COMPUTER OUTPUT AS EVIDENCE
FINAL REPORT

TECHNOLOGY LAW DEVELOPMENT GROUP
SINGAPORE ACADEMY OF LAW
DECEMBER 2004

Authors:

Daniel Seng

Associate Professor, Faculty of Law, National University of Singapore

Sriram S. Chakravarthi

Assistant Director, Singapore Academy of Law

ISBN 981-05-2865-5

About the Final Report

This final report, completed in December 2004, consolidates the findings and responses that were received by the Technology Law Development Group ("TLDG") for its Consultation Paper entitled "Computer Output as Evidence", published in September 2003. It also includes the draft Evidence (Amendment) Bill 2005 which gives effect to the recommendations made by the TLDG in the Consultation Paper.

This report reflects the authors' and the respondents' opinions and 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 report has no regulatory effect and does not confer any rights or remedies.

Any correspondence on the final report 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

About the Technology Law Development Group

The Technology Law Development Group 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. Its advisory group comprises representatives from the legal sector, information technology industry, financial services industry and government.

Table of Contents

Final Report

Summary of Provisional Recommendations in the Consultation Paper

1. The TLDG Consultation Paper on Computer Output as Evidence (the "Paper" or the "Consultation Paper")[1] was published in September 2003. In that Paper, which arose from a request from the Attorney-General's Chambers, we reviewed the existing provisions of the Singapore Evidence Act and offered our provisional recommendations relating to the need to reform the law relating to the admissibility of computer output as evidence. We explored 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 to 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.

2. In our Paper, we provisionally recommended the adoption of Option 2, which entailed the abolition of the existing computer-specific approach of admitting computer output in the Singapore Evidence Act. In its place, we proposed the adoption of a technology neutral, non-computer specific approach for admitting electronic evidence. However, we also proposed that these provisions be supplemented by presumptions to facilitate the admissibility of

---

[1] Daniel Seng and Sriram Chakravarthi, *Computer Output as Evidence: Consultation Paper* (Singapore Academy of Law 2003) [hereinafter *Consultation Paper*].

certain types of electronic evidence. We then released the Paper for review and public consultation. We circulated copies of the Paper to overseas academics and experts and sought their views and opinions. As part of our public consultation process, we also conducted three separate seminars to brief participants and solicit their feedback:

- Briefing to legal service officers with the Attorney-General's Chambers (3 November 2003);
- Briefing to senior police officers of the Singapore Police Force and Justices' Law Clerks, Supreme Court of Singapore (13 November 2003); and
- Public seminar entitled Computer Output as Evidence, organised by the Singapore Academy of Law (19 November 2003).

The Consultation Process and Responses to the Paper

3. The seminars were well-attended. Participants included members of the legal academia, legal service officers, government regulators, public prosecutors, state counsel, lawyers, justices' law clerks, registrars, legal counsel, police officers, auditors, IT consultants and other professionals. The participants comprised representatives from the legal sector, information technology industry, financial services industry and government. We had very useful discussions with many of these participants and we are grateful for their interest and their feedback.

4. The TLDG also received five written responses during the consultation period which ended on 30 November 2003. These responses are included in this Report at Annexes 1-5. Subsequently, the TLDG received three additional written responses in January 2004. These responses have been included in this report at Annex 6-8 respectively. We are very encouraged by the responses. While six of these responses are from Singapore, two are from overseas.

