged, except in limited circumstances, and for limited purposes.[12] Finally, the rule against admitting in evidence the misconduct of the accused on other occasions ensures

---

7 §10, Wigmore, Volume I (Tillers Ed, 1983), at 673.

8 Cross and Tapper, at 56. To this list may be added the rules requiring corroboration, rules against admitting privileged information, such as the privilege against self-incrimination, legal professional privilege and without-prejudice statements, and rules against admitting evidence for reasons of public policy, such as state privilege and improperly obtained evidence.

9 Cross and Tapper, at 532. It has been held that s 62, Evidence Act, encapsulates the oral evidence rule and provides the basis for the exclusionary rule against hearsay in Singapore. See *Soon Peck Wah v Woon Che Chye* [1998] 1 SLR 234 (Singapore Court of Appeal).

10 See ss 47-53, Evidence Act.

11 Cross and Tapper, at 511.

12 Cross and Tapper, at 323. The position in Singapore is set out in ss 56 and 134, Evidence Act.

that generally, only his conduct for the offence in question is placed under judicial inquiry.[13]

Probative Policy and Extrinsic Policy

3.8. The justifications offered by these classes of exclusionary rules can in turn be divided into two sets. The hearsay rule and the opinion rule (as are rules of corroboration) are examples of rules dealing with probative policy.[14] These rules lay down auxiliary tests and safeguards that require particular kinds of facts to exceed the required minimum probative value – to ensure the further reliability of the evidence.[15] These are rules that are designed to avoid special dangers with these types of evidence irrespective of the nature of the inference and effect.[16]

3.9. The rule against character and previous misconduct (as are rules dealing with privileged information) are examples of rules that exclude evidence on the basis of extrinsic policies – because the admission of such evidence will injure some other cause more than it would help the cause of truth.[17] Thus such evidence is excluded to avoid the collateral disadvantages associated with otherwise admitting such evidence.[18] These collateral disadvantages may be described as policies such as the preservation of legal

---

13 Adapted from Cross and Tapper, at 57. See also Cross and Tapper, at 334. The position in Singapore is set out in ss 11, 14 and 15, Evidence Act. See *Tan Meng Jee v PP* [1996] 2 SLR 422 (Singapore Court of Appeal) and *Lee Kwang Peng v PP* [1997] 3 SLR 278 (Singapore High Court).

14 §12, Wigmore, Volume I (Tillers Ed, 1983), at 689.

15 §1172, Wigmore, Volume IV (Chadbourn Ed, 1972), at 396.

16 *Ibid.* Wigmore further refines this classification into five other categories of rules: rules that prefer one kind of evidence to another, or scrutinise the evidence to expose its possible weakness and to make clear the precise value that it deserves, or remove sources of danger and distrust of such evidence, or reject evidence that confuses the process of proof under certain conditions, or require other types of evidence to be associated with it before it can be admitted. See §1173, Wigmore, Volume IV, (Chadbourn Ed, 1972), at 398.

17 *Ibid.*

18 §1172, Wigmore, Volume IV, (Chadbourn Ed, 1972), at 396.

professional privilege and the prejudice to the accused of evidence of his previous misconduct.

3.10. Of course, exceptions exist for these exclusionary rules. For instance, hearsay evidence may be admitted where it is in the form of reliable business records,[19] opinion evidence may be admitted where it falls within the witness's special area of expertise,[20] character evidence may be admitted for the purpose of impugning the credibility of the accused as a witness,[21] and his previous misconduct may be admitted where its probative value is so strong as to outweigh any prejudicial effect such evidence may have on the trier of fact.[22]

Application to Electronic Evidence

Principle of Equivalence

3.11. What principle or principles should govern the admissibility of computer-related or electronic evidence? The starting point is arguably the principle of non-discrimination against electronic records (or the principle of equivalence of electronic records), as stated in section 6 of the Electronic Transactions Act ('ETA'):

> **Legal recognition of electronic records**
>
> 6. For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability *solely* on the ground that it is in the form of an electronic record.[23] [our emphasis]

3.12. This principle is identical to Article 5 of the UNCITRAL Model Law on Electronic Commerce ('Model Law'), from which section 6, ETA is derived. The following useful instruction and guidance on this principle can be found in the UNCITRAL Commentaries to the Model Law:

---

19 S 32(b), Evidence Act.

20 *Supra*, note 10.

21 *Supra*, note 12.

22 *Supra*, note 13.

23 S 6, Electronic Transactions Act (Cap 88, 1999 Rev Ed).

> Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. It is intended to apply notwithstanding any statutory requirements for a "writing" or an original. That fundamental principle is intended to find general application and its scope should not be limited to evidence or other matters covered in chapter II… *By stating that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message", article 5 merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability.* However, article 5 should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein.[24] [our emphasis]

3.13. A terser but equally assertive statement can be found in the commentaries by the National Conference of Commissioners on Uniform State Laws ('NCCUSL') on the US Uniform Electronic Transactions Act 1999:

> This section sets forth the fundamental premise of this Act: namely, that *the medium in which a record, signature, or contract is created, presented or retained does not affect it's* [sic] *legal significance*. Subsections (a) and (b) are designed to eliminate the single element of medium as a reason to deny effect or enforceability to a record, signature, or contract. The fact that the information is set forth in an electronic, as opposed to paper record is irrelevant. [25] [our emphasis]

Universality of the Principle of Equivalence

3.14. The universality of the principle of equivalence is undoubted: it can be found in electronic commerce and electronic transaction legislations enacted worldwide. [26]

---

[24] Para 46, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996.

[25] Commentaries on s 7, US Uniform Electronic Transactions Act 1999, at http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (visited 29 March 2001).

[26] See, *e.g.*, s 7(a), US Uniform Electronic Transactions Act 1999, s 101, US E-Signatures in Global and National Commerce Act 2000, s 107, NCCUSL proposed US Uniform Computer Information Transactions Act 2000 and Article 9, EU Directive on Electronic Commerce 2000 (Directive 2000/31/EC dated 8 June 2000).

This principle establishes a very important point self-evident in today's highly computerised business environment. Much vital information – ranging from business transactions to inventories to financial records to personal data – is captured and stored exclusively in the form of electronic records. And when such information is to be presented in physical form, the necessary printouts – paper documents – are produced for the first time. Similarly, many corporations are digitizing their paper documents – and converting and storing them in digital form. The electronic record and the paper document are used very much interchangeably and in a non-discriminatory fashion in both the private as well as the public sector. The principle of non-discrimination against electronic records is as much a reminder about the equivalence of electronic records with paper-based records in today's commercial realities, as it is an injunction not to discriminate against electronic records.

3.15. But the principle of equivalence of electronic records does not presume that the electronic record will be the same as the physical record *for all purposes*. The principle states that "information shall not be denied legal effect, validity or enforceability *solely* on the ground that it is in the form of an electronic record."[27] This implies that in suitable circumstances and for valid reasons, other than for the only reason that it is in electronic form, it is permissible to deny electronic records legal effect, validity and enforceability. Thus both the principle of equivalence and the principles governing the exclusionary rules of admissibility of evidence call for a policy reason or justification for a rule of evidence that only deals with the admissibility of electronic records.

3.16. Where reasons of probative policy or auxiliary policy as explained above call for the exclusion of electronic evidence, these rules of evidence could not be said to have operated to exclude electronic evidence "solely" because of the medium on which such evidence is tendered. To

---

27 S 6, Electronic Transactions Act, *supra*, note 23.

illustrate, an electronic record that is hearsay will be inadmissible in evidence through the operation of reasons of probative policy (the hearsay rule) unless an exception can be found for admitting such records (*e.g.* the business records exception). Similarly, electronic records of discussions between solicitor and client are inadmissible in evidence through the operation of reasons of auxiliary policy (the rule protecting the privileged communications between solicitor and client).

3.17. Hence if there is a rule of admissibility providing for the separate admission in evidence of electronic records, it will necessarily be subject to close scrutiny. Conversely, if the rule of admissibility providing for the admissibility of electronic evidence is actually the application of a rule of probative or auxiliary policy, the equivalence principle is not infringed. It is on this basis that we will analyse Singapore's existing computer output provisions in sections 35 and 36 of the Evidence Act that deal with the admissibility of electronic records.

Sections 35 and 36 and the Equivalence Principle

3.18. Are sections 35 and 36 of the Evidence Act consistent with the equivalence principle?

3.19. The Explanatory Statement to the Evidence (Amendment) Bill 1995 explains that amendments to the predecessors to our existing sections 35 and 36 were made "principally to facilitate the use of information technology and the admissibility as evidence of information stored or produced by the use of such technology."[28] The Explanatory Statement further explains why the predecessor provisions were amended:

> Sections 35 and 36 have become dated because of the rapid advances in technology over the last 20 years. The new provisions are intended to cover not only the traditional computer print-out but also computer output whether in audio, visual, graphical,

[28] Explanatory Statement to the Evidence (Amendment) Bill 1995 ('Explanatory Statement').

> multi-media, printed, pictorial or any other form. The provisions are also not limited to traditional main-frame computers but are wide enough to cover stand-alone personal or portable computers, local area or wide area networks, bulletin board services and even a global network of networks such as Internet. The provisions are also not limited to civil proceedings or business records. No distinction is made between the public and private sectors. They will also enable law enforcement officers to produce evidence of computer output seized or obtained by them.[29]

3.20. The Explanatory Statement makes it clear that the 1996 amendments[30] to sections 35 and 36 were intended to apply to *all* forms of electronic output. The language of section 35(1) reinforces this by stating that "where computer output is *tendered in evidence for any purpose whatsoever*, such output shall be admissible if it is relevant or otherwise admissible according to the other provisions of this Act or any other written law, and it is [admissible pursuant to one of the three modes of admissibility]." So not only do the provisions apply to "computer output", which, as explained in Part I of this Paper, is very expansively defined, they apply to all such computer output "tendered in evidence for any purpose whatsoever."[31] This is an important point to make, because the existing sections 35 and 36 reversed the position taken under the old sections 35 and 36, where a legal distinction was made between computer output as real evidence and as documents. Where computer output is real evidence, the old section 35 would not apply to such evidence.[32] It will only apply if the output is a document.[33]

3.21. So far from narrowing the rule of admissibility of computer evidence in section 35, the 1996 amendments *broadened* the scope of the application of the rule of admissibility. Where computer output as real evidence was

---

29 *Ibid.*

30 Amendments made pursuant to the Evidence (Amendment) Act 1996, whose effective date of commencement is 8 March 1996.

31 See Seng, D, "Computer Output as Evidence" [1997] SJLS 130 at 141. This approach was adopted in *Lim Mong Hong v PP* [2003] 3 SLR 88.

32 *PP v Ang Soon Huat* [1991] 1 MLJ 1 (Singapore High Court).

33 *Aw Kew Lim & Ors v PP* [1987] 2 MLJ 601 (Singapore High Court).

previously admissible as long as it was relevant, under the new section 35, it is only admissible if it is *both relevant and* falls within one of the three modes of admissibility.[34] If such evidence fails to meet one of the modes of admissibility, the language of section 35(1) is unequivocal - it *shall* not be admissible.[35]

3.22. Thus, far from facilitating the use of information technology and the admissibility in electronic evidence, it may be argued that the provisions actually make it much more difficult to admit electronic evidence. Although section 35(1) has made a provision for its admissibility rules to be overridden by written law, only a few pieces of legislation such as the Land Titles Act, the Companies Act and the Business Registration Act contain such overriding provisions.[36]

3.23. By requiring all electronic evidence to be admitted because parties have reached an express written agreement to admit such evidence,[37] or because such evidence was produced pursuant to an approved process,[38] or because the party tendering the evidence has secured proof as to the accuracy of the output and proper operation of the computer that produced the evidence,[39] *but not requiring the same of non-electronic evidence*, it is submitted that the equivalence principle has not been observed. Of course, it should be pointed out that the enactment of section 35 precedes the equivalence principle as set out in s 6, ETA. But if the issue is one of compliance with the equivalence principle, it is submitted that our evidence rules dealing

---

34 *Supra*, note 31.

35 *Ibid*, at 142-143. Cf: *Industrial & Commercial Bank Ltd v Banco Ambrosiano Veneto Spa* [2003] 1 SLR 221, 225. But this is not the view expressed by the Singapore High Court in *Lim Mong Hong v PP, supra,* note 31.

36 These provisions are set out in Appendix II of this Paper.

37 S 35(1)(a), Evidence Act.

38 S 35(1)(b), Evidence Act.

39 S 35(1)(c), Evidence Act.

with the admissibility of electronic evidence are in non-compliance with the spirit of the equivalence principle.

Q. Does section 35 subject electronic evidence to a higher standard of admissibility than other forms of evidence, contrary to the equivalence principle?

Assessing the Three Modes of Admissibility

3.24. The difficulty of admitting electronic evidence may be supported by an examination of the three modes of admissibility prescribed under section 35. Of the three modes of admissibility, the first mode – "express agreement" – is the most cost-effective. But it presupposes that parties had applied their minds to this problem of the legal admissibility of their electronic records. Since such an agreement may be made "at any time", in commercial matters, the most apt juncture for parties to agree to the admissibility of electronic records is when they reach a consensus about their business obligations and commercial terms. Where the differences between the parties are so great as to give rise to the commencement of civil proceedings, it could hardly be expected for the party against whom the electronic evidence is to be adduced to consent to its admissibility pursuant to section 35(1)(a).

3.25. The problem is even more acute in relation to criminal proceedings. Since the prosecution will seek to adduce evidence against the accused in such proceedings, it would hardly behove the accused to consent to its admissibility. In fact, such consent by the accused calls into question the very veracity of the agreement, which is why section 35(2)(a) requires such an agreement to be reached between the prosecution and a legally-represented accused.

3.26. The second mode – "approved process" – is really only feasible for large corporations and organisations like IRAS. To date, the only process that has been approved by the Minister pursuant to section 35(5) has been document imaging systems that are operated, maintained and audited pursuant to the Evidence (Computer Output) Regulations

1996.[40] A lot of background work goes into securing the two certificates required to support the admission of the evidence – the first certifying that the document imaging process operated by the company or organisation is an approved process[41] and the second certifying that the computer output is obtained from such an approved process[42]. Before the certificate can be issued, there must be an initial certification by a certifying authority that the document imaging system – hardware, software and system – complies with the detailed compliance criteria in the First Schedule of the Evidence (Computer Output) Regulations 1996,[43] followed by a periodic certification – yearly for the first 3 years, and thereafter once every 2 years – that the system remains in compliance.[44] Thus corporations and organisations will only see this option as a cost-effective option if they deal with large quantities of third party physical records that are critical to their businesses and operations and can afford the comprehensive[45] and relatively costly auditing processes to verify that (i) their document imaging systems can provide an accurate representation of the contents of a document, (ii) that the integrity of physical processes surrounding the capture, committal and output of images is properly maintained and (iii) that the integrity of the image systems surrounding the capture, committal and output of images is also properly maintained.[46]

3.27. The third and final mode of admissibility – "proof of proper operation and accuracy" – is the fall-back for the proponent of the electronic evidence who fails to secure its admission under the first two modes. Section 35 provides that such mode of proof may be met by a certificate

---

40 *Supra*, Part I, note 15.

41 S 35(3), Evidence Act.

42 S 35(4), Evidence Act.

43 Regulation 10, Evidence Regulations 1996.

44 Regulation 12, Evidence Regulations 1996.

45 Paragraph 12, First Schedule, Evidence Regulations 1996.

46 Paragraph 3, First Schedule, Evidence Regulations 1996.

containing the appropriate legal declarations. In its current form, it has a rather complicated requirement of requiring the proponent to prove (i) two negative conditions that "there is no reasonable ground for believing that the output is inaccurate because of the improper use of the computer, and that no reason exists to doubt or suspect the truth or reliability of the output" (the "not unreliable output" condition)[47] and (ii) a positive condition that "there is reasonable ground to believe that at all material times the computer was operating properly" (the "proper operation of computer" condition).[48] It is arguably not easy to apply.[49] It is often difficult to identify and find the right persons to make the prescribed legal declarations:[50] the certifier is usually, but not necessarily, the systems operator or information systems manager.[51] He may be the expert who has gained access to the system,[52] and may arguably even be the appropriate manager or officer with some level of supervisory or managerial control over the data operator.[53] The prescribed statutory requirement for the right person to make the prescribed legal declarations as a pre-condition for the admissibility of electronic evidence has given rise to much litigation concerning the qualifications required of this certifier.[54]

3.28. Furthermore, pursuant to the proof by certification route of section 35(6), the identified certifier has to make certain prescribed representations about the output pertaining to its identity, description of the manner in which it was produced,[55]

---

47 S 35(1)(c)(i).

48 S 35(1)(c)(ii).

49 See *Lim Mong Hong v PP*, *supra,* note 31 at para 42 where Yong Pung How CJ observed that proof of a negative is generally more difficult than proof of a positive.

50 *Supra*, note 31, at 153-155.

51 Explanatory Statement, *supra*, note 28.

52 Section 35(8), Evidence Act. See also Explanatory Statement, *supra,* note 28.

53 *Supra*, note 31, at 153.