5. The respondents' details and their responses are included in this report in the Annexes as follows:

Annex 1	**Respondent I** Mr Ng Seng Liang Director CID Singapore Police Force
Annex 2	**Respondent II** Mr John D. Gregory General Counsel, Policy Branch Ministry of the Attorney General (Ontario) Toronto, Canada
Annex 3	**Respondent III** Ms Yee Fen Lim Senior Lecturer in Law Department of Law Macquarie University Sydney, Australia
Annex 4	**Respondent IV** Ms Judy Kon Strategy and Engagement Executive EBO IBM Global Services Asia Pacific Singapore

Annex 5 **Respondent V**
Mr Andrew Chan Chee Yin
Partner, Allen and Gledhill
Singapore
(On behalf of the IT and Electronic Litigation Committee of the Law Society, Singapore)[2]

Annex 6 **Respondent VI**
Mr Foo Chee Hock *
Deputy Registrar
Supreme Court
Singapore
* (Submissions prepared by Ms Thian Yee Sze, Senior Assistant Registrar and Ms Dawn Tan, Assistant Registrar, Supreme Court, Singapore)

Annex 7 **Respondent VII**
Mr Andrew C.L. Ong *
Director
Drew and Napier LLC
Singapore
* (with inputs from Mr Edric Wong)

Annex 8 **Respondent VIII**
Mr Jaswant Singh
Criminal Justice Division
Attorney-General's Chambers
Singapore

6. In summary, five of the respondents (Respondents I, II III, VI and VIII) were in favour of the proposed Option 2, one respondent (Respondent VII) was in favour of a variation of the proposed Option 2, one respondent

[2] Views expressed do not necessarily represent the views of the Law Society, Singapore.

(Respondent IV) was against both Options 2 and 4 for reform and one respondent (Respondent V) was in favour of reform but proposed a new methodology.

Summary of Responses

A. Responses in favour of Option 2

7. Respondents I ("the Singapore Police Force"), II ("Ms Lim"), III ("Mr Gregory"), VI ("the Supreme Court") and VIII ("the Criminal Justice Division") were in favour of the approach of technology-neutrality which "allows for flexibility in the rules of evidence to embrace further changes due to advent in technology"[3]. This technology-neutral approach as espoused in the proposed Option 2 "aptly strikes a balance between flexibility on the one hand and predictability on the other"[4]. Ms Lim and Mr Gregory stated that such a technology-neutral approach has been adopted in all the [Information Technology] IT statutes around the world.[5] In fact, Mr Gregory observed that this is the model adopted for e-commerce statutes around the world that are based on the UNCITRAL Model Law on e-commerce. He opined:

> The main purpose of these statutes is probably to let lawyers relax, since their clients are out there doing e-commerce and making and keeping e-records anyway.[6]

8. However, the approach of admitting electronic evidence without any guidelines or rules, such as that proposed as Option 1 in our Paper, was not favoured by the Singapore

---

3 *See*, *e.g.*, Response from the Singapore Police Force, Annex 1, at 29.

4 Response from the Supreme Court, Singapore, Annex 6, at 65 [hereinafter *Annex 6*].

5 Response from Mr John Gregory, Annex 2, at 40 [hereinafter *Annex 2*]; Response from Ms Yee Fen Lim, Annex 3, at 43 [hereinafter *Annex 3*].

6 *Annex 2*, at 36.

Supreme Court, Ms Lim or Mr Gregory.[7] They all gave different reasons. The Supreme Court was of the view that while such an approach may work in the United States where "the courts have the benefit of significant pool of case law with precedential and instructive value"[8], this approach was unlikely to work in Singapore as the Singapore courts "lack such a fund of experience to guide them".[9] Ms Lim was of the view that while Option 1 preserved full flexibility, it would be too drastic to change from the current prescriptive regime to one offering very little legislative guidance.[10] Mr Gregory was of the view that although the courts were just letting any evidence in and dealing with questions of integrity of electronic evidence as matters of weight, the courts remained cognizant of the relevance of various evidence rules of admissibility such as the best evidence rule.[11] Mr Gregory however explained that the need for guidance comes in because there is a need to "prevent the need for full-scale technical defences of e-records."[12] He agreed with the thesis in our Paper that issues of reliability of electronic evidence can be dealt with as matters of authentication.[13] He further stated that the Canadian Uniform Electronic Evidence Act ("UEEA") consciously adopted a test that avoided setting up additional hurdles to the admissibility of electronic evidence.[14] According to Mr Gregory, "we didn't want to set up additional hurdles to the admission of evidence than the courts had - we were trying to remove barriers not create them".[15]

---

7 *Annex 6*, at 59 (Supreme Court); *Annex 3*, at 43 (Ms Lim); *Annex 2*, at 36 (Mr Gregory).