54 See *e.g. R v Shepherd* [1993] AC 380 (House of Lords).

55 S 35(6)(a), Evidence Act.

particulars of the processing and storage devices[56] and provide an attestation from his personal knowledge as to the absence of reasonable ground for believing the output to be inaccurate, untrue or unreliable,[57] and his belief that the computer was operating properly at all material times, or if it was not so operating, that the accuracy of the output would not be affected.[58] In fact, the Evidence Act recognises how onerous this can be and only requires the certifier to make his certification "to the best of [his] knowledge and belief".[59] Nonetheless, this cannot be an empty or poorly substantiated knowledge or belief because his knowledge or belief may be challenged,[60] and a false certification carries penal sanctions.[61] The fact that few, if any, certifiers will have actual knowledge, that most will necessarily draw inferences from their managerial or operational experience to make the certifications and that each item of electronic evidence must be supported by a separate certificate to this effect escalates the burden placed on the proponent seeking to admit electronic evidence. And the true value of the certifier's certification is called into question by the sheer complexity of the modern computing environment. For instance, pursuant to section 36(5)(b), doubts may be raised about whether the certifier is holding a "responsible position" that permits him to exercise effective control over the computer and its electronic evidence to support the admissibility of such evidence and for him to make an honest certification.

3.29. These conclusions are consistent with the anecdotal evidence from legal practitioners, company officers, auditors and other professionals who have expressed their concerns that the recording and storage of business records in electronic form may expose such records to the

---

56 S 35(6)(b), Evidence Act.

57 S 35(6)(c), read with s 35(1)(c)(i), Evidence Act.

58 S 35(6)(c), read with s 35(1)(c)(ii), Evidence Act.

59 S 35(9), Evidence Act.

60 S 36(3), Evidence Act.

61 S 35(11), Evidence Act.

risks of legal inadmissibility. In practice, the problem is managed in both civil and criminal proceedings not by way of the parties expressly agreeing to admit such evidence, but by disregarding or ignoring the substantive rule in section 35.[62]

Q. Do the admissibility standards set by section 35 interfere with or limit the admissibility of electronic evidence?

Changes to Computing Paradigms: The Prevalence of Computing Devices

3.30. But it is no real surprise that sections 35 and 36 of the Evidence Act are not consistent with the equivalence principle. The amendments made to the old sections 35 and 36 were first proposed in 1995[63] and effected in 1996.[64] It was after its enactment that the equivalence principle rose in ascendancy. In 1995, we witnessed the commercialisation of the Internet, the start of the electronic commerce boom and the mobile handset boom. In 1999, palmtops and personal digital assistants fell in price and became affordable for the average consumer. Between 1999 and 2001, Internet usage boomed, telephone companies merged and fell into bankruptcy, and peer-to-peer ('P2P') software such as Napster rode the growth of the Internet and died, only to be replaced by other software such as Kazaa and Grokster. These were epochal changes from a computing perspective as well as from an evidential perspective. It is submitted that these changes have made a review of sections 35 and 36 both urgent and necessary.

3.31. That these changes are necessary may be perceived from a close review of two definitions introduced pursuant to the

---

62 See Appendix IV for a list of Singapore cases that have taken this approach.

63 Explanatory Statement, Evidence (Amendment) Bill. While the Explanatory Statement expressly acknowledges the advent of the Internet, the sheer scale and breadth of changes it has brought about have caught many by surprise.

64 Pursuant to the Evidence (Amendment) Act 1996 (No 8 of 1996).

Evidence Act amendments in 1995 and their originating legislation. As explained in Part I of this Paper, the term "computer output" receives a very general and broad definition pursuant to the amendments. In effect, any statement or representation in any form that is produced by a computer[65] will be "computer output".

3.32. As explained in Part I of this paper, the definition of a computer encompasses data processing devices, data storage devices, communications devices and groups or interconnections of such devices. This definition is identical to, and is taken from the same definition of a "computer" in the Computer Misuse Act 1993.[66] This definition is in turn adapted from the following definition, taken from the South Australian Evidence Act 1929, which was amended in 1972:

> "computer" means a device that is by electronic, electro-mechanical, mechanical or other means capable of recording and processing data according to mathematical and logical rules and of reproducing that data or mathematical or logical consequences thereof;[67]

3.33. If this is the origin of our definition of a "computer", it betrays its age as well as the approach towards the admissibility of electronic evidence. This definition of a computer reflects the 1970's and early 1980's era of mainframes and minicomputers where computers were huge machines used in government departments, scientific laboratories and large business organisations for specialised functions that essentially involved dedicated data operators feeding carefully controlled data into these computers. The data would then be processed in carefully controlled computing environments and then reproduced in the form

---

65 See definition of "computer output" in s 3(1), Evidence Act.

66 Cap 50A, 1998 Rev Ed. The mystery of the common origin of the definition of "computer" and "computer output" is solved if it is observed that the Computer Misuse Act 1993 (No 19 of 1993) (Cap 50A, 1994 Rev Ed) was promulgated with admissibility provisions for the reception of computer output in evidence in ss 11-13. These were subsequently superseded by the 1996 amendments to the Evidence Act.

67 S 59A, Part 6A, South Australia Evidence Act 1929, as amended in 1972.

of printouts or on magnetic tape. To describe electronic evidence as "computer output" also confirms its mainframe legacy.

3.34. To the credit of the Parliamentary draftsmen, this clearly outdated definition was given a facelift in the Computer Misuse Act 1993. By adding references to "a group of such interconnected [data processing] devices", "performing [and including] data storage functions" and "operating … communications facilities", the lifespan of the 1993 definition of a "computer" was significantly improved.[68] However forwarding-looking these changes may have been in 1993, unfortunately, technological innovation has outstripped these adaptations.

3.35. Firstly, this definition has a very wide reach when one takes into account the advent of the microprocessor. If a device that has a microprocessor is considered a computer, a lot of modern day electrical devices and appliances are "computers" because they operate through embedded microcontrollers that are sophisticated data processing devices that are programmed to process input from a variety of sources and generate output in a variety of ways. A lay person would clearly associate mainframe, workstations, personal computers and personal digital assistants as computers. Furthermore, computing functionality is increasingly being built into tools and devices such as mobile phones and digital watches. But to the engineer, the building blocks are the same – microprocessors.

3.36. Whether we are at home, at work or at play, we are surrounded by computers. Modern day home appliances such as air conditioners, refrigerators and microwave ovens make extensive use of microcontrollers to more efficiently regulate temperature, conditions, usage and electrical consumption. In our offices, digital photocopiers, telephone systems, scanners, facsimile machines, printers and other multi-function machines are computers. In fact, IS departments are starting to manage copiers as computers, because it has been found that copiers are as vulnerable to

---

[68] S 2(1), Computer Misuse Act (Cap 50A, 1994 Rev Ed).

security issues as computers. Cars that are on our roads have "computers" built into them. For our entertainment, we depend on microcontroller driven devices such as TVs, VCRs and CD, VCD, DVD and MP3 players. Even toys are increasingly being made with "computers" in them for that additional element of interaction and realism. Given the use of microprocessors in such devices, it is not possible to exclude such devices as "non-programmable" devices from the ambit of the breadth of the definition of a "computer" under the Evidence Act.

3.37. Secondly, the definitions, the modes of admissibility and the certification mechanisms prescribed in section 35 presuppose some centralisation of control and management with a centralisation node for processing and storing of information. For instance, section 35 refers to the need for certification "by a person holding a responsible position in relation to the operation or management" of the computer system.[69] The definition already acknowledges the use of networked computers. But unlike the typical client-server network model, where control resides with the systems administrator of the server, some modern networks such as P2P networks lack a centralised person who has this exclusive operational or managerial control of the network. Business models such as application service providers ('ASPs') and web services use a division of responsibility model where the service provider manages the computer and communications systems and some aspects of the software and electronic business operations, but the rest of the responsibility is divided between the client and the software and hardware vendors or even with other service providers. In such computing and business models, it will be hard to identify the party or organisation responsible for the reliability of the electronic evidence, let alone secure the involvement of this party or organisation in the certification process.

---

[69] See, *e.g.*, ss 35(3), (4) and (7), Evidence Act.

3.38. In addition, references to "a person holding a responsible position in relation to the operation or management of the relevant computer system"[70] who has to identify such output, describe the manner in which it was produced and give particulars of any device involved in the processing and storage of such output[71] speak indirectly of a closed network environment. They do not sit well with modern conceptions of a distributed companies open network environment with open source involving distributed responsibilities for hardware, software and data.

Technology Neutrality and Other Rules of Evidence

3.39. With such a broad spectrum of devices falling under the rubric of "computers", any "audio, visual, graphical, multimedia, printed, pictorial, written"[72] statement or representation from such devices will be "computer output". This brings an enormous category of evidence under the framework of section 35 of the Evidence Act. The current legal scheme thus extends its reach beyond statements or representations in electronic form: practically any useful evidence in the form of a statement or representation derived from electronic devices will be subjected to the requirement of one of three modes of admissibility. This analysis, if correct, suggests that not only does section 35 discriminate against electronic records but it also has the effect of discriminating against any relevant statement or representation emanating from electronic devices!

3.40. This discrimination against electronic evidence and electronic devices in general is surely not an intended consequence of the Evidence (Amendment) Act 1996. To recap, the amendments made to the old sections 35 and 36 were intended to facilitate, and not hinder, "the use of information technology and admissibility as evidence of information stored or produced by the use of such

---

70 An expression that is the cornerstone of s 35. See ss 35(3), (4), (6) and (7), Evidence Act.

71 S 35(6), Evidence Act.

72 Definition of "computer output", s 3(1), Evidence Act.

technology."[73] But is there any reason – either by way of probative policy or auxiliary policy – for discriminating against electronic evidence?

3.41. An examination of common law rules and other evidential provisions in the Evidence Act and in the Criminal Procedure Code suggests the opposite conclusion. At common law, in the case of *Derby v Weldon (No 9)*,[74] it was held that a computer file is a document and is admissible. Similarly, the UK and US courts have not found any objections against admitting records on the magnetic medium (such as tape recordings),[75] photographic medium (such as microfilm and microdots)[76] or as television films/ cinematographic films, [77] videotapes, [78] and facsimile transmissions[79]. Nor have the courts shirked from concluding that computer printouts of computerised chemical analysis machines, [80] printouts from Intoximeters for measuring breath alcohol levels [81] and printouts from

---

73 Explanatory Statement, *supra*, note 28.

74 [1991] 1 WLR 652. Such a file remains a document even though it has been electronically deleted but could be recovered. See also *R v Halpin* [1975] 1 QB 907, [1975] 2 All ER 1124. *Cf. R v Plymouth City Council and Plymouth Magistrates' Court, ex parte Johns* (27 October 1994, unreported), *Prism Hospital Software Ltd v Hospital Medical Research Institute* [1992] 2 WWR 157.

75 *R v Stevenson* [1971] 1 All ER 678, [1971] 1 WLR 1, *R v Robson* [1972] 1 WLR 651, *Grant v Southwestern and County Properties Ltd* [1975] Ch 185.

76 *Barker v Wilson* [1980] 2 All ER 81, [1980] 1 WLR 884. See also *Grant v Southwestern and County Properties* [1975] Ch 185, 196-197.

77 *Senior v Holdsworth, ex p Independent Television News Limited* [1976] QB 23, [1975] 2 All ER 1009, [1975] 2 WLR 987, *Sapporo Maru v Statute of Liberty, Re The Statute of Liberty* [1968] 2 All ER 195.

78 *Chmara v Nguyen* (1993) 104 DLR (3d) 244, 249-250.

79 *Hastie and Jenkerson v McMahon* [1990] 1 WLR 1575. *Cf.* In *Darby v DPP* (1994) 159 JP 533 it was held that the display of a speed trap computer was not a document.

80 *R v Wood* (1982) 76 Cr App Rep 23, [1982] Crim LR 667, *PP v Ang Soon Huat* [1991] 1 MLJ 1 (Singapore High Court), *Sophocleous v Ringer* [1988] RTR 52.

81 *Castle v Cross* [1985] 1 All ER 87.

computerised phone systems registering calls and calling information[82] are admissible.

3.42. Despite being drafted more than 130 years ago, the definition of a "document" in the Evidence Act is surprisingly resilient for its technology neutrality. A "document" is defined in the Evidence Act as follows:

> "document" means any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of those means intended to be used or which may be used for the purpose of recording that matter;[83]

3.43. There has never been any suggestion that the definition has to be amended to cater to documents recorded in an electronic medium or expressed by an electronic device. The reference in the definition to "any matter expressed or described upon any substance" has been general enough to provide for the admission of electronic records as documents. This also draws support from the robust approach taken at common law that the need to interpose an instrument (such as a computer) to view or perceive the information recorded on the medium does not make such a medium any less a document.[84]

3.44. Similarly, a "document" is defined in a technology-neutral manner in the Criminal Procedure Code ('CPC'):

> "document" includes, in addition to a document in writing —
>
> (a) any map, plan, graph or drawing;
>
> (b) any photograph;
>
> (c) any disc, tape, sound-track, or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and
>
> (d) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as aforesaid) of being reproduced therefrom;

---

82 *R v Spiby* (1990) 91 Cr App Rep 186, [1991] Crim LR 199, *R v Neville* [1991] Crim LR 288 (English Court of Appeal – Criminal Division).

83 S 3(1), Evidence Act.

84 *Grant v Southwestern and County Properties Ltd* [1975] Ch 185.

> "film" includes a microfilm;
>
> "statement" includes any representation of fact, whether made in words or otherwise.[85]

3.45. And pursuant to this provision, it has been held by Yong Pung How CJ in the Singapore High Court in the case of *Roy S Selvarajah v PP* that the computer database records with the Data Processing Centre of the Immigration Department are admissible as "documents" under section 380, CPC.[86]

3.46. We submit that a technology-neutral approach will not pose any serious obstacle to the admissibility of electronic evidence as such. The courts have adopted a very pragmatic view of the issue of admissibility of electronic evidence, and in cases such as *R v Neville*, even ruled that its conclusion remains the same regardless of whether the electronic evidence is admissible pursuant to a computer specific admissibility provision or pursuant to common law rules of admissibility.[87] This strongly suggests that it is possible to develop technology-neutral rules that rely on existing probative and auxiliary policies to regulate the admissibility of electronic evidence. Such a solution is the least invasive and most balanced yet incremental approach to the problem. We also submit that it is only where we conclude that existing probative and auxiliary policies do not deal adequately with issues posed by electronic evidence, that we can justify the enactment of a "self-contained code governing the admissibility of computer records"[88] such as the current regime in sections 35 and 36 of our Evidence Act. The previous regime in the old sections 35 and 36 for admitting electronic evidence only

---

85 S 378(4), Criminal Procedure Code (Cap 68, 1985 Rev Ed) ('CPC').

86 [1998] 3 SLR 517 (Singapore High Court). Arguably, a provision like s 380, CPC, which is "without prejudice to section 35 of the Evidence Act" cannot operate to override the effects of s 35, Evidence Act. Thus even if electronic evidence is found to be admissible pursuant to s 380, CPC, it must still be rendered admissible pursuant to s 35, Evidence Act.

87 *Supra*, note 82.

88 *R v Minors and Harper* [1989] 1 WLR 441, 446.

admitted hearsay computer records. It is to this issue that we now turn to identify the possible reasons for the specified treatment of electronic evidence.

Q. Should the rules of evidence that deal with the admissibility of electronic evidence be technology-neutral?

Q. Should the definitions of the term "computer" and "computer output" in the Evidence Act be retained?

Q. Should the definition of the term "document" in the Evidence Act be revised to include electronic records?[89]

Electronic Evidence as Real Evidence and as Hearsay

The Relationship between Real Evidence and Hearsay

3.47. In defining a "computer" in the Evidence Act, Parliament excluded from the ambit of this definition, devices which are non-programmable or which do not contain any data storage facility.[90]

---

89 An example of such an approach is found in section 3 of the Malaysian Evidence Act, which defines a "document" as follows: "document" 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. *Illustration*: A matter recorded, stored, processed, retrieved or produced by a computer is a document."

90 Statutory exception to the definition of "computer" in s 3(1), Evidence Act.

3.48. This immediately suggests that there are two broad categories of electronic evidence: (i) evidence derived from programmable devices, i.e. computers and computing devices, and (ii) evidence derived from facilities where information sought to be admitted via such evidence is first stored. This exactly mirrors the debate as to whether electronic evidence should be classified as real evidence or hearsay.

3.49. This distinction is well founded at common law, which draws a sharp distinction between computer output or records produced by electronic devices without human intervention (real evidence) and output in the form of records of human assertions, depending on human perception and the supply of such information to the computer (hearsay).[91] This distinction[92] has been judicially sanctioned and applied in cases such as *R v Wood*,[93] *Castle v Cross*[94] and *R v Spiby*[95]. It is the basis for the distinction between the two cases of *PP v Ang Soon Huat*[96] and *Aw Kew Lim v PP*[97], both decided by the Singapore High Court and by the same judge, concerning the old section 35 of the Evidence Act.

3.50. This dichotomy has also split legislative drafting on the issue of admissibility of electronic evidence. In some jurisdictions such as the Commonwealth of Australia, New South Wales, Tasmania, Australian Capital Territories and Malaysia, the electronic evidence admissibility provisions apply equally to both electronic real evidence as well as

---

91 *Supra*, note 31, at 137-140.

92 Initially proposed by Prof. Smith, See Smith, "The Admissibility of Statements by Computer" [1981] Crim LR 387, at 390.

93 *Supra*, note 80.

94 *Supra*, note 81.

95 *Supra*, note 82.

96 *Supra*, note 32.

97 *Supra*, note 33.

hearsay.[98] In other jurisdictions, such as Queensland,[99] South Africa,[100] and Canada,[101] the electronic evidence admissibility provisions only apply to electronic documents, by treating computers as recording devices.

3.51. Our sections 35 and 36, which are closely modelled on the South Australian model,[102] apply to both electronic real evidence as well as hearsay.[103] Section 35(1) is explicitly worded to govern the admissibility of computer output being "tendered in evidence for any purpose whatsoever". As the House of Lords said in *R v Shepherd*, such a duty imposed on the court not to admit any electronic evidence applies to any electronic document produced with or without the input of information provided by the human mind.[104]

Three Categories of Electronic Evidence

3.52. The real evidence/hearsay distinction can be best brought out by considering electronic evidence as emanating from, broadly speaking, three different ways for electronic devices to generate electronic evidence. Evidence may be produced by:

(a) an electronic device that stores information; or

(b) an electronic device that processes information; or

---

98 Ss 146, 147, Commonwealth of Australia Evidence Act 1995, New South Wales Evidence Act 1995 and Tasmanian Evidence Act (identical to ss 146, 147, Commonwealth of Australia Evidence Act 1995), ss 90A, 90B, Malaysian Evidence Act 1950.

99 S 95, Queensland Evidence Act.

100 S 1(1), South African Computer Evidence (No 57 of 1983), which uses the formulation of "computer print-out" and "authenticated computer print-out".

101 Canadian Uniform Electronic Evidence Act 1995.

102 Ss 59A, 59B, 59C, South Australian Evidence Act 1929.

103 *Butterworths Annotated Statutes of Singapore*: *Evidence*, Vol 5, at 120-121. See also Seng D, "Computer Output as Evidence", *supra*, note 31, at 140-141.

104 *Supra*, note 54. The same conclusion was reached in *Lim Mong Hong v PP, supra,* note 31.

(c) an electronic device that both stores and processes information.[105]

3.53. In the first category, evidence in the form of electronically stored records involves the use of the computer and other electronic devices as essentially data storage devices. The electronically stored records are admitted for the human observations and input which they capture. The hearsay rule must apply to such records. In the second category, where the computer and such other electronic devices are programmed to process information, and the evidence that is adduced is that which has been processed by the computer, the level and significance of human intervention drops and these devices are essentially data processing devices.[106] Where the computer and such other electronic devices and the information therein are the evidence, the fact that such devices and the information recorded therein are electronic in nature is hardly a bar to their admissibility as real evidence.[107]

3.54. Of course, an item of electronic evidence may contain different types of "processed" information, or even both "stored" and "processed" information. An illustration of this third category of evidence may be found in *R v McKeown*.[108] Here, the printout was from an Intoximeter which showed the time of the test and the results of the test. It was held that the error in the time (it was 15 minutes slow) on the printout did not affect the accuracy of the alcohol analysis and admitted the printout. The court took expert evidence that the clock mechanism in the Intoximeter was separate from the alcohol mechanism.

---

105 Seng D, "Computer Output as Evidence", *supra*, note 31, at 166-173.

106 *Ibid*, at 173-178.

107 *Ibid*, at 179-180.

108 [1995] Crim LR 69, decision of the Divisional Court rejecting the evidence reversed by the House of Lords in [1997] 1 All ER 737, [1997] 1 WLR 295. The same conclusions were reached in *DPP v Horswill* (2 July 1997, unreported) (Queen's Bench Division), *DPP v Page* (19 May 1998, unreported) (Queens' Bench Division) and *DPP v Barber* (1998) 163 JP 457 (Queens' Bench Division).

This is a sensible decision and it affirms the correctness of classifying processed information as real evidence. On the other hand, if the printout showed the name of the driver tested and the breath alcohol reading, this is a hybrid item of evidence with elements of hearsay *e.g.* the name supplied by the driver that is not intrinsically part of the machine, and elements of real evidence *e.g.* the readings supplied by the processing component of the machine.[109]

3.55. Occasionally, the distinction between these three categories of evidence can be a fine one. For instance, in the case of *R v Pettigrew*[110], the prosecution sought to adduce in evidence a computer printout recording the first and last serial numbers of a bundle of 100 notes. This was a crucial piece of evidence which enabled the prosecution to trace the notes in the possession of the accused back to the bank from which they were stolen. Whether it was inadmissible hearsay or not really turned on whether the computer had "read" the serial number on the first note, or had been supplied this number by the human operator. In the former, it would be real evidence and admissible as every aspect of the printout was generated without human intervention. In the latter, it would be partly hearsay and partly real evidence: while the computer counted the notes, it was an unidentified human operator who fed the first number into the computer, which recorded it, and printed it as part of its printout.[111]

3.56. In most instances, courts have applied common sense to determine if a printout is hearsay or otherwise. Sometimes,

---

109 In certain circumstances, even the time that is recorded in the machine will be disregarded where there is evidence that it is inaccurate. See *DPP v Ward* (12 February 1998, unreported) (Queen's Bench Division), where Schiemann LJ held that as between the time shown on the Intoximeter printout suggesting that the legal breath analysis warning came after the first breath sample was given (at 0154 hours), and the time recorded in the police officer's statement that the warning was given before the breath sample (which commenced at 0156 hours), as what was important was the sequence of events and not the time of the clock, the court believed the police officer and disregarded the time shown on the printout.

110 (1980) 71 Cr App R 39, [1980] Crim LR 239.

111 Seng D, "Computer Output as Evidence", *supra*, note 31, at 138-139.

the nature of the information adduced on the printout allows the courts to make these decisions readily. For instance, information such as the names of the residents of a community, the community charges due from them and the charges remaining unpaid were derived from "information implanted by a human" and were clearly not derived from the community register. Thus it did not matter that the outputs were tendered in the form of a computer printout. The court excluded the printout in evidence as being hearsay and the charges against the accused listed in the printout for failing to make the community payments were quashed.[112]

3.57. But again, the line can be blurred in some instances. A case that calls for careful analysis is *R v Ewing* where the prosecution admitted in evidence a computer printout from a bank's computer, showing the transactions on the account.[113] The court concluded that it was hearsay, but admitted it pursuant to a hearsay exception. But just as Electronic Data Interchange records could not be said to be hearsay,[114] the banks records as extracted and reproduced on the printout could not be said to be hearsay. The electronic records *are* the manifestation of the transaction.[115] While the conclusion reached was the right one, the reasoning process which was deployed by the court was not.[116] This wrong approach was set right in *R v Governor of Brixton Prison, ex parte Levin* where it was held by

---

112 *R v Coventry Justices Ex Parte Bullard and Bullard* [1992] RA 79.

113 [1983] QB 1039, [1983] 2 All ER 645, [1983] 3 WLR 1.

114 Bradgate, "The Evidential Status of Computer Output" (1990) 6 Computer Law and Practice 142, at 145-146. The Uniform Law Conference of Canada makes the same point by removing from consideration of the Canadian Uniform Electronic Evidence Act 1995, EDI records. However, it reaches this conclusion on the basis that "EDI's special legal issues concern contract law, not evidence law." See Uniform Law Conference of Canada, "Civil Section Documents – Electronic Evidence: Computer Produced Records in Court Proceedings", 1994 Proceedings of Annual Meetings, at para 22, *supra*, Part II, note 2.

115 Smith, "Case Commentary on *R v Ewing*" [1983] Crim LR 472, at 473.

116 Seng D, "Computer Output as Evidence", *supra*, note 31, at 179.

the House of Lords that the computer printouts recording the fraudulent funds transfers were not assertions that such transfers had taken place, were not hearsay and were admissible in evidence.[117]

Q. Do the real evidence rule and the hearsay rule have continued relevance in relation to electronic evidence?

The Hearsay Rule (and its Exceptions) Exist Separately from Electronic Evidence

3.58. This analysis confirms that the hearsay rule as a rule of probative policy exists independently of the electronic nature of the medium of the evidence. The hearsay rule is concerned with the reliance on unattested human input made in out of court statements for the facts stated, be they in electronic form or otherwise. On this analysis, there is no objection to the admission of electronic business records if they fall within the hearsay exceptions. They are admitted, not as electronic records, but as business records that, by virtue of the circumstances in which they are kept, exhibit a high degree of reliability.

3.59. Therefore, it is submitted that the approach to create a special exception to the hearsay rule to admit electronic business records is not appropriate. The same business

---

117 *R v Governon of Brixton Prison, ex parte Levin* [1997] 3 All ER 289, [1997] 3 WLR 117, [1998] 1 Cr App Rep 22, [1997] Crim LR 891. One can apply this approach to test the correctness of this conclusion. Suppose instead of effecting the transactions on the accounts in the computer, the bank, being an old-fashioned traditional bank that does not believe in computerisation, chooses to keep all the transaction receipts as they are processed over the bank counter. The status of the customer's account can only be ascertained by examining all such receipts and consolidating them. If such receipts are tendered in evidence, starting from the very first receipt to the latest receipt, there is no reason to deny their admissibility on the basis of hearsay. Now, suppose the transaction instructions on all these receipts are actually stored electronically and a printout abstracted of these transaction instructions is sought to be admitted. If there is a hearsay objection to the admissibility of physical receipts, there should be a similar hearsay objection to the admissibility of the printout. The fact that the printout is extracted from electronic records does not change the nature of the evidential analysis.

exception rules should apply, regardless of whether the records are electronic or otherwise.

3.60. Similarly, to set up electronic admissibility provisions that cater solely to "computer output" or "computer printout" where such devices are simply used to store information and to admit such evidence independently of the hearsay rule is also inappropriate. The probative policy of the hearsay rule – reliance on records containing human representations – cannot and should not be disregarded, simply because the records are in electronic form. There is nothing in the nature of electronic evidence that lends additional reliability to human representations captured in electronic form. To do so will be to create a dangerous new exception for electronic evidence which will unduly favour electronic evidence.

Q. Should there be a provision in the Evidence Act to provide for the admissibility of electronic business records?

Q. Should there be a provision in the Evidence Act to provide for the admissibility of electronic evidence as an exception to the hearsay rule?

Authentication Issues with Electronic Evidence

3.61. So what is in the nature of electronic evidence that triggers such close legislative, judicial and academic scrutiny? In *R v Shepherd*, Lord Griffiths said:

> Documents produced by computers are an increasingly common feature of all business and more and more people are becoming familiar with their uses and operation. Computers vary immensely in their complexity and in the operations they perform. The nature of the evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case. The evidence must be tailored to suit the needs of the case. I suspect that it will very rarely be necessary to call an expert and that in the vast majority of cases it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer in the

> sense of knowing what the computer is required to do and who can say that it is doing it properly.[118]

3.62. In *DPP v McKeown*, Lord Hoffman has this to say:

> The purpose of section 69 [of UK PACE 1984], therefore, is a relatively modest one. It does not require the prosecution to show that the statement is likely to be true. Whether it is likely to be true or not is a question of weight for the justices or jury. All that section 69 requires as a condition of the admissibility of a computer-generated statement is positive evidence that the computer has properly processed, stored and reproduced whatever information it received. It is concerned with the way in which the computer has dealt with the information to generate the statement which is being tendered as evidence of a fact which it states.[119]

3.63. These two statements by the members of the House of Lords suggest that there is a general reluctance to trust electronic evidence. Computers were seen as new or novel devices, whose internal functions were complex and relatively mysterious. Their use could be abused, and they could fail to operate properly. The courts would therefore call for other evidence to assuage these concerns.

3.64. Lord Hoffman calls such evidence "positive evidence", and Lord Griffiths describes the adducing of such evidence to "discharge the burden". Both learned law lords are really describing a new class of evidence, separate and independent from the electronic evidence which is sought to be admitted in evidence. They are describing the adducing in evidence of "authentication evidence". As section 9 of our Evidence Act explains:

> **Facts necessary to explain or introduce relevant facts**
>
> 9. Facts necessary to explain or introduce a fact in issue or relevant fact, or which support or rebut an inference suggested by a fact in issue or relevant fact, or which establish the identity of any thing or person whose identity is relevant, or fix the time or place at which any fact in issue or relevant fact happened or which show the relation of parties by whom any such fact was transacted, are relevant in so far as they are necessary for that purpose.

---

118 *Supra*, note 54.

119 *Supra*, note 108, at 302D, per Lord Hoffmann.

3.65. The over-arching objectives behind the mechanisms in section 69, UK Police and Criminal Evidence Act 1984 ('UK PACE 1984') and section 35, Evidence Act are the same: both provide that "a statement in a document produced by a computer" or "computer output" shall not be admissible "unless" it is shown that it could be relied upon. The supporting evidence required in both section 69, UK PACE 1984 and section 35(1)(c) has to establish that (i) there are no reasonable grounds for believing the evidence to be inaccurate because of improper use of the computer, and (ii) there is reasonable ground to believe that at all material times the computer was operating properly, or, if not, that any respect of its improper operation or failure to operate would not affect the evidence.

3.66. Thus these provisions provide that such supporting evidence is statutorily necessary to explain or introduce the electronic evidence. If the supporting evidence is not forthcoming, the electronic evidence is inadmissible. As the US Federal Rules of Evidence describes, authentication evidence is a condition precedent to the admissibility of the evidence itself:

> **ARTICLE IX. AUTHENTICATION AND IDENTIFICATION**
>
> **Rule 901. Requirement of Authentication or Identification**
>
> (a) General provision.—The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

3.67. As a rule of authentication, authentication evidence is required regardless of whether the evidence that is to be supported is hearsay or real evidence. For instance, section 9 of the Northern Territories Evidence (Business Records) Interim Arrangements Act 1984 ('EBRIAA'), requires the court to assess the reliability of business devices as well as the means from which information is reproduced or derived from such devices. This, and the use of

expressions such as "reproduced or derived",[120] confirms the Northern Territories legislature's appreciation that authentication applies to both "stored" and "processed" information. Similarly section 9, Evidence Act as well as Rule 901, US Federal Rules of Evidence, operate as "a condition precedent to admissibility" for all types of evidence. As Lord Griffiths said in *R v Shepherd*:

> It is surely every bit as important that a document produced by a computer and tendered as proof of guilt should be reliable *whether or not it contains hearsay*.[121]

The Role of Authentication Evidence

3.68. The crucial role that authentication evidence plays in our trial process is not to be discounted.[122] Authentication is nothing more than a special aspect of relevancy[123] that is inherently necessary.[124] Authentication provides the proponent of any evidence the opportunity to discharge the burden that is placed upon him: that the evidence sought to be adduced is what the proponent claims it is. It applies equally to chattels as it does to documents.[125] The prosecution must prove that the accused is the perpetrator, for instance, through witnesses' identification,[126] and that the item or article analysed and presented in court as evidence is the same item or article seized from the accused.[127] If the

---

120 "Or both reproduced and derived". See s 5(1)(c), EBRIAA.

121 *Supra*, note 54.

122 See, generally, *Butterworths Annotated Statutes of Singapore*: *Evidence*, Vol 5, *supra*, note 103, at 53-58.

123 Morgan, *Basic Problems of Evidence* (1962), at 378.

124 "The foundation on which the necessity of authentication rests is not any artificial principle of evidence, but on an inherent logical necessity." See §2129, Wigmore, Volume VII (Chadbourn Ed, 1978), at 703.

125 §2129, Wigmore, Volume VII (Chadbourn Ed, 1978), at 703-704.

126 Rules like *R v Turnbull* [1976] 3 All ER 549, [1976] 3 WLR 445 have been applied locally in cases *Heng Aik Ren Thomas v PP* [1998] 3 SLR 465, *Awtar Singh s/o Margar Singh v PP* [2000] 3 SLR 439, *Ye Wei Gen v PP* [1999] 4 SLR 101, *PP v Ong Phee Hoon James* [2000] 3 SLR 293.

127 That is, shown to be one that has a personal connection with the accused. See §2129, Wigmore, Volume VII (Chadbourn Ed, 1978), at 703.

"chain of evidence" is broken, for instance, because the exhibits seized from some other offender may have been mixed with those seized from the accused, it can no longer be asserted that the drugs tested were the drugs seized from the accused.[128] If the burden of proving authentication cannot be met, the consequence is the inadmissibility of the unauthenticated evidence.

3.69. The Evidence Act is replete with authentication rules for documents. Part II of the Act deals almost exclusively with such rules, ranging from proof of signatures on documents to public documents to various presumptions as to the genuineness,[129] proper authority,[130] authorship,[131] execution,[132] origin as to time and place,[133] and the integrity, correctness, completeness and accuracy[134] of the documents.

3.70. And there should be no doubt that the language used in sections 35 and 36 is the language of authentication.[135] Section 35 requires the proponent seeking to admit evidence under both the approved process and the certified output modes of admissibility to prove the proper use of a computer and its proper operation.[136] Section 36 further allows for the admission of such other additional

---

128 See *Lim Swee Seng v PP* [1995] 1 SLR 425, *Satti bin Masot v PP* [1999] 2 SLR 637. See also *Sia Soon Suan v PP* [1966] 1 MLJ 116, *Lim Young Sien v PP* [1994] 2 SLR 257, *PP v Chew Yoo Choi* [1990] 2 MLJ 444.