8 *Annex 6,* at 65.

9 *Id.*

10 *Annex 3*, at 43.

11 *Annex 2*, at 39.

12 *Id.* at 37.

13 *Id*. at 40.

14 *Id*. at 32.

15 *Id*.

9. All five respondents – the Singapore Police Force, Ms Lim, Mr Gregory, the Supreme Court and the Criminal Justice Division – agreed with Option 2 and its use of presumptions to facilitate the application of the test of authentication. In its written response supporting the proposed Option 2, the Supreme Court agreed that Option 2 aptly strikes the right balance between flexibility on the one hand and predictability on the other by focusing on the issue of authentication.[16] In this regard, the Supreme Court was of the view that:

> [A] court need not rely on presumptions of system integrity where there is some other evidence to suggest that electronic evidence produced or generated by the system is reliable. Conversely, a data input error independent of the record keeping process or a manifest error such as a double entry will vitiate the presumption of an authenticated electronic record.[17]

10. Mr Gregory in his response made two additional observations. The first was that it is fairly easy for the proponent to present evidence capable of supporting a finding that the evidence was what it purports to be in the absence of a dispute.[18] On the other hand, there is a need to prevent "full-scale technical defences of e-records once one makes an authentication question of them"[19]. For this reason the presumptions to facilitate the passage of records were introduced in the UEEA. But the presumptions were intended to be easily rebuttable.[20] As Mr Gregory observed:

> [T]he opponent does not have to prove the contrary, [he just has to] raise evidence to the contrary. After that, the parties are on their own – no presumption

16 *Annex 6*, at 65.

17 *Id.*

18 *Annex 2*, at 32.

19 *Id.* at 37.

20 *Id*. at 35.

> [applies] – and then one gets into the reliance on standards *etc*.[21]

11. According to Mr Gregory, another technique that is used to prevent a full-scale enquiry of the e-records is via 'a notice to admit' process in the Canadian Rules of Civil Procedure. The way it works is that one party tells the other a set time before trial what documents the first party will produce, and if the other party does not object within a fairly tight time limit, no objection can be brought to trial.[22]

12. We note that this process is very similar to the concept of 'agreed bundle' in Singapore's civil procedure rules[23] except that there is no prescribed statutory time limit and the rules of procedure leave it to the parties to decide on the effect of including the documents *i.e.* whether the documents admitted in the bundle are admitted because no further objections concerning their authentication can be brought at trial or whether the parties reserve their position as regards any further objections as regards the authenticity of the documents.[24]

13. Mr Gregory observed that the Uniform Law Conference of Canada ("ULCC") was not amenable to allowing parties to admit evidence via agreements. This is because while this may work in civil cases it will not work in criminal cases since it has been attacked in Canada on the basis that parties could otherwise change the law of evidence by private agreement.[25] (We take a more practical view of this issue, because, as we noted in the Consultation Paper, this is likely to be less of an issue in most instances as the accused is unlikely to agree to evidence offered by

---

21 *Id*.

22 *Id*. at 37.

23 Rules of Court (Cap 322, R 5, 2004 Rev Ed), O 34A, r 3A(3).

24 *Consultation Paper*, at paras 3.127, 3.128.

25 *Annex 2*, at 37.