129 Ss 81, 82, 83, 86, 88, Evidence Act.

130 Ss 84, 85, 86, 87, Evidence Act.

131 Ss 82, 84, 89, 90, 92, Evidence Act.

132 Ss 82, 87, 91, 92, Evidence Act.

133 S 89, Evidence Act.

134 Ss 82, 85, 86, 88, 90, Evidence Act.

135 See, Seng D, "Computer Output as Evidence", *supra*, note 31, at 157-166.

136 See para 5, First Schedule, Evidence Regulations 1996 and s 35(1)(c), Evidence Act.

evidence to support or rebut the aforesaid evidence. Together, sections 35 and 36 call for evidence of:[137]

- the nature and circumstances of input,[138]
- absence or presence of any ill-will or ill-motive on the part of the human supplier or operator,[139]
- proper recording of data and operation of the computer system,[140] and
- absence of manipulation or proper operation of the computer system to produce the electronic evidence.[141]

Comparing Section 9 with Sections 35 and 36

3.71. How would the scheme for establishing authentication of electronic evidence in sections 35 and 36 of the Evidence Act compare with section 9 of the Evidence Act? We make three observations.

3.72. Firstly, sections 35 and 36 are over-inclusive in terms of the types of evidence they include. They encompass all types and forms of evidence emanating from electronic devices. This result on its own seems to discriminate against all electronic devices, and severely tests the equivalence principle. Section 9, on the other hand, already applies to all forms of evidence, tangible and documentary, real and hearsay. Its encompassing nature is a function of the rules of relevance.

3.73. The operating premises for these two sets of provisions are very different. The authentication rule in section 9 is premised on the need to provide supporting evidence for all items of evidence. However, the premise behind section 35 is that electronic evidence is unreliable and it requires

---

137 For a more detailed analysis of the effects of these provisions, please consult Seng D, "Computer Output as Evidence", *supra,* note 31, at 167-169 and 175-177.

138 S 36(4)(a), Evidence Act.

139 S 36(4)(b), Evidence Act.

140 S 35(1)(c)(ii) read with s 35(6)(b), Evidence Act.

141 S 35(1)(c)(i) and (ii) read with s 35(6)(a), Evidence Act.

particular supporting evidence. But there is a need to re-examine that premise in today's business environment. In the words of Lord Griffiths in *R v Shepherd*, if his lordship made the observation in 1993 that "[d]ocuments produced by computers are an increasingly common feature of all business", the pertinent observation to be made in 2003 must surely be "What documents used in our businesses are *not* documents produced by computers?" If there had been any general mistrust for computers and documents produced from computers, it has been replaced with a general acceptance of computers and their output.

3.74. However, our mistrust of computers and other electronic devices has not been so completely overcome that we can unequivocally rely on the presumption expressed in the Latin phrase *praesumuntur omnia rite esse acta*. Given the exceedingly wide range of electronic devices operating under a diverse spectrum of reliability, this observation, which has received judicial sanction, must be correct.[142]

3.75. Nor do blanket statements such as "hardware is more reliable than software because you can more easily detect hardware problems" carry significant weight. Modern computing hardware is made up of increasingly complex software elements, and given the interchangeable nature of hardware and software, programming as well as design errors can easily find their way into hardware. Manufacturers have often made hardware revisions, in very much the same way software developers release patches to fix defective software. And with the tight integration of hardware and software in processing information, it may be difficult to ascertain whether it was hardware or a software error that produced an unreliable piece of electronic evidence.

3.76. Secondly, the scheme developed for section 35 seems under-inclusive in its statutory prescription of the required authentication evidence. The principle mode of admissibility is certification. Section 35(1)(c) states that

---

142 Per Lord Griffiths in *R v Shepherd*, *supra,* note 54.

authentication may be supported by way of "a certificate signed by a person holding a responsible position in relation to the operation or management of the relevant computer system", as prescribed in section 35(6).[143] Such a certificate must in turn:

- purport to identify such output,
- describe the manner in which it was produced,
- give particulars of any device involved in the processing of such output,
- also give particulars of any device involved in the storage of such output,
- state that the certifier has "no reasonable grounds for believing that the output is inaccurate" because of improper use of the computer,
- state that "no reason exists to doubt or suspect the truth or reliability of the output",
- state that the certifier has "reasonable grounds to believe that at all material times the computer was operating properly" and
- if not, state that "in any respect in which it was not operating properly or out of operation, the accuracy of the output was not affected by such circumstances".[144]

3.77. It will be evident from the certification requirements that they are intended *ex facie* to be comprehensive. But practical difficulties have arisen in the observance of this requirement. Our certification requirement in section 35 is largely similar to the scheme in section 69 in the UK PACE 1984. Under the UK PACE 1984, the certificate must be introduced by "a person occupying a responsible

---

143 In *Lim Mong Hong v PP*, *supra*, note 31, it was held that the certification mode of admissibility did not operate to the exclusion of general proof of proper use and operation of the computer.

144 S 35(6) read with s 35(1)(c), Evidence Act.

position in relation to the operation of the computer".[145] This has given rise to interpretation issues as to whether electronic evidence can be certified without calling a computer expert. Thus in *R v Shepherd*, the evidence in question was the till rolls from the supermarket tills: a store detective testified as to the operation of the tills which were connected to the supermarket's central computer. But she had no technical understanding of the operation of the computer. The House of Lords accepted that she was not such a "responsible person", but allowed the evidence because it was possible to call for oral evidence from a witness who can give evidence that shows "she is fully familiar with the operation of the store's computer and can speak to its reliability."[146] After *R v Shepherd*, a whole range of witnesses have testified as to the reliability of the electronic evidence, from directors[147] to managers[148] to experts to operators. Even for the same device (for instance, the Intoximeter), different witnesses have testified as to its reliability, ranging from directors[149] to consultant forensic scientists with specialised knowledge of breath measuring equipment for the Intoximeter[150] to police officers who had operated the device,[151] even on the same issue of reliability of the Intoximeter printout.[152] (For instance, it is inconceivable how a director of the company which supplied the Intoximeter to the police could testify that the clock component and the analytical component were separate and the error in the time did not affect the reliability of the alcohol analysis, when the director himself

145 Para 8, Part II, Schedule 3, UK PACE 1984.

146 *R v Shepherd*, *supra,* note 54.

147 *R v Governor of Brixton Prison, ex p Levin, supra,* note 117.

148 *R v Governor of Brixton Prison, ex p Levin, ibid.*

149 *DPP v McKeown supra*, note 108.

150 *DPP v Page* (19 May 1998, unreported – QBD).

151 *DPP v Barber* (19 May 1998, unreported – QBD), *DPP v Ward* (12 February 1998, unreported – QBD), *DPP v Horswill* (2 July 1997, unreported – QBD).

152 *Ibid.*

admitted he had no expertise in electronics and was unable to substantiate his claim from the circuit diagrams of the Intoximeter.)[153] The root of this problem appears to be an assumption, perhaps facilitated by the statutory certification scheme, that so long as a witness testifies as to the reliability of the electronic device, no further authentication evidence is required. A statutory certification scheme masks the requirement to ensure that there is a clear link between the nature of the authentication required and the qualifications of the witness supplying the authentication evidence. A good example can be found in the case of *T v Ipswich Youth Court*, where an IT security manager, who only had knowledge of system security, in particular, third party threats to security, and would have no responsibility for the maintenance of computer records, or knowledge of system malfunction or operator error,[154] was asked to testify that the printouts from the lottery shop's computer were proper. His professional qualifications were clearly not relevant to the issue at hand and the court had remarked that the manager of the lottery shop would have been "a far more appropriate witness".[155]

3.78. But over-reliance on the qualified expert, whose testimony is of little relevance to the issues at hand, may lead to clearly weak reasoning. Thus, in *T v Ipswich Youth Court*, the judges placed so much emphasis on the fact that the IT security manager was such a statutorily qualified witness, "as a person familiar with the operation of the computer", that they were even prepared to make the reasoning leap that as an IT security manager, he would be "told of any defect in the computer system from the company which had in fact never broken down"[156] notwithstanding evidence to the contrary.

3.79. Under the current statutory scheme in section 35, only electronic documents produced by way of the approved

---

153 *DPP v McKeown, supra*, note 108.

154 *T v Ipswich Youth Court* (6 October 1998, unreported – QBD).

155 *Ibid.*

156 *Ibid.*

process are presumed accurate; no such presumptions exist for certified accurate electronic evidence.[157] It is still open to the court to call for further evidence to support or contradict the authentication evidence. Thus certified accurate electronic evidence will be most affected by the parallel scheme in section 36 that gives the court the discretion to call for the affidavit, not from the "person holding a responsible position in relation to the operation or management of the relevant computer system" who has produced the certificate, but from other people, such as other responsible operators or managers,[158] employees who had control or access[159] and appointed third parties who were given such control or access[160] over any relevant records and facts, as well as court appointed or accepted experts.[161] In addition, oral evidence may be supplied to further support or contradict all the authentication evidence hitherto advanced.[162] And this whole process may culminate in the court giving such evidence zero or little weight, having regard for "all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the output".[163] This was the approach taken by Yong Pung How CJ in *Lim Mong Hong v PP* where His Honour admitted the computer output in question (a Microsoft excel printout termed "Incoming and Payment Analysis") but practically rejected it by giving it negligible weight and relevance.[164] The presence of section 36, which is ostensibly designed to supplement section 35, actually exposes the shortcomings of the modes of admission in section 35. This could hardly contribute to the confidence of the proponent of the evidence who has

157 Seng D, "Computer Output as Evidence", *supra,* note 31, at 155.

158 S 36(2)(b), Evidence Act.

159 S 36(2)(c), Evidence Act.

160 S 36(2)(d), Evidence Act.

161 S 36(2)(e), Evidence Act.

162 S 36(3), Evidence Act.

163 S 36(4), Evidence Act.

164 *Lim Mong Hong v PP, supra*, note 31.

gone to considerable lengths to procure the requisite section 35(6) certification.

3.80. Thirdly, the very reasons why sections 35 and 36 are under-inclusive in their prescription of the required authentication evidence also, paradoxically, make them over-inclusive in terms of the same authentication evidence. While the authentication requirements in these sections may be appropriate (or even inadequate, as explained above) for contentious electronic evidence, they will be too onerous and demanding for the vast majority of electronic evidence.[165] It should be observed that the UK Law Commission was extremely critical of section 69, UK PACE 1984, from which our section 35 was directly derived. The UK Law Commission commented that "advances in computer technology had made it increasingly difficult to prove satisfaction with the examination and certification conditions especially in relation to networked systems" and doubted if proponents of electronic evidence could satisfactorily prove compliance with the terms the provision.[166] Based on their recommendations, section 69, UK PACE 1984 has been repealed, as is section 5, UK CEA 1968, from which section 69, UK PACE 1984 was ultimately derived. A similar examination and certification model in section 3 of the South African SACEA 1983 has also been repealed. It is very telling that two out of the three jurisdictions from which we derived our section 35 – UK and South Africa – have repealed their computer output admissibility provisions. And in South Australia, the computer output admissibility provisions have been judicially interpreted away as supplementing common law rules for the admissibility of electronic evidence.[167] These

---

165 For instance, it would appear to be highly excessive and quite unnecessary to require a full-fledged inquiry as to the proper use and operation of a time keeping device on something as ubiquitous as time pieces. And to apply the certification requirements strictly to all digital photocopies of documents will be to introduce an unnecessary burden to the trial process.

166 UK Law Commission Report No 245, *supra*, Part II, note 71, paras 13.6 - 13.10.

167 See *supra*, Part II, para 2.51.

three jurisdictions have moved away from strict statutory rules providing for the examination and authentication of electronic evidence in favour of a practical and pragmatic approach centring on the existing common law rules of authentication. As the UK Law Commission opined, "[T]he real issue for concern was authenticity and …this was a matter which was best dealt with by a vigilant attitude that concentrated upon the weight to be attached to the evidence, in the circumstances of the individual case, rather than reformulating complex and inflexible conditions to admissibility".[168]

3.81. This very same approach in favour of practicality and flexibility and avoiding the strict statutory approach of section 35 is reflected in current practice where parties have elected not to dispute and courts have chosen not to examine the authenticity of electronic evidence. (An examination of some Singapore cases that have bypassed section 35 can be found in Appendix IV.) These instances would hardly constitute admission of such evidence by *express* agreement under the first mode of admissibility in section 35.[169] Arguably, the strictures that section 35 pose to the trial process have been circumvented by the expediency of ignoring it – by both lawyers and judges alike.

3.82. It is submitted that, what lawyers and judges have done, in effect, is to treat the issues pertaining to electronic evidence as authentication issues. As a precondition to admissibility under section 9, authentication becomes a *non sequitur* where parties choose not to dispute authenticity. In such an instance, if the opponent of the evidence does not dispute the authenticity of, say, the printout, its authenticity is no longer "in issue"[170] and authentication evidence will no longer be "necessary to explain or introduce" the printout. As Wigmore explained, "authentication [is] not necessary when [it is] not in issue or when admitted [or by

168 See *supra,* Part II, para 2.29.

169 S 35(1)(a), Evidence Act.

170 S 3(1), Evidence Act.

way of] judicial admission [or] opponent's spoliation."[171] For this reason, even in the absence of an express agreement by the party against whom the evidence is introduced, courts have admitted digital photocopies of documents, surveillance videotapes and readings of time from watches and clocks, where only general and not exacting precision is required.

3.83. Thus, section 9 is thus perfectly consistent with the equivalence principle. As noted by a learned author:

> [T]he standard for authenticating computer records is the same for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form.[172]

3.84. For these reasons, we submit that an open-ended authentication solution based on section 9, Evidence Act and similar to the approach adopted in relation to US jurisprudence for Rule 901, Federal Rules of Evidence is the most appropriate. This is the modern approach taken in the UK, as explained by the UK Law Commission in their 1997 report on PACE 1984. The justification advanced by the Law Commission for the abolition of section 69, PACE 1984 is that many jurisdictions around the world do not have specific admissibility rules for examination and certification of electronic evidence and "no special problems" have arisen as such.[173] This is because most of the time, the courts would not be remiss in admitting electronic evidence where there are extrinsic assurances as to its reliability. But where there are pertinent disputes as to the authenticity of electronic evidence, the courts can call for a "more comprehensive foundation" for the evidence because of its complex nature.[174]

---

171 §2132, Wigmore, Volume VII (Chadbourn Ed, 1978), at 714.

172 US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* ('DOJ Report'), at 142.

173 UK Law Commission Report No 245, para 13.12, s*upra,* part II, note 71.

174 *United States v Scholle*, 553 F.2d 1109, 1125 (8th Cir. 1977).

Q. Can the issues relating to the reliability of electronic evidence be adequately resolved as issues relating to the authentication of such evidence?

Authentication of Electronic Evidence

3.85. As Wigmore explained, authentication is a rule of inherent logical necessity,[175] a rule that evidence must be associated with a person, a time, a place or other known condition.[176] It is not possible to spell out all the possible rule of authentication of electronic evidence, given the prevalence of electronic devices as well as the infinite variety of circumstances involved – electronic evidence as real evidence, as documents and as hearsay statements, and its use in different environments for different purposes.[177] And not all issues of electronic authentication will be relevant in every case. However, because electronic authentication is a relatively new concept, and because electronic records are inherently mutable, authentication issues will take on greater relevance and immediacy. This Paper seeks to elaborate on some of the authentication issues for illustrative purposes.

3.86. *Identification*. Used in a technical sense, "identification" presupposes the existence of two objects that are apparently different but have been referred to, and the issue is whether they are in fact one and the same object.[178] Identification authentication evidence is called for when there are, for instance, two entries for the debiting of the same amount at the same time in the bank statement. Since it is crucial to determine whether these are two separate transactions for the same amount, or a computer error where a debit is "counted twice" in the computer records, authentication identification evidence such as the unique transaction identification code for each transaction entry

---

175 §2129, Wigmore, Volume VII (Chadbourn Ed, 1978), at 703.

176 §2130, Wigmore, Volume VII (Chadbourn Ed, 1978), at 709.

177 *Ibid.*

178 *Ibid.*

and the date/time stamp for each entry transaction will enable this issue to be resolved. Identification authentication evidence is particularly necessary for those electronic records where it is not unusual to find duplicate entries.

3.87. *Chain of evidence*. This describes the evidence that has to be presented to provide an adequate foundation that the object offered in evidence is the object that was involved in the incident. A significant issue in criminal law is that the prosecution bears the burden of proving beyond reasonable doubt that the exhibit before the court was the exhibit seized from the offender. Where there is a break in the chain of evidence, and the court is not persuaded that the exhibit is that related to the subject matter of the dispute, for instance, that the drugs analysed and exhibited were the drugs seized from the accused, an acquittal would have to be recorded.[179]

3.88. Issues as to chain of evidence will normally arise if there are discrepancies as to the key characteristics of the items of evidence, *e.g.* its quality and quantity. In criminal investigations, because most exhibits will be under police custody pursuant to clear police guidelines and rules for handling evidence, starting with their retention and custody, their safekeeping, their movement and their eventual production in court, the burden of proving chain of evidence authentication is normally met by having the police officer who first secured its retention and custody testify that that was the item.[180] In this regard, the clear making of the item for identification immediately after retention and seizure, the immediate sealing or preservation of the item to prevent tampering, and the making of appropriate exhibit registry entries will go a long way towards discharging this burden of proving the chain of evidence.[181]

---

179 *Butterworths Annotated Statutes of Singapore*: *Evidence*, *supra*, note 103, at 53-54.

180 *Su Ah Ping v PP* [1980] 1 MLJ 75.

181 *Namasiyiam & Ors v PP* [1987] 2 MLJ 336, *Pavone v PP (No 2)* [1986] 1 MLJ 423, *Shamsuddin bin Hassan v PP* [1991] 3 MLJ 314, *Ong Lee Koon & Anor v PP* [1995] 2 SLR 750.

3.89. Given the ubiquity of some electronic devices, it is thus very important for purposes of preserving the chain of evidence to record down their unique identification numbers. A statement such as "seized in evidence: one black 3.5" 1.44 MB floppy disk or one CD-ROM" is not helpful in discharging this burden if there are many caches of similar-looking or similarly identified disks that are in custody, and there is no way of distinguishing between them, or if they are mixed up.

3.90. *Integrity*. Integrity describes the requirement for the object that is involved in the incident to remain substantially unchanged when it is presented in court as an exhibit. If the item of evidence in question is relatively impervious to change, the trial court has a broad discretion to admit the evidence merely on the basis of testimony that the item is the one in question (chain of evidence) and presume it is in a substantially unchanged condition.[182]

3.91. Some forms of electronic evidence will pose greater challenges for police prosecutors in this regard, given the mutability of electronic evidence in the form of read-writable storage media such as tapes, diskettes, hard disks and CD-RWs, flash-read only memories and other solid-state electronic recording devices. Where doubts arise, especially where a long time elapsed between the retention of the evidence and its eventual production,[183] the intermediate officer handling the exhibit must testify.[184] Similarly, where electronic evidence is susceptible to tampering or contamination, the court may exercise its discretion to require more elaborate authentication evidence.[185]

3.92. In this regard, we are confident that the police will have proper guidelines for the retention, custody, safekeeping and identification of electronic evidence.

---

182 §212, Strong, *McCormick on Evidence* (5th Ed., 2002), Vol 2, at 9.

183 *Abdullah bin Yaacob v PP* [1991] 2 MLJ 237.

184 *Teoh Hoe Chye v PP* [1987] 1 MLJ 220, *PP v Chew Yoo Choi* [1990] 2 MLJ 444.

185 McCormick, *supra*, note 182, Vol 2, at 9.

3.93. *Attribution to Individuals*. An item or a document may only be relevant upon establishing the existence of some connection between that item or document and a particular individual, i.e. that it came from that individual (origination), that the document was written or signed by the individual (authorship) and that the individual had signed the document with the intention of signing or approving the document (execution). While in everyday affairs of business and social life, it is customary to just examine the document itself for evidence as to its source and act upon it, a more rigorous process is adopted in a court of law. If the document is signed or written by X, it must be proved that the signature or the handwriting is that of the person X.[186] If the document is executed by X, it must be proved that the document is signed by X as authentication and signed and delivered in the presence of X's witnesses,[187] unless X himself admits of its execution.[188] As section 9 states, attribution of evidence constitutes "facts that may explain or establish the identity of any thing whose identity is relevant". As illustration (a) to section 9 shows:

> The question is whether a given document is the will of A.
>
> The state of A's property and of his family at the date of the alleged will may be relevant facts.

3.94. In this illustration, if the will purported to be A's accurately describes the state of A's property and of his family at the date of the alleged will, and the will discloses such knowledge that only A is likely to have, the inference that the will is A's is very strong. This illustration is useful because it demonstrates that issues of origination, authorship and execution need not always be established by evidence of handwriting and handwritten signatures.[189]

---

186 S 69, Evidence Act.

187 Ss 70-71, Evidence Act.

188 S 72, Evidence Act.

189 Ss 69, 75, Evidence Act.

3.95. In fact, in the electronic environment, this is infeasible.[190] Whereas it may be said that handwritten signatures are unique to each individual and thus uniquely identify the individual, there is no such assumption when applied to electronic signatures, which are merely "any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record"[191], unless several procedural and technical safeguards have been satisfied. These procedural and technical safeguards provide indirect proof that the electronic signature applied originates from and is authored and executed by the signatory. Section 17, Electronic Transactions Act, sets out these procedural and technical safeguards:

> **Secure electronic signature**
>
> 17. If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —
>
> (a) unique to the person using it;
>
> (b) capable of identifying such person;
>
> (c) created in a manner or using a means under the sole control of the person using it; and
>
> (d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated,
>
> such signature shall be treated as a secure electronic signature.

3.96. Contrary to common misperception that it only applies to digital signatures, which are a form of secure electronic signatures (provided they meet additional procedural and technical safeguards unique to digital signatures),[192] section 17 applies equally to other classes of signatures such as biometric signatures. This is, of course, provided that these

---

190 S 69(2), Evidence Act.

191 S 2, Electronic Transactions Act.

192 S 20, Electronic Transactions Act.

signatures implement procedural and technical safeguards set out in section 17. These safeguards afford secure electronic signatures with characteristics that will conjunctively and circumstantially prove that the signatory signed the electronic signature and that the document to which the signature applied had not been tampered with since it was signed (integrity). If these safeguards are satisfied, the following presumptions of authorship (section 18(2)(a)) and execution (section 18(2)(b)) apply:

> **18. Presumptions relating to secure electronic records and signatures**
>
> (2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that —
>
> (a) the secure electronic signature is the signature of the person to whom it correlates; and
>
> (b) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

3.97. Alternatively, in the absence of electronic signatures, one can rely on the origination rules in section 13 of the Electronic Transactions Act, which prescribe a series of escalating rules for ascertaining if a transmitted electronic record can be "deemed to be" or be "entitled to be regarded as" the originator's. The UNCITRAL Commentaries on these provisions[193] describe them as presumptions that under the enumerated circumstances, a data message would be considered a message of the originator.[194] It is also clear from the UNCITRAL Commentaries that the ultimate rule is that an electronic record is that of the originator if it is proved to be sent by the originator himself, regardless of the operation of the presumptions.[195] Thus, if the recipient of the message had

---

193 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, *supra*, note 24.

194 *Ibid*, para 83.

195 *Ibid*, para 88. The same Commentaries made no distinction between language such as "deemed to be that of the originator" and "entitled to regard an electronic record as being that of the originator and to act on that assumption".

received the message from the originator, and had applied "a procedure previously agreed to by the originator" to "ascertain whether the electronic record was that of the originator",[196] notwithstanding the originator's subsequent retraction note,[197] if it can be proven that the message was the originator's, he would be bound by his message pursuant to section 13(1), Electronic Transactions Act.[198] This suggests that the Electronic Transactions Act is not intended to exhaustively set out all the possible modes of proving authentication.

3.98. *Attribution to machines*. An item or a document may be relevant only if there can be established existence of some connection between that item or document and a particular machine. For instance, section 35(6) of the Evidence Act requires the proponent to establish "particulars of any device involved in the processing and storage of such output". The identity of the machine may be relevant because the individual is identified by the machine he uses.[199] The identity of the machine may also be relevant because there may be considerations such as the reliability of the machine or its proper calibration, which will in turn affect the quality of the evidence produced from that machine.

3.99. *Calibration, Operation and Accuracy*. Some devices require some initial settings or calibration before they operate, or they can produce accurate results. If they are calibrated wrongly or improperly, the operation of the machines will be affected, and their readings and output will also be erroneous. In *Mehesz v Redman*, the South Australian court

---

196 S 13(3)(a), Electronic Transactions Act.

197 S 13(4), Electronic Transactions Act.

198 *Supra*, note 193, at para 88. In the scenario previously outlined, evidence suggesting that the originator had transmitted his retraction note to avoid being bound by the data message which he had sent to the recipient is circumstantial evidence that the data message did originate from the originator in the first instance.

199 For instance, the IP address found in email headers enable the message to be traced to the machine and thus associated with the user.

described the use of sample standards of alcohol to calibrate the gas chromatograph used for measuring the amount of alcohol in blood samples.[200] The procedure for the proper use of the machine is also important. In *Castle v Cross*, the UK court described the eleven steps in the correct procedure for using an Intoximeter to measure the alcohol in the subject's breath sample.[201] In *Reid v DPP*, evidence of the proper calibration and proper usage of the Intoximeter permitted the court to conclude that errors in the printout from the Intoximeter were not related to, and affected by, the computer component of the Intoximeter that analysed breath samples, which was held to be operating and functioning properly.[202]

3.100. It will be evident from the discussion above that the issue of calibration, operation and accuracy may be more acute when the electronic evidence is partly computer-generated and partly computer-stored. In such a case, a witness may have to testify that he has personal knowledge of the subject matter indicated in the electronic record, and that the record is accurate.[203]

---

200 (1979) 21 SASR 569.

201 *Supra*, note 81.

202 (1998) The Times March 6, 1998. "For my part, it seems clear beyond doubt that the Crown Court was entitled to conclude that the computer part of the Intoximeter was operating and functioning properly. The necessary calibration checks and purges had been properly carried out and the readings displayed on the screen after the appellant had provided specimens of breath were the same as those on the printout subsequently produced. All this is a matter of factual finding in the Crown Court. In the circumstances, the Crown Court was entitled to conclude that the abnormalities in the printout were unconnected to the operation of the computer part of the Intoximeter and that the abnormalities of parts of the typeface of the printout were not related to the storage, processing and retrieval of information by the computer."

203 *Gosser v Commonwealth of Kentucky* 31 S.W.3d 897, 903 (Ky. 2000). The witness must explain how two and three-dimensional computer-generated diagrams of the crime scene could purport to show scale and measurements, how such measurements were made or obtained and how they were inputted into the computer. A similar approach is taken in relation to demonstrative evidence. See s 68A, Evidence Act which requires "any fact or opinion asserted in any [computer-generated] material" to be "proved by relevant and admissible evidence, and if such fact or opinion is

3.101. *Chronology*. The chronology of electronic evidence is as much about relevant date and time information related to the evidence (such as when it was accessed, when it was modified, when it was last saved) as it is about the sequence (whether it was accessed before or after another document).[204] It may also be pertinent in con-junction with other issues of authentication, *e.g.* on issues of integrity, accuracy and chain of evidence, the lapse of time between the input of the data, the operation of the computer and the generation of the printout will be highly relevant in a determination of these issues.[205] However, in many other cases, such as *R v McKeown*, the issue of chronology in relation to the quality of the evidence is not relevant because extrinsic evidence proves it to the contrary.[206]

Classes of Electronic Evidence

3.102. Our review of the jurisprudence in this area shows that the courts have adopted slightly different approaches in relation to authentication issues when admitting different types of electronic evidence. These may be classified as business records, personal computer records and email and other Internet records.

---

one that is admissible only on the proof of some other fact or opinion, such last-mentioned fact or opinion must be proved before evidence is given of the fact or opinion first-mentioned."

204 In some instances, the chronological sequence as an issue of authentication is more important than the actual timing itself. See *DPP v Ward*, *supra*, note 109.

205 See, for instance, *Ler Wee Teang Anthony v PP* [2002] 2 SLR 281. In this case, the communications was done between the parties on the same premises on presumably two different computers. The issue of the chronology of the communications will be more pertinent if the parties were not in actual physical proximity when they communicated.

206 In *R v McKeown*, *supra*, note 108, it was held that the discrepancy between the time shown on the printout and the actual time did not affect the Intoximeter's alcohol readings.

Business Records

3.103. Courts have appeared to accept electronic evidence business records much more readily than other forms of electronic evidence. Where such records have been admitted pursuant to the business records exception to the hearsay rule, the courts have also been prepared to rule positively on the issue of authentication. Parties usually challenge business records on three different bases:

- that they were altered, manipulated or damaged after they were created,
- that the computers or computer programs are not reliable, or
- that origin and authorship of these records are unknown.[207]

3.104. These authentication issues have been handled differently by the courts, depending on whether the electronic business records are hearsay records or are computer-generated records.

3.105. Business records of statements made by persons who are unavailable to give evidence are hearsay and may be admitted if they are made in the course of business. Section 32(b) states:

> **Cases in which statement of relevant fact by person who is dead or cannot be found, etc., is relevant**
>
> 32. Statements, written or verbal, of relevant facts made by a person who is dead or who cannot be found, or who has become incapable of giving evidence, or whose attendance cannot be procured without an amount of delay or expense which under the circumstances of the case appears to the court unreasonable, are themselves relevant facts in the following cases:
>
> *or is made in course of business*;
>
> (b) when the statement was made by such person in the ordinary course of business, and in particular when it consists of any entry or memorandum made by him in books kept in the ordinary course of business or in the discharge of professional duty, or of

[207] DOJ Report, *supra*, note 172, at 144-145.

> an acknowledgment written or signed by him of the receipt of money, goods, securities or property of any kind, or of a document used in commerce, written or signed by him, or of the date of a letter or other document usually dated, written or signed by him;

3.106. To be admissible business records, such electronic records must be made "in the ordinary course of business" "in the discharge of a professional duty" or must be some other document used in a system of commerce such as acknowledgments for moneys, goods, securities and properties. They may also include the dates of documents usually dated, written and signed by the maker of such documents. It is the routine and regularity of this conducted practice followed by the maker of the statement that gives the assurance of reliability of such records. As Phipson on Evidence states, "The grounds of reception are … the presumption of truth which arises from the mechanical and generally disinterested nature of the entries made in the ordinary course of duty, and from their constant liability, if false, to be detected by the declarant's superiors."[208] Furthermore, business operations depend on this regularity to ensure that their records are not altered, manipulated or damaged. For this reason, the business records exception in section 32(b) applies only to those records made "in the ordinary course of business".[209] Transactions of an exceptional kind are excluded from the ambit of section 32(b).

3.107. The US courts have adopted the approach of waiving or relaxing the requirement of authentication where the electronic records sought to be admitted are business records. "[C]omputer business records have a greater level

---

208 Phipson, *supra*, note 2, at 844.

209 In *Vaynar Suppiah v KMA Abdul Rahim & Anor* [1972-1974] SLR 239, [1974] 2 MLJ 183 a surveyor's report assessing damage to the shipping cargo was adduced in evidence by bill of lading holders. It was held not to be made "in the ordinary course of business" because this was not part of the business of the holders. What should have been admitted were the field survey reports made by the holders themselves when they inspected the cargo.

of trustworthiness than an individually generated computer document."[210] In *US v Salgado*, the prosecution sought to admit in evidence as business records the telephone toll records to prove the telephone numbers were subscribed by the accused and his accomplice, a situation not unlike that in *R v Spiby*. The defence challenged their admissibility, contending that evidence should be adduced to show that the computer system was sufficiently accurate. The US 6th Circuit Federal Court said:

> The government is not required to present expert testimony as to the mechanical accuracy of the computer where it presented evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business… The record indicates that Mr. Deering [witness from the telephone company] testified that South Central Bell relied on these computer-generated records to ensure the accuracy of its billing. He was not required to testify concerning any programming features which were in place to guarantee accuracy.[211]

3.108. As the telephone company itself relied on the accuracy of its own computer system for recording subscription numbers and their tolls for billing purposes, its records are, in a sense, "self-authenticating". Here, there is a sufficient basis for the presumption *praesumuntur omnia rite esse acta* to apply because of the convergence between the requirements of the business records exception to the hearsay rule and the requirements of authentication. It is difficult to fault this pragmatic approach taken by the US courts, subject only to the observation that where there is a manifest error in the electronic records, this presumption of the proper operation of computer systems for purposes of business must surely be rebutted, and authentication evidence must be called for. For reasons explained above, telephone toll records are unlikely to be hearsay, but are

---

[210] *The People of The State of Colorado v Huehn*, 53 P.3d 733, 737 (Colo. App. 2002).