27 *Consultation Paper*, at para 3.25.

prosecution which is likely to incriminate him.[27]) Under our current proposals, no distinction is made between electronic evidence in civil or criminal proceedings. We note that respondent VIII – the Criminal Justice Division – agrees with our view that Option 2 will not prevent defence counsel for the accused from mounting a valid (and effective) challenge to such evidence.[28]

14. Mr Gregory is fully supportive of all the three presumptions outlined in the Consultation Paper for Option 2.[29] To recap, we had proposed that the first presumption (the adverse party presumption) provide 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.[31] We also proposed that the second presumption (the neutral third party presumption) provide 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.[32] Finally, we had also proposed a third presumption (ordinary electronic device presumption), that presumes that a commonplace electronic device properly used will ordinarily produce that electronic record or document.[33]

15. To recap, the first two presumptions were based on the Canadian UEEA and the third and last presumption was based on the Australian Commonwealth Evidence Act

---

28 Response from the Criminal Justice Division, Singapore, Annex 8, at 75. [hereinafter *Annex 8*].

29 *Annex 2*, at page 36.

31 *Consultation Paper*, at para 4.16.

32 *Id*.

33 *Id*.

1995. Mr Gregory observed that the first two presumptions originated from the work done by the ULCC on the UEEA.[34] He approved of our rider to the first presumption as adapted from the original formulation in the UEEA *i.e.* that the presumption only covers the authentication issues arising from the generation of records in the hands of the adverse party,[36] In such cases, Mr Gregory correctly observed that the proponent has to account for the integrity of the record once it comes into his hands.[37] As for the ordinary electronic devices presumption, Mr Gregory agreed with the presumption as worded that 'machines that produce computer-generated evidence are not presumed reliable until the courts are very familiar with them'.[38]

16. On the issue of standards, it may be noted that the Consultation Paper did not refer to or prescribe any particular standards for the retention of electronic evidence. On the other hand, Mr Gregory noted that the UEEA does refer to certain standards *e.g.* the Canadian General Standard Boards Standard.[39] However, Mr Gregory noted that the ULCC was pressurized to refer to the use of standards especially since the Canadian General Standard Board was in the late stages of adopting a standard on electronic records as evidence.[40] Mr Gregory makes the point that in principle it should be helpful to record managers to tell them "what to think about to keep their records admissible" although he expressed some reservations that the standard is too closely associated with the UEEA.[41]

---

34 Annex 2, at page 36.

36 *Id.*.

37 *Id*.

38 *Id*, at 35.

39 *Id*, at 37.

40 *Id*.

41 *Id*, at 38.

17. On the point of the best evidence rule, Mr Gregory was in favour of retaining it and was very supportive of our American-inspired approach pursuant to sections 1001 and 1003 of the United States Federal Rules of Evidence.[42]

B. In favour of a variation of proposed Option 2

18. Respondent VII – Mr Andrew Ong of Drew and Napier LLC – in his written response to the TLDG, took a similar view that "Sections 35 and 36 raises [sic] the admissibility standards admitting electronic evidence in a manner that is unnecessarily inconvenient."[43] While agreeing with the majority of respondents that the Evidence Act should be amended so that electronic evidence may be admitted more easily, the respondent did not favour Option 2 in its current form. Instead, the respondent preferred the retention of computer-specific provisions similar to the existing sections 35 and 36 of the Evidence Act but in a "relaxed form", by substituting them with a set of presumptions similar to Section 5 of the Canadian UEEA instead.[44]

19. Without further elaboration on the details of the variation of Option 2, the respondent's preferred option would be quite similar to the approach proposed under Option 4.

C. Not in favour of Status Quo and Options 2 and 4

20. Respondent IV – Ms Judy Ong of IBM Global Services, Asia Pacific – was not in favour of the current regime for admitting computer output.[45] Neither was she in favour of any of the options for proposed reform as advanced in the Paper.[46] The respondent envisaged the use of technology

---

42 *Id*, at 41.

43 Response from Drew & Napier LLC, Annex 7, at 67 [hereinafter *Annex 7"*].

44 *Id*. at 73.