[211] 250 F.3d 438 (6th Cir. 2001). See also *US v Linn*, 880 F.2d 209, 216 (9th Cir. 1989), *US v Briscoe* 896 F.2d 1476, 1494-1495 (7th Cir. 1990), *US v Miller* 771 F.2d 1219, 1237 (9th Cir. 1985), *US v Cestnik* 36 F.3d 904, 909-10 (10th Cir. 1994), *US v Goodchild* 25 F.3d 55, 61-62 (1st Cir. 1994), *US v Moore* 923 F.2d 910, 914 (1st Cir. 1991), *US v Briscoe* 896 F.2d 1476, 1494 (7th Cir. 1990), *US v Catabran* 836 F.2d 453, 457 (9th Cir. 1988).

better treated as computer-generated records and thus real evidence.[212]

3.109. Section 34 of our Evidence Act, which deals with the admissibility of account books where they are "regularly kept in the course of business", will, for the same reasons, satisfy the authentication requirements of accuracy. Of course, this does not preclude the court from calling for evidence to establish the reliability of the computer system, especially where the records are a mixture of raw data input into the system and data calculated according to a programmed formula from raw data.[213]

3.110. With electronic business records that are computer-generated and would be admitted as real evidence or direct evidence, the evidential safeguards available to admit hearsay business records do not apply. One court claims that computer-generated records "would be even more reliable than ... average business record(s) because they are not even touched by the hand of man."[214] It is submitted that the issue here is not so much the alteration, manipulation or damage to the records: the automated nature of such records will make such changes difficult, but not impossible. The real issue is the reliability of the computer systems and the computer programs therein. Authentication is still required.[215]

3.111. However, again, depending on the nature of the businesses operations, the courts may be more inclined to accept such business records on the basis that they are reliable enough to be relied upon by the businesses for their crucial

---

212 See DOJ Report, *supra*, note 172, at 151.

213 See *Transport Indemnity Co. v Seib* 178 Neb. 253, 132 N.W.2d 871 (1965). See also *Lim Mong Hong v PP, supra*, note 31 which also dealt with and admitted account books. The accused who opposed the admission of the evidence challenged it on the basis that it constituted multiple hearsay. Another way to mount the same challenge is to contend that the accounting entries that were made were not "regularly kept …in the course of business".

214 *US v Vela* 673 F.2d 86 (5th Cir. 1982).

215 See *United States v De Georgia* 420 F.2d 889 (9th Cir. 1969).

operations. Bank transaction records[216] and telephone toll records[217] have been given this more relaxed treatment. However, this approach does not apply to all business records. To illustrate, in the case of *People v Lugashi*, the court observed that banking records of credit card account transactions prepared in the regular course of banking business in accordance with banking regulations are in a different category from ordinary business and financial records of a private enterprise.[218] The court took the view that in relation to the former class of business records the level of assurance provided is higher because of the general business and market reliance on these records and the spectre of regulatory sanction. Further reliability is lent to the evidence because such records are often produced by an independent third party who is not a party to the proceedings nor is interested in the outcome of the proceedings.[219]

3.112. But this does not mean that business records may not be successfully challenged, even if the organisation relies upon such records for its own purposes. For instance, in *R v Plymouth City Council and Plymouth Magistrates' Court, ex parte Johns*,[220] the court heard evidence that the Council was transitioning to a new computer system for calculating community charges, and there was an internal report circulated within the Council admitting that the computer programs for the new system were not operating properly. The same report also documents inaccuracies from the system arising from complaints from over-charged payers. On this basis, the court had no difficulty quashing the convictions of the accused for not paying the community charges, as serious doubts had been raised about the

---

216 *State v Veres* 436 P.2d 629, 637 (Ariz.App. 1968), *People v Lugashi* 205 Cal. App. 3d 632, 252 Cal. Rptr. 434 (Cal. Ct. App. 1988), *United States v. Moore* 923 F.2d 910 (1st Cir. 1991).

217 *Supra*, note 214.

218 *People v Lugashi, supra*, note 216.

219 *Ibid*, at 641.

220 *R v Plymouth City Council and Plymouth Magistrates' Court, ex parte Johns* (27 October 1994, unreported).

reliability of the printout which ostensibly documented the accused's unpaid charges. The point made here is that where the risk-tolerance level for such computers is very low, the presumption that they are operating properly may be easily rebutted by some evidence of a material error in the computer system.

3.113. Because the focus is on the regularity of the business operations as proof of the authenticity of business records, both the UK and the US courts have adopted a less strict approach with regards to the qualification of the witnesses testifying as to these records. In *R v Spiby*,[221] the court did not require the testimony of a programming expert, but was satisfied with the assurance from the manager that the computer recording calls made from the hotel rooms was operating reliably. In *US v Vela*,[222] the court accepted testimony from an employee of the telephone company who was described as a custodian of the telephone records that the records were prepared in the usual course of the company's regularly-conducted business activity and vouched for the general reliability of the process, though he was unable to identify the brand, type and model of each computer or to vouch for the working condition of the specific equipment during the billing periods. In *People v Lugashi*, the court held that testimony of computer experts was not necessary where the data retrieved were based on automated processes rather than manual entries: all that was required was testimony from an individual who knew the process and worked with the records generated.[223] Similarly, in *R v Shepherd*,[224] a store detective was allowed to testify that the central computer to which

---

221 *Supra*, note 82.

222 *Supra*, note 214.

223 *Supra*, note 216, at 640. The witness need not have actual personal knowledge of the operation of the hardware and software, and may acquire some aspects of her knowledge through hearsay. Otherwise, "only the original hardware and software designers could testify since everyone else necessarily could understand the system only through hearsay" (at 641).

224 *Supra*, note 54.

the tills were connected was operating properly. In all these cases, lay witnesses, not computer experts, were permitted to testify to the general business operations that produced the electronic records.[225]

3.114. Of course, where there is evidence to suggest that the assumption of proper business operations is untrue, the court may call for expert evidence and subject these computer systems to much closer scrutiny. The assumption that business records are generally reliable does not obviate the need to address other authentication issues not related to the reliability of the records, such as identification of duplicate records (unfortunately, still a common business occurrence), attribution and chain of evidence (records from different businesses may become mixed up) and chronology (some businesses practice less strict time keeping standards).

Personal Computer Records

3.115. Personal computers and personal digital assistants are nowhere as reliable as business systems. They are used in a very different operational environment, both from hardware and a software standpoint as well as usage standpoint. Personal computer records are generally not secure. Home users share computers, either through the Internet or via peer-to-peer networking programs, share files and resources with other users, some unknown and unidentifiable, over the Internet. Serious issues may be raised about the integrity and reliability of such systems and the evidence therein.

3.116. These, and additional considerations arising from chain of evidence issues, arose in the case of *US v Whitaker*.[226] In this case, the prosecution introduced evidence of the drug

---

225 In *Lugashi*, *supra*, note 216, at 640 the court wanted to avoid the necessity of producing "a horde of witnesses representing each department of a company's data processing system, not to rebut an actual attack on the reliability of their data, but merely to meet the minimal requirement for admissibility".

226 127 F.3d 595 (7th Cir. 1997).

transaction records implicating the accused that prosecutor experts had extracted from his accomplice's computer, with the assistance of the accomplice, while it was in police custody. Defence counsel had objected to its admissibility, contending that the prosecution failed to provide foundation for a proper chain of evidence, from the seizure of the computer to the production of evidence in court. Defence counsel also claimed that the accomplice could, "with a few rapid keystrokes", have added the accused's alias to the electronic records in order to implicate the accused.

3.117. While the objection is in principle sound, on the facts, this was met somewhat by evidence of prosecution's police witness who had witnessed the accomplice's operation of his computer and the retrieval of the records. The US Federal Court called this a "wild-eyed speculation" on the part of the accused,[227] and refused to reverse its admission. More importantly, in the *Whitaker* case, the police witness testified but was not cross-examined on this point. On the record, there was clearly no evidence to support the accused's allegation, which was thus dismissed by the court. But this case does illustrate the poor practice of the prosecutor in allowing an accomplice who has obviously his own interests to protect to access the accused's computer system that had previously been secured by the police. This case should not be seen as condoning such a practice. It would have been better if access to the seized computer was conducted by a neutral third party, for purposes of retrieving the relevant records.

Email and Other Internet Records

3.118. For email and other electronic communications records, the primary issue of authentication is attribution.

3.119. The US courts have generally admitted in evidence email,[228] Internet postings[229] and chat room records.[230] However,

---

227 *Ibid*, at 602.

228 E.g. *US v Siddiqui* 235 F.3d 1318 (11th Cir. 2000).

the courts have rejected such records where the proponent is unable to properly authenticate their origins. An email tendered in evidence to show an admission by the accused is relevant only if the email did originate from the accused as the author. Similarly, a defamatory Web posting tendered to show an inflammatory libel by the defendant group is only admissible if the posting was proved to be made by the defendant.[231]

3.120. In the absence of witnesses and self-authenticating measures such as electronic signatures (described above), authenticating the authorship of these records is often achieved by way of authenticating the machines that produced these records. In the computing environment, the "what" is often used to circumstantially identify the "who". To prove that the email originated from the sender, the IP address of the transmitting computer is extracted from the email header and matched against the IP address of the sender's computer. However, this is not always possible. The accuracy of this process depends on the co-operative operations of the intermediate computers (the mail servers) transmitting the email. Mail servers may be hijacked and reprogrammed to falsify the email headers and thus the originating addresses of these messages. In an open network environment, the intermediate communications and computing devices are not within the exclusive control of either the sender or the recipient of the electronic messages. Thus, spammers use this technique to send unsolicited messages from unprotected school computers, thereby getting around spam filters designed to block messages originating from the spammers' machines.[232] It may be a truism to say that one should not rely on the email header solely to prove that the email

---

229 E.g. *US v Jackson* 208 F.3d 633 (7th Cir. 2000), *St. Clair v Johnny's Oyster & Shrimp, Inc.* 76 F.Supp. 2d 773 (S.D. Tex. 1999).

230 E.g. *US v Simpson* 152 F.3d 1241 (10th Cir. 1998), *US v Tank* 200 F.3d 627 (9th Cir. 2000).

231 *United States v Jackson*, *supra,* note 229.

232 See http://straitstimes.asia1.com.sg/techscience/story/0,4386,191206,00.html? (visited 26 May 2003).

came from the originator because the email shows that it has originated from his email address.

3.121. In this regard, the presumptive rules of attribution in section 13 of the Electronic Transactions Act offer some assistance. But an unsolicited email from a previously unknown party is unlikely to satisfy any of the rules in section 13. The recipient has no knowledge as to whether it was actually sent by the originator, or was sent with his authority, or from a computer system programmed by the originator. There does not exist any prior attribution procedure, nor is the recipient aware of any relationship between the originator and his agent that made the email possible. However, outside of section 13 of the Electronic Transactions Act, attribution may be established via other means. A timely acknowledgment to a previously transmitted message (the "reply letter doctrine")[233] can provide evidence of its origination. For instance, if B had previously sent an electronic message to A with a certain request, proof of the origination of the reply as being that from A may be inferred from the fact that A replied in answer to B's prior request or that A referred to B's prior request in his reply, just as A's reply constitutes an implied acknowledgment of his receipt of B's message.[234]Of course, the assumption here is that the first message was reliably transmitted to A.[235] Furthermore, to support this inference, it must be shown that only A had access to messages sent by B to that email account, and that only A could use that email account to reply to his messages. It is not uncommon for email accounts to be shared or hijacked or access passwords to be circulated. Foundation evidence to admit email must meet all these challenges.

3.122. Attributing postings or IRC conversations to their originator or publisher is more difficult, since many of

---

233 McCormick, *supra*, note 182, at 51. See, *inter alia*, *Washington v State* 539 So.2d 1089 (Ala.Crim.App. 1988), *Milner Hotels, Inc. v Mecklenburg Hotel* 256 S.E.2d 310 (N.C.App. 1979).

234 S 14(5), Electronic Transactions Act.

235 McCormick, *supra*, note 182, at 51.

these electronic services permit their subscribers to assume an alias, or even make anonymous postings.[236] The most pertinent information about postings will be stored on the originator's computer. Access must be had to that computer's records for information such as the date and time of the posting, and any information such as the originator's IP address which will allow the proponent to verify the origin of the posting.

3.123. The proponent may be assisted in this regard if records of the posts are stored on the originator's computer system or if the originator's computer system yields indicia of information peculiar to the parties to the conversation or the contents of the conversation itself. In the case of *US v Simpson*,[237] prosecution found on the accused's computer, records that listed the name, address and telephone number that the undercover agent had sent to one "Stavron". This strengthened the inference that "Stavron" was the alias used by the accused, and that the conversation conducted by the undercover agent was with the accused. Some proponents have taken to securing Internet log in records from ISPs to show that the originator was online at the instant moment. Other ISP logs may provide more detailed information such as the sites visited by the various subscribers at the various times. Of course, some posting forums implement editorial policies which permit the forum editors to exercise editorial control or even delete various postings. These will clearly make the process of authenticating such postings even more difficult.

3.124. All in, while electronic communications records pose special challenges for authentication, these challenges are not insurmountable.

---

236 IRC conversations are much more difficult to attribute, since most of these conversations take place in real time, bypass most intermediate computers and are not recorded or stored anywhere.

237 *Supra*, note 230.

Avoiding Authentication

3.125. Generally, the proponent of the electronic evidence always has the legal burden to authenticate the evidence. Where the proponent of the evidence has adduced some evidence to authenticate the evidence, the evidential burden lay on the opponent to refute the authentication evidence. In many instances, the opponent has not refuted the authentication evidence because it has not provided a foundation for raising an issue as to the authentication evidence.[238] Thus, in *R v McKeown*, the defence sought evidence of the Intoximeter's circuit diagram to prove that the inaccuracy of the time reading did have some effect on the breath analysis. The court rejected the application.[239] If defence counsel had supported that application with expert evidence from an engineer that the circuit diagram will definitively show how the time keeping component was linked to the breath analysis component, thus rebutting the proponent's expert's empirical observation, there would be no reason for the court to reject the application.

3.126. The discussion above on authentication demonstrates that as the precondition for the admission of all items of evidence, formal proof of authentication may be difficult if not troublesome, time consuming and quite unnecessary in cases where there is no legitimate doubt concerning the evidence. In practice, formal proof of authentication is largely avoided.

3.127. In civil proceedings, formal proof is avoided by way of the practice of the parties collating an "agreed bundle". The agreed bundle dispenses with formal and strict proof of provenance of a document. Modern discovery and interrogatories substantially eliminate many concerns of authenticity. By putting non-contentious documents in an agreed bundle, the parties generally intend that it will not be necessary to prove the documents existence and

---

238 See *e.g. US v Whitaker*, *supra*, note 226.

239 *DPP v McKeown*, *supra*, note 108.

execution, or the need to produce the original.[240] In so doing, parties agree that authentication issues of integrity and attribution are no longer in issue. And as facts admitted, they need not be proved.[241] But parties may nonetheless include two different versions of the same document in the agreed bundle. In such a case, it is still necessary to prove the contents of the document – only proof of due execution is dispensed with.[242]

3.128. Although there is no mechanism for an "agreed bundle" in criminal proceedings, authentication issues are often informally waived by the opponent informally, as where the opponent does not seek to challenge the admissibility of the evidence when it is first tendered in court. Of course, where doubt arises as to whether the opponent has really waived his rights to challenge the authenticity of the evidence, the court generally gives the opponent the benefit of the doubt. But, as explained above, after the proponent has tendered some authentication evidence, the opponent has to discharge his evidential burden to put authentication in issue.

The Best Evidence Rule and "Originals" of Electronic Evidence

Rationale for the Best Evidence rule

3.129. The need to produce original copies or primary evidence of documents such as writings, recordings and photo-

---

240 *Butterworths Annotated Statutes of Singapore*: *Evidence*, Vol 5, *supra*, note 103, at 181. The effect of including the documents in the agreed bundle is to be decided by the parties: Supreme Court Practice Directions (1997) Practice Directions Nos 3 and 4 of 1993 (High Court and Subordinate Courts), Part VI, para 34(3)(a)) and Subordinate Courts Practice Directions (1997), Part VI, para 34(3)(a).

241 S 60, Evidence Act, although the learned commentator to this section questioned if s 60 was the relevant provision for admitting documents without proof, and observed that s 60 was more applicable to the formal admission of facts and formal admissions in writing.

242 *Butterworths Annotated Statutes of Singapore*: *Evidence*, Vol 5, *supra*, note 103, at 181.

graphs in court is a well-entrenched rule. Section 66 states that documents must be proved by primary evidence unless the documents fall within an exception to the rule. Copies of the original documents – secondary evidence – may only be admitted in circumstances spelt out in section 67. Among the exceptions are: when the original is in the possession or power of the opponent, [243] when the opponent admits of the existence, conditions or contents of the original,[244] when the original has been destroyed or lost,[245] when the original is of such a nature as not to be easily movable,[246] when the original is a public document,[247] when the copy is a certified copy of the original permitted in law,[248] or when the original consists of numerous documents which cannot be conveniently examined in court.[249]

3.130. The rule has been variously justified: as part of the best evidence rule,[250] the prevention of fraud,[251] or the importance of the written word.[252] The concern is that the courts should be presented with the original versions of the documents, given the centrality of construction of words in deeds, wills or contracts, and the possible errors that may be introduced through copies of writings or even oral testimonies of writings.[253]

---

243 S 67(a), Evidence Act.

244 S 67(b), Evidence Act.

245 S 67(c), Evidence Act.

246 S 67(d), Evidence Act.

247 S 67(e), Evidence Act.

248 S 67(f), Evidence Act.

249 S 67(g), Evidence Act.

250 Thayer, *Preliminary Treatise on Evidence at the Common Law,* at 489 (1898).

251 §§ 1177-1282, Wigmore, Volume IV (Chadbourn Ed, 1972), *Governor of Pentonville Prison, ex p Osman* (1990) 90 Cr App R 281, *Kulasingam s/o Samuel v Rasamah d/o JV Thambipillai* [1997] 1 MLJ 288.

252 Morgan, *Basic Problems of Evidence* 385 (1962).

253 McCormick, *supra*, note 182, §231, at 62.

Application to the Electronic Environment

3.131. But in the day and age of improved reprographic techniques such as photocopying machines, coupled with avenues for discovery and pre-trial assessments of documents, including originals and copies of documents, the "best evidence" rule looks to be increasingly anachronistic.

3.132. Under our laws, all electronic "copies" including electronic records will be classified as secondary evidence.

> **65. Secondary evidence means and includes —**
>
> (a) certified copies given under the provisions hereinafter contained;
>
> (b) *copies made from the original by electronic, electrochemical, chemical, magnetic, mechanical, optical, telematic or other technical processes, which in themselves ensure the accuracy of the copy, and copies compared with such copies;*
>
> (c) copies made from or compared with the original;
>
> (d) counterparts of documents as against the parties who did not execute them;
>
> (e) oral accounts of the contents of a document given by some person who has himself seen it.
>
> *Illustrations*
>
> (a) A photograph of an original is secondary evidence of its contents, though the two have not been compared, if it is proved that the thing photographed was the original.
>
> (b) A copy compared with a copy of a letter made by a copying machine is secondary evidence of the contents of the letter if it is shown that the copy made by the copying machine was made from the original.
>
> (c) A copy of a document in the form of a print-out, or image on a monitor screen, retrieved from a magnetic or optical storage device, such as a tape, hard disk, laser disc or CD-ROM, is secondary evidence of the contents of the document if it is shown that the copy retrieved from the storage device *satisfies the conditions providing for the admissibility of such output.*
>
> (d) A copy transcribed from a copy but afterwards compared with the original is secondary evidence, but the copy not so compared is not secondary evidence of the original, although the copy from which it was transcribed was compared with the original.

> (e) Neither an oral account of a copy compared with the original nor an oral account of a photograph or machine-copy of the original is secondary evidence of the original.
>
> [our emphasis]

3.133. These changes to section 65, made in 1996, were intended to remove the doubt that secondary evidence includes "micro-films, photographs and photocopies of original documents and copies captured by document image processing systems".[254] But while the changes extended the concept of "mechanical process" to include electronic processes, the changes also potentially widened the scope of section 65 to encompass electronic copies of electronic records. In this regard, two very different interpretations of the application of section 65 to electronic copies of electronic records are possible.

3.134. In the first interpretation, section 65 is displaced by the rule in section 35, in particular, section 35(10). As illustration (c) to section 65 states, it has to be proven that "the copy retrieved from the electronic record" satisfies the conditions providing for the admissibility of such output. This seems to allude to section 35(10)(b), which states that "computer output tendered in evidence under [section 35] and duly authenticated shall not be inadmissible as evidence of proof of the contents of the original document merely on the ground that it is secondary evidence". Thus under this approach all copies from electronic records are "perfect" copies once they are admitted pursuant to section 35. The concept of an "original", which connotes that copies are inferior, is generally of little application in the electronic environment.[255]

---

254 Explanatory Statement, *supra*, note 28.

255 The exception will be the use of copy-protection technologies to prevent intellectual property infringement, which is becoming increasingly widespread. See *e.g.* Art 11, WIPO Copyright Treaty, Art 18, WIPO Performances and Phonograms Treaty, Art 16.4(8), US-Singapore Free Trade Agreement, s 1201, US Digital Millennium Copyright Act 1998 and Art 6, EC Directive on the Harmonisation of Certain Aspects of Copyright

3.135. In the second interpretation, section 65 preserves and retains the application of the best evidence rule to electronic evidence. In other words, where an electronic copy of an electronic record is made it must still be shown to be a "copy" of the "original" electronic record.[256] This may be established where it is proved that the reproduction process "ensures the accuracy of the copy".[257] This approach finds some similarity with the approach taken by the US Federal Rules of Evidence, which does preserve the distinction between primary and secondary evidence for electronic evidence.

3.136. Rule 1001 of the Federal Rules of Evidence reads:

> (3) Original.—An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. *If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".*
>
> (4) Duplicate.—A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, *or by mechanical or electronic re-recording,* or by chemical reproduction, *or by other equivalent techniques which accurately reproduces the original.*
>
> [our emphasis]

3.137. However, while preserving the distinction, the Federal Rules of Evidence accepts that an "electronic copy" is an original where it "reflects the original data accurately" but where it merely accurately reproduces the original, it will be a duplicate or a "copy". In the former, the emphasis is placed on the accuracy of the contents – the data. In the latter, the emphasis is placed on the accuracy of the duplication technique. So generally speaking, electronic copies of electronic records and printouts made from

---

and Related Rights in the Information Society ('Copyright Directive') (Directive 2001/29/EC).

256 Notwithstanding the language of s 35(10)(b), Evidence Act.

257 S 65(b), Evidence Act.

those records will be originals,[258] because there is an assurance that the electronic duplication process will reflect the data accurately – if not exactly. But where there is no such assurance[259], the copy that is made is a "duplicate". Thus in *United States v Edgemon*,[260] the printouts of computerised call records were held to be admissible as "original evidence" for listing the calls made by the accused, or alternatively a "duplicate" ("secondary evidence") as being reproduced from the original electronic call records.

3.138. The approach taken under the Federal Rules of Evidence is sensible, technologically neutral and forward looking and we submit, may be usefully adopted into our Evidence Act to clarify the issues regarding the application of the secondary evidence rule to electronic evidence.

Q. Should the best evidence rule be retained in relation to electronic evidence?

---

258 *Doe v US* 805 F. Supp. 1513 (D.Haw. 1992), *Laughner v State* 769 N.E.2d 1147 (Ind. Ct. App. 2002).

259 For instance, with "lossy" replication techniques implemented pursuant to anti-circumvention technological measures. See also, *supra*, note 255.

260 1997 U.S. Dist. LEXIS 23828, s*upra*, Part II, note 60.

Part IV. Options for Reform

4.1. Having made a case in Part III for the necessity to revise and streamline the provisions of sections 35 and 36 of our Evidence Act and suggesting some legislative models that may be usefully considered, we now turn our attention to explore options for reforming these provisions. In this Part, we discuss four alternate options that may be considered for possible law reform. These options are as follows:

- Option 1. Adopt a non computer-specific approach to admit electronic records.
- Option 2. Adopt a non computer-specific approach to admit electronic records but provide presumptions that facilitate the admissibility of such electronic records.
- Option 3. Adopt a business records approach to admit business records maintained in electronic form.
- Option 4. Retain the existing computer-specific approach but ease the rules of admissibility.

These options are now described in turn.

Option 1. Adopt a non computer-specific approach

4.2. This approach is based on the principle of non-discrimination, which requires that electronic evidence be treated no differently from evidence not in electronic form. As explained in Part III, this is one of the fundamental principles of the UNCITRAL Model Law on Electronic Commerce, and is actually enshrined in our Electronic Transactions Act.[1] In this approach, we do not envisage that any rules such as those set out in sections 35 and 36 of the Evidence Act would regulate the admissibility of electronic evidence. Instead, the existing rules providing

---

1 Article 9, UNCITRAL Model Law on Electronic Commerce, s 6, Electronic Transactions Act.

for the relevancy and admissibility of evidence will apply to admit electronic evidence in the same manner as any other item of evidence.

4.3. Under this approach, where an electronic record is tendered as evidence of the facts stated therein, the existing rules of evidence in the Evidence Act such as hearsay, the best evidence rule and rules on authentication will regulate its admissibility. If an electronic record is real evidence, the rule against hearsay will not apply as it will be admissible at common law. This distinction between electronic records as "stored records" and as "generated records" is well recognized at common law. As Part III illustrates, no legal difficulties exist in the application of rules of hearsay and of real evidence to electronic evidence.

4.4. Part III also illustrates that the existing common law rules of authentication readily apply to electronic evidence. Electronic evidence is characterized by the fact that it may be more vulnerable to undetected tampering and unauthorized manipulations. But authentication evidence such as proof of identification of the evidence, maintenance of a chain of evidence, proper integrity, attribution to individuals and machines, proper calibration, operation and accuracy of the electronic device and proper chronology of the evidence will go a very long way towards addressing these concerns. Of course, the resolution of these authentication issues may be facilitated by the use of technologies such as data encryption and digital signatures to secure such electronic records. In fact, the Electronic Transactions Act recognises this by way of various presumptions as to the attribution and integrity of electronic records secured through the use of secure electronic signatures.[2]

4.5. This technology-neutral approach only admits of one apparent derogation, and that is in relation to the best evidence rule. The concept of an "original document" is already of little or no relevance in this era of perfect or

---

2 See, *e.g.* s 18, Electronic Transactions Act.

near-perfect reprographic processes for documents.[3] It is of even less relevance when applied to electronic records as documents since, as Part III explains, electronic copies are, for the most part, identical and perfect.[4] Under Option 1, the law in this regard will be revised to recognize that electronic copies that are shown to reflect the data accurately are "original evidence", whereas those copies that only reproduce the original in an accurate fashion but that are not electronically identical to the "original" will be treated as "secondary evidence".[5]

4.6. This approach deviates from the existing rule in section 35(10) of the Evidence Act, which treats all computer output authenticated in the manner as prescribed in section 35 as "originals" even though they are admitted as "evidence of proof of the original document". As previously explained, most but not all electronic copies are to be equated with "originals".[6] In this regard, we are of the view that the approach advanced above, similar to that embodied in Rules 1001(3) and 1003 of the US Federal Rules of Evidence, is the correct approach to take. In reality, it is a technologically-neutral approach, as the emphasis is not on characterizing the form of the copy, but on the process that is used to produce the copy.

4.7. Ultimately, the approach envisaged under Option 1 calls for an enlightened judicial assessment of electronic evidence to address these issues of hearsay, authentication and best evidence. By giving the courts a wide discretion to call for evidence to authenticate the electronic evidence in any manner that the court deems appropriate, and not prescribing, unlike the current regime in section 35, express requirements that the proponent of the electronic evidence has to satisfy before the evidence can be considered for admissibility, full flexibility is preserved. So where the electronic evidence is from an extremely reliable

---

3 *Supra*, Part III, para 3.134.

4 *Supra,* Part III, paras 3.131 - 3.135.

5 *Supra*, Part III, para 3.137.

6 *Supra,* Part III, paras 3.131 - 3.135.

and trustworthy source or there is hardly any room for dispute or debate that it is unreliable, the court should be more receptive to admit the evidence with little if any supporting evidence to authenticate the electronic evidence. On the other hand, where the electronic evidence is from a questionable source, or is prepared *ad hoc* or pursuant to proceedings between the parties, the court may require clear and unequivocal evidence to authenticate the electronic record. To illustrate, let us assume the proponent wishes to tender in evidence an electronic banking or telecommunications record. The court examines the record and discovers a manifest error on the record. Where a manifest error appears in an electronic record that was previously assumed to be reliable and trustworthy, any *prima facie* assumptions of reliability and trustworthiness must be displaced, and the court, just as the opponent, may call for clear and unequivocal authentication evidence. The nature of the authentication evidence required will, of course, depend on the nature of the authentication issue. In a case of a manifest error in an otherwise trustworthy electronic record, the court may call for evidence such as the source of the information, the accuracy and reliability of the data input and processing system, and in some instances, even the security of the electronic system if it is networked or where unauthorized access to it is suspected.[7]

4.8. Option 1 does not envisage any specific provisions to deal with considerations of weight of electronic evidence, since in our opinion such issues will be dealt with adequately as issues of authentication. In any event, even if an item of electronic evidence is found to be authentic, it is always open to the court to ascribe it very little weight, if at all, if, for instance, it is contradicted by other, more reliable evidence.[8] Option 1 does not seek to constrain the court in the exercise of this judicial function, just as the current section 36 gives the court much leeway in assessing the

---

7 *Supra,* Part III, paras 3.108 - 3.112.

8 *Supra*, Part III, para 3.80.

evidence, preferring instead to rely on submissions from counsel and general judicial awareness of advancements and limits of technology to deal with these issues.[9]

4.9. Adoption of such a generic non-computer specific approach offers several advantages as compared to a computer-specific approach. Firstly, this approach as envisaged in Option 1 pledges close allegiance to the non-discrimination principle.[10] Secondly, a technology-neutral approach allows the rules of evidence to embrace any technology changes that may occur in the future. Thirdly, its simple yet flexible stance regarding authentication frees the courts from the shackles of examining the nuances of pre-admissibility conditions and instead allows the courts to concentrate on the real issues – the strengths and weaknesses of the tendered electronic evidence. This is the approach taken in the US, under the Federal Rules of Evidence, as well as in the UK, after the series of reforms made to the hearsay rule in both civil and criminal proceedings. The conspicuous absence of any computer-specific provisions dealing with the admissibility of electronic evidence does not seem to have hampered in any way the use and admissibility of electronic evidence in these jurisdictions. In fact, as Part III demonstrates, US jurisprudence is replete with illustrations of the admissibility of electronic evidence such as email, chat records, electronic business records and even personal electronic records.[11]

4.10. Of course, one has to accept that such an approach does not afford any statutory guidance among the business, legal and judicial community as regards the proper use and admissibility of electronic evidence. However, as electronic evidence becomes more widely used and accepted, many of these concerns will dissipate. It is our opinion that the circumstances today are different from those in 1995, when the amendments to the Evidence Act to cater to the

---

9 *Lim Mong Hong v PP* [2003] 3 SLR 88.

10 *Supra*, Part III, paras 3.18 - 3.23.

11 *Supra*, Part III, paras 3.102 - 3.112.

admissibility of electronic evidence were first mooted. The improvements in computing interfaces and the proliferation of personal electronic devices such as PDAs and handphones, not to mention the near ubiquity of PCs and laptops, have further narrowed the gap between the technologists and the users of technology.

4.11. We are of the opinion that Option 1 be carefully considered for adoption in view of the significant advantages that follow from this approach. Adopting such an approach will broadly entail making the following changes to the Evidence Act:

- Repeal the computer-specific provisions (sections 35 and 36) as well as the computer-specific definitions (in section 3) of the Evidence Act.
- If necessary, expand the scope of the term "document" defined in section 3 of the Evidence Act to include electronic records,[12] or redefine the term "evidence" to include such "electronic records".[13]
- Modify the best evidence rule in the Evidence Act (sections 35(10), 65 and 66) to require the production of "original" copies of electronic documents where the copies are electronically identical to the "original", but admitting such "copies" only where the reproduction measures reproduce the "original" in an accurate fashion.

Option 2. Adopt a non computer-specific approach but provide presumptions to facilitate the admissibility of electronic evidence

4.12. The approach proposed as Option 2 is similar to the proposed Option 1 wherein we accept that the rules of evidence should not contain any provision explicitly providing for the admissibility of computer output. However, unlike Option 1, we recommend the use of specific

---

12 Malaysian Evidence Act 1950, s 3. See also, *supra*, Part II, para 2.107.

13 Indian Evidence Act 1872, s 3. See also, *supra*, Part II, para 2.98.

presumptions to facilitate the admissibility of certain types of electronic evidence.

4.13. The objective behind having such presumptions is the recognition that some types of electronic evidence are inherently more reliable than others, and that rules should exist to facilitate their admissibility. More precisely, we envisage such electronic evidence to be those that are more readily authenticated than other types of electronic evidence. Thus the presumptions that we envisage are authentication presumptions.

4.14. Presumptions similar to those that we envisage already exist at common law such as the maxim *praesemuntur omnia rite esse acta*, which is the presumption that mechanical instruments were in order when they were used. In our comparative analysis in Part II, we noted that one of the justifications advanced by the UK Law Commission for the repeal of section 69, UK PACE 1984 is that proponents of electronic evidence in criminal proceedings are able to rely on the common law presumption of the proper functioning of mechanical instruments to cast the evidential burden of proving the reliability of electronic evidence on the opponent of the evidence.[14] We also observed that similar presumptions are to be found in sections 146 and 147, Australian Commonwealth Evidence Act.

4.15. It should be noted that we are proposing evidential and not legal presumptions. In other words, the effect of triggering such presumptions is to cast merely an evidential burden, and not a legal burden, on the opponent of the electronic evidence. The opponent is under no legal obligation to rebut the presumptions. What the presumptions do is to make it easier for the proponent of the evidence to prove the authenticity of his electronic evidence. We do not accept the use of legal presumptions here because the preconditions that trigger the authentication presumptions of electronic evidence are of a lower order than the precise, technical and regulated preconditions prescribed for presuming authenticity, authorship and integrity of secure

14 *Supra*, Part II, note 84, paras 13.13 - 13.14.

electronic records and signatures under the Electronic Transactions Act.[15] Unlike the use of prescribed or commercially reasonable security procedures that provide a high level of assurance of the attribution of authorship, integrity and non-repudiation of electronic records, the preconditions that we envisage are non-technical in nature, and they relate more to ordinary business processes.