45 Response from IBM Global Services Asia Pacific, Annex 4, at 47.

46 *Id.* at 47.

which is testimony independent to authenticate electronic evidence.[47] The respondent did not describe or elaborate on this technology but we presume that the respondent was referring to digital signature and encryption technologies based on reliable data sources.

21. To elaborate, respondent IV was extremely critical of the current admissibility provisions. As to admission by express agreement, the respondent's view was that if the proponent of the electronic evidence has engaged in time-based data manipulation, such fraud can never be discovered. As a consequence, manipulated electronic evidence gets substituted for true data by the express agreement route.[48] The respondent was similarly critical of admission by approved process and by proof of proper operation and accuracy. Her observation was that both processes will not prevent an insider from engaging in unauthorized manipulation and tampering of electronic evidence which is impossible to ascertain or discover.[49]

22. Respondent IV also took the view that both Options 2 and 4 failed to take into account the intrinsic vulnerability of currently generated electronic data.[50] The respondent was of the opinion that this vulnerability exists both for enterprise, government as well as private or small business users.

23. We agree with the respondent's concerns regarding the intrinsic vulnerability of electronic evidence. However, we do not think that there can be purely legal solution to this problem. As explained in the Consultation Paper, unreliable evidence – be it electronic or otherwise – should be dealt with via clear awareness of the issues and an enlightened approach towards authentication of such

---

47 *Id*.

48 *Id*. at 45.

49 *Id*.

50 *Id*. at 47.

evidence.[51] Our recommendations seek to do just that, by clarifying the necessity for electronic evidence to be authenticated in court. But how they are authenticated is still largely an issue for systems and records management for which technological solutions have to be implemented in conjunction with sound business practices. We are of the opinion that Option 2 and its presumptions will have the effect of encouraging best systems and records management processes and business practices, as these will in turn facilitate the admissibility of electronic evidence generated or produced by such systems in court.

D. Alternatives to the Reform Options

24. The joint response of respondent V – the IT and ELS Committees of the Law Society of Singapore – was that a completely different approach must be adopted for admitting electronic evidence. While the respondent favoured a review of the current rules of evidence, which is viewed as being "unduly restrictive and should be reformed"[52], the approach advocated by the respondent is to have specialised rules of evidence for admitting electronic evidence "when [they are] sought to be admitted as computer output."[53] The respondent draws inspiration for this approach from a technique used in the area of hearsay evidence in that the hearsay rules only apply where the purpose of the hearsay is admitted for the purpose of proving its contents. The approach thus proposed is for a broad principle of admissibility to admit computer output depending on "accuracy, authenticity and reliability of the output"[54]. However, the respondent was of the view that there should be various "safe harbours" where computer output will be admitted unless the opponent shows that the evidence

---

51 *Consultation Paper*, at paras 3.85 - 3.128.

52 Response from the IT Committee and the ELS Committees of the Law Society, Annex 5, at 49 [hereinafter *Annex 5*].

53 *Id*. at 51.

54 *Id*. at 53.

does not satisfy the board principle of admission.[55] According to the respondent, "[s]uch safe harbour grounds could include the current ground for admissibility of documents produced in an approved process, but with an appropriate review with a view to liberalization."[56]

25. The respondent was in favour of retaining the "approved process" mechanism for admissibility. The reason adduced was that the Evidence (Computer Output) Regulations has been accepted by the Inland Revenue Authority of Singapore ("IRAS") in its guide for "Keeping of Records in Imaging System". In the view of the respondent, the abolition of these provisions for approved processes may result in the evidential rules for admissibility and the IRAS rules governing retention of records being out of sync.[57] While we agree with the respondent on the need for liberalization, we do not think any law reform recommendations should be strictured by existing regulations. Instead, the existing regulations should only be retained where they are consistent with the overall objectives (and results) of the reform process.