4.16. A good example of such evidential presumptions can be found in section 5, Canadian UEEA. Under section 5, there are three alternative presumptions as to the integrity of electronic record systems. ("Integrity" is one of the issues of authentication.[16]) Section 5 provides that the integrity of an electronic record system is presumed where there is (i) evidence that at all material times, the computer system and the record keeping system were operating properly, (ii) evidence that the record was recorded or stored by the opponent of the evidence and thus originated from the opponent, and (iii) evidence that the record was recorded or stored in the usual and ordinary course of business by a neutral third party.[17] Although section 5 UEEA is only intended to deal with electronic records as

---

15 We contend that the presumption in s 18, ETA is a legal presumption because it uses the formulation "it shall be presumed, *unless evidence to the contrary is adduced*." [our emphasis] This requires the opponent of the evidence to adduce contrary evidence to rebut the presumption. A similar approach can be seen in s 10-120 of the Illinois Electronic Commerce Security Act 1999 1999: s 10-120 from which our s 18 ETA is derived. See the Illinois Attorney General's Commission on Electronic Commerce and Crime - Final Report of the Commission on Electronic Commerce and Crime - May 26 1998, Commentaries to s 10-120. On the other hand, the formulation used in s 5, Canadian UEEA is "in the absence of evidence to the contrary". This also suggests that the presumption is of a lower order than the presumption in s 18, ETA. The formulation in s 5 also does not mandate the production of evidence to contradict the presumption: it only envisages the absence of evidence to the contrary, which is a clear formulation for an evidential presumption. Another formulation for an evidential presumption is found in ss 146, 147 Australian Commonwealth Evidence Act which uses the formulation "unless evidence sufficient to raise doubt about the presumption is adduced".

16 *Supra,* Part II, para 2.9.

17 *Supra*, Part II, paras 2.9 - 2.11.

stored records, we are of the opinion that these presumptions deserve very close consideration, because they deal with the most common situations where electronic evidence is admitted as electronic stored records. The first presumption (section 5(a)) embodies the truism that a proponent seeking to adduce the electronic evidence must prove the proper operation of the record keeping system.[18] The second presumption (section 5(b)) similarly recognises this axiom, for it provides that where a proponent seeks to admit an electronic record derived from the opponent's record keeping system, the integrity of the opponent's record keeping system must be presumed as the onus is on the opponent to show that his record keeping system is unreliable.[19] Finally, the third presumption (section 5(c)) provides that where the proponent seeks to admit in evidence an electronic record kept as a business record by a neutral third party, the integrity of the third party's record keeping system is presumed because such a third party has produced the record independently of either the proponent or the opponent to the proceedings.[20]

4.17. Upon closer examination, we are of the opinion that the second and third presumptions of section 5, UEEA, are technology-neutral and apply equally to computer-generated records as well as computer-stored records. Furthermore, we note that the first presumption is not really a presumption as such[21] but more akin to a restatement of the general rule of authentication similar to that in section 35(1)(c) of our Evidence Act. We see considerable elegance and utility in the second and third presumptions and would recommend an adapted version for their

---

18 *Supra*, Part II, para 2.9.

19 *Supra*, Part II, para 2.10.

20 *Supra*, Part II, para 2.11.

21 S 5(a), UEEA uses the formulation "by evidence that supports a finding…" which suggests that some evidence must be adduced to support a finding of the integrity of the electronic records system, whereas ss 5(b) and (c) use the formulation "if it is established".

possible introduction into our Evidence Act, in the form of illustrations to the authentication provision in section 9.

4.18. As for electronic records as computer-generated records, reference may be made to section 146, Australian Commonwealth Evidence Act 1995. Section 146 requires the proponent to prima facie satisfy the court of the accuracy in respect of devices and processes used before the presumption that the device or process will produce the expected outcome may operate.[22] In contrast, section 147 deals essentially with business records that can take the form of electronic stored records, and presume the accuracy of the device used to generate the records where it shown to be used for the purpose of a business.[23] We are of the opinion that the presumptions in section 5, UEEA, are an expanded version of the presumptions in section 147, Australian Commonwealth Evidence Act 1995 and would thus favour the UEEA presumptions. As for section 146, we would recommend its inclusion in our Evidence Act, as an illustration to section 9, although it will merely be a restatement of the common law maxim *praesemuntur omnia rite esse acta*.

4.19. Several advantages ensue from adopting such an approach. Firstly, this approach combines the technology neutrality of Option 1 with the acceptance of the need for specific rules to facilitate the admissibility of electronic evidence in certain circumstances. It achieves this somewhat paradoxical objective by not mandating any formalistic requirement for the admissibility of electronic records but instead focuses on the issue of authentication of electronic evidence.[24] Thus, a court may not need to rely on the presumptions of system integrity where there is some other evidence to suggest that the electronic evidence produced or generated from the system is reliable. However, a data input error independent of the record keeping process or a

---

22 *Supra*, Part II, para 2.80.

23 *Supra*, Part II, para 2.81.

24 *Supra*, Part III, paras 3.71 - 3.84.

manifest error such as a double entry will vitiate the presumption of an authenticated electronic record.[25] Secondly, the presumptions provide for the easy admissibility of electronic records by ensuring that in most instances, the authentication requirements as to admissibility of electronic business records – which we expect will form the bulk of the electronic evidence adduced in evidence – are readily satisfied.[26] As our survey of the cases decided in Singapore shows, parties to a transaction will generally not dispute an electronic record originating from the opponent.[27] If the opponent contends that the record has been fabricated by the proponent, the opponent will be able to tender his version of the document in evidence, and the court will decide which version is authentic. Similarly, in proceedings where parties to the dispute rely on the electronic business records of a neutral third party, the mechanism for admitting such records should be greatly simplified as such records are unlikely to be in dispute between the parties.[28] Thirdly, the use of presumptions avoids the formalism of compliance with statutory preconditions to admissibility such as the certification process, which as Part III illustrates, may have little, if any, bearing on the authentication issues at hand before the court.[29]

4.20. On the matter of the repeal of the existing certification mechanism in section 35 of the Evidence Act, objections may be raised by companies and businesses that have invested considerable financial, technical and manpower resources to set up certified "approved processes" for the storage of electronic records, pursuant to the Evidence (Computer Output) Regulations.[30] Examples of these institutions include the Inland Revenue Authority of Singapore ('IRAS') in its storage of submissions and

---

25 *Supra*, Part III, paras 3.108-3.112.

26 *Supra*, Part III, paras 3.103.-3.114.

27 See Appendix IV of this Paper for a list of Singapore cases.

28 *Supra*, Part II, paras 2.10-2.11.

29 *Supra*, Part II, paras 2.10-2.11.

30 S 35(1)(b) read with s 35(3) and s 35(4), Evidence Act.

returns by taxpayers.[31] We however feel that this concern can be overcome in two ways. The first is that the reliance on mechanisms similar to certified "approved processes" will greatly facilitate the process of authenticating electronic records extracted from such approved processes. In fact, the use of an independent third party auditor to verify the proper operation of the document imaging system means that an affidavit sworn by such a third party is clear and unequivocal evidence that will support such a finding, and no better evidence than this can be called for. And in the absence of manifest error on the electronic record or some other special circumstances, the opponent of such electronic evidence will find it difficult to challenge the testimony of the independent third party. So the investments made in such a record keeping system and the auditing processes are not wasted.[32] In fact, in view of the requirements of authentication, the record keeping system should be retained, albeit without any prescribed formalities for certification and auditing. Secondly, taking IRAS' document imaging system as an example, as the evidence adduced will most likely take the form of digitized versions of documents submitted by taxpayers, since these documents originate from the taxpayers themselves, the second presumption as set out in section 5, UEEA applies. Thus, subject to proof by IRAS of the proper operation of the document imaging system, the onus remains on the taxpayer to refute IRAS' documentary records of his documents.[33]

4.21. Therefore, we are of the opinion that Option 2 is actually marginally superior to Option 1, because the use of the presumptions provides a means to facilitate the admissibility of electronic evidence, and provide indirectly a means of transition from the existing legal regime to the new regime. At the same time, the presumptions provide the required certainty and predictability for businesses with

---

31 *Supra*, Part II, para 2.10.

32 *Ibid.*

33 *Supra*, Part II, para 2.10.

electronic records. Technology neutrality can also be preserved through the use of suitably worded presumptions. As such, we are strongly in favor of the adoption of this approach.

4.22. In summary, the changes recommended under Option 2 are:

- Repeal the computer-specific provisions (sections 35 and 36) as well as the computer-specific definitions (in section 3) of the Evidence Act.
- If necessary, expand the scope of the term "document" defined in section 3 of the Evidence Act to include electronic records,[34] or redefining the term "evidence" to include such "electronic records".[35]
- Introduce three new illustrations to section 9, Evidence Act to provide for the following evidentiary presumptions: (i) that electronic evidence generated, recorded or stored by the opponent of the evidence but adduced by the proponent against the opponent is presumed to be authentic in relation to those authentication issues arising from the generation, recording or storage by the opponent, (ii) that electronic evidence generated, recorded or stored in the usual and ordinary course of business by a neutral third party is presumed to be authentic, and (iii) that where an electronic device or process is one that, or is of a kind that, if properly used, ordinarily produces that electronic record/document, it is presumed that, in producing the electronic record/document on the occasion in question, the electronic device or process produced that electronic record/document. Each of the presumptions will stand unless evidence sufficient to raise doubt about that presumption is adduced.
- Modify the best evidence rule in the Evidence Act (sections 35(10), 65 and 66) to require the production of "original" copies of electronic records/documents where

---

34 Malaysian Evidence Act 1950, s 3. See also, *supra*, Part II, para 2.107.

35 Indian Evidence Act 1872, s 3. See also, *supra*, Part II, para 2.98.

the copies are electronically identical to the "original", but only admitting such "copies" where the reproduction measures reproduce the "original" in an accurate fashion.

Option 3. Adopt a business records approach to admit business records maintained in electronic form

4.23. This approach, described as Option 3, provides a mechanism for the easy admissibility of business records in general, which will include electronic business records as stored records. Business records are already admissible pursuant to section 32(b), Evidence Act, as an exception to the hearsay rule. What this approach envisages however is an admissibility provision to collapse the hearsay rule, the authentication rule and the best evidence rule into one general rule to provide for the admissibility of business records. Such an approach is taken from that adopted in UK under the CEA 1995 and in the Northern Territories of Australia under the EBRIAA, as described in Part II.[36] Under this Option, the revised section 32(b) will supplant sections 35 and 36. It may also supplement sections 35 and 36 as an additional mode of admissibility.

4.24. The objective behind such an approach is to provide an easy admissibility mechanism for the records maintained in electronic form by the business community. Most of the relevant and pertinent electronic records admitted in evidence are business records, and the business community has expended considerable resources to computerize its operations and store its business records in electronic form. Option 3 thus responds to the needs of the business community and also accepts the fact, as pointed out in Part III,[37] that business records are generally presumed to be inherently reliable, especially where the records are used by the businesses for their operations. The case law shows that once a business record is admitted pursuant to a

---

[36] See Part II, paras 2.66 - 2.71.

[37] *Supra,* Part III, paras 3.103 - 3.114.

hearsay exception, few if any legal hurdles remain in relation to the issues of authentication and best evidence.

4.25. While the approach uses the term "business record" to fix the scope of its application, we envisage that its scope is not restricted to records maintained by 'business' organizations but extends to such records maintained by public authorities and non-profit organizations.[38]

4.26. While this approach may be perceived to be advantageous as it provides a significantly easy avenue to admit electronic business records, it is submitted that the approach lacks utility. Firstly, the scope of the approach is rather narrow as it applies only to records retained in the course of business and not to non-business documents. For non-business documents, the general rules of evidence will remain applicable.[39] This approach fails to provide rules, and offers no guidance, for dealing with electronic non-business records such as personal email and chatroom logs. Secondly, since the provision envisaged here is a three-in-one rule, the proponent of a business record will have to satisfy certain prescribed statutory conditions to ensure the general reliability and integrity of business records. Proof of this may take the form of a certification process. We have already made known our disfavour of certification mechanisms. A certification mechanism will require a statutory enumeration of the requirements of a certificate, including the information required on the certificate, the people who are competent to certify, penalties for erroneous or misleading certificates and provisions to cross-examine the certifier. A certificate is also no assurance as to the correctness and reliability of the contents of the business record so certified, *e.g.* where there is a manifest error evident on the face of the record. In such a case, the courts will call for additional evidence and the certificate is of no utility. Thirdly, as Option 3 is premised on the business record falling within the business records

---

38 S 9, CEA 1995.

39 The treatment of non-business documents will depend upon whether Option 3 is envisaged as a substitute or a supplement to ss 35, 36 Evidence Act.

exception as proof of its authenticity, it will have no application to business records that are real evidence. Furthermore, to include provisions to admit business records as real evidence will mean that this Option will be no different from Option 2.

4.27. In summary, the changes recommended under Option 3 are:

- Modify the existing rule in section 32(b), Evidence Act, to state that where written statements of relevant facts are relevant facts pursuant to section 32(b), notwithstanding sections 9, [35], 65, 66 and 67, they may be proved by the production of a document that is made in the ordinary course of business that embodies those statements, or by the production of a copy of that document thereof, either authenticated by a certificate to that effect signed by an officer of the business, or authenticated in such manner as the court may approve.

Option 4. Retain the existing computer-specific approach but ease the rules of admissibility

4.28. We envisage this approach proposed as Option 4 to be similar to the computer-specific approach provided by the existing sections 35 and 36 of the Evidence Act. This approach recognises that there are issues of reliability, integrity and authenticity of electronic evidence irrespective of whether such evidence is computer-stored or computer-produced. The statutory provisions therefore take these issues into account and provide an elaborate and highly instructive mechanism by prescribing preconditions for the admissibility of electronic evidence. We describe the mechanism as instructive because they instruct and guide the proponent of the evidence and the court as to the evidentiary issues that they have to consider when admitting the evidence.

4.29. Examples of such an instructive approach can also be seen in the Evidence Acts of South Australia[40] and India[41]. Both have their origins in the UK CEA 1968 which had adopted such an approach – a combination of setting out the preconditions for the proper use and operation of the computer and for ensuring the reliability of the output supported by statutorily prescribed certification mechanisms. But it is highly notable that the UK Law Commission has since disavowed this approach, describing it as "outdated and aimed at providing for the operations of mainframe computers existing in the 1960's."[42]

4.30. We do not think that this is the best Option available, since it indiscriminately assumes that all electronic records are unreliable and prone to error, but we ought to mention that the utility of this approach is in its instruction to the proponent and to the court. We should also mention that this Option is premised on making incremental and evolutionary modifications to our existing sections 35 and 36.

4.31. Thus, under this Option, the three modes of admissibility will supplement and not exclude the existing common law rules of admissibility of electronic evidence.[43] The revised section 35 will only state the broad principles regarding the authentication of the accuracy and reliability of computer output, but the three modes of admissibility that will be retained are inclusionary and descriptive, and not exhaustive and prescriptive in nature. While parties may continue to use any of the three modes of admissibility, they are free to utilise the inherently flexible common law approach to authentication.

---

40 *Supra,* Part II, paras 2.45 - 2.55.

41 *Supra,* Part II, paras 2.97 - 2.104.

42 *Supra*, Part II, note 70, UK Law Commission Report No 216, para 3.14.

43 This is similar to the judicial approach taken by the South Australian courts, which have interpreted away section 59B of the South Australia Evidence Act and have treated it as complementary to the rules of admissibility at common law and the banking records statutory exception. See Part II, para 2.51.

4.32. In the light of caselaw developments and the analysis above, the changes recommended under Option 4 are:

- Modify section 35(1) to provide that where computer output is tendered in evidence for any purpose whatsoever, such output shall be admissible if it is relevant or otherwise admissible under the Evidence Act or any other written law, and it is authenticated by the party tendering such output proving that (i) the output is accurate and reliable and (ii) at all material times the computer that produced the output was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the accuracy and reliability of the output was not affected by such circumstances.

- Introduce a new section 35(2) to provide that proof of such authenticity as prescribed in section 35(1) may be dispensed with where the affected parties do not object to the authenticity of such output, either by way of an express agreement or by way of an unequivocal course of conduct undertaken by the opponent of such output that is consistent with the opponent's dispensation of all possible objections to its authenticity.

- Modify and revise section 35(6), (7) and (8) to provide that an affidavit (similar to that set out in section 36(2)) made by any qualified person in relation to the computer output may be tendered to authenticate such output. The persons who are qualified to make such an affidavit *include* "persons holding a responsible position in relation to the operation or management of the relevant computer system" (section 35(6), (7)) and such persons "who had obtained or been given control or access to the relevant computer system" (section 35(8)). The court will retain the discretion to determine if the maker of an affidavit is such a qualified person to make the affidavit tendered to authenticate such output.

- Modify the rest of section 35 to provide that:

    - where a compliant certificate is issued pursuant to section 35(3) and (4), it shall be presumed, unless

the contrary is proved, that the output produced by an approved process is authentic;

- where a compliant certificate is issued pursuant to section 35(6), (7) or (8) (as modified above), it shall be presumed, [unless the contrary is proved/unless evidence sufficient to raise doubt about the presumption is adduced][44], that the output is authentic;

- Clarify that the certificates issued pursuant to sections 35(3), (4), (6), (7) and (8) are not to the exclusion of other modes of authenticating the output.

Q. Should sections 35 and 36 of the Evidence Act be the subject of legal reform? If so, which option of reform as advanced above do you prefer and why? Are there any other alternative options for the reform of sections 35 and 36 of the Evidence Act?

[44] The formulations suggested above alternatively give effect to the provision as a legal presumption or as an evidential presumption as to authentication of the computer output. See, *supra*, note 15.

List of Questions