Conclusion and Final Recommendations

26. We are very pleased with the broad spectrum of responses that we received. The respondents represent the judiciary, the IT industry, the legal profession, academia, a law reform institution as well as the Government. We would like to thank the respondents for taking the time and trouble to share their views with us. We are even more heartened by the fact that the majority of respondents supported our proposed Option 2.

27. In light of our recommendation, a draft Evidence (Amendment) Bill ("the Bill') based on our proposed Option 2 has been included in this Report. The Bill

---

55 *Id*. at 54.

56 *Id*.

57 *Id*.

represents the fruits of numerous hours of internal consultations, exchanges and discussions between the authors and with Mr Charles Lim Aeng Cheng, TLDG member. The commentary on the Bill can be found in the Explanatory Statement attached therein. (In this regard, we would like to acknowledge our deepest thanks to Mr Lim for his invaluable help and input in assisting us in the drafting of the proposed Evidence (Amendment) Bill.)

28. In particular, it is worth noting that none of the respondents supported the current rules of admissibility. In particular, Mr Gregory thought "that there was good reason not to follow … the full demanding certificate-supporting route that the English had adopted in 1988 [sic]".[58] Nearly all the respondents felt that it was time to review the current provisions relating to admissibility of computer evidence. As stated in the response of the Supreme Court:

> [A]dvancements in software and hardware technologies, exponential growth in usage of the Internet after the passage of the [Evidence] amendment Bill, and indeed the widespread acceptance of computer output (broadly defined) in the business community, necessitate revising the current approach and perhaps rethinking this distrust.[59]

29. The approach we finally recommend entails abolishing the existing sections 35 and 36 of the Evidence Act (the Bill, clause 4) and replacing them with rules of authentication (the Bill, clause 3). This takes the form of expanding and clarifying the existing authentication provision (Evidence Act, section 9), and are implemented in clause 8 of the Bill.

30. The presumptions that we proposed in option 2, which were derived and adapted from the Canadian UEEA, have received Mr Gregory's sanction as one of the draftsmen of the UEEA. We are of the opinion that the presumptions

---

58 *Annex 2*, at 36.

59 *Annex 6*, at 65.

will represent a transition measure in the move from the current very prescriptive regime to a more relaxed regulatory regime. As Ms Lim puts it, "[t]he adoption of the presumptions certainly would guide the business community, legal profession and judiciary in adjusting to the new regime".[60] The final version of the Bill, as appended to this report, also arrogates to the Minister the power to make recommendations to facilitate the authentication of documents stored using a document imaging system that complies with the rules (the Bill, clause 8). In this regard, we feel that we have met the concerns of respondent V (IT and ELS Committees of the Law Society of Singapore) by providing an avenue for ensuring that "if there are changes made to the law, transitional provisions should be made to ensure that previously admissible electronic evidence do [sic] not suddenly somehow become not admissible".[61]

31. We also recommended that the secondary evidence rule be clarified to recognise that electronic copies of documents that are shown to reflect the contents of original documents are treated as primary evidence (the Bill, clause 5). Consequential amendments to the Evidence Act are also made in clause 6 of the Bill.

32. What we also found useful from Mr Gregory's feedback is the reminder of the need for standards to facilitate the admissibility of electronic evidence and the prescription of standards which will be helpful to record managers. Mr Gregory's feedback clearly highlights the utility of having a national standards body adopting standards for admitting electronic records as evidence. We find echoes of this same sentiment in the Law Society's (respondent V) response. But we also find ourselves in agreement with the CJD's response – that having standards will mean that

60 *Annex 3*, at 43.

61 *Annex 5*, at 49.

technological changes may render such standards obsolete.[62]

33. (We note in passing that respondent VII had proposed a variation to Option 2 in the form of retention of computer-specific provisions similar to sections 35 and 36, but incorporating the Canadian UEEA presumptions in Option 2.[63] With respect, we do not prefer this variation because we do not think it is feasible to combine the procedural formalism of the computer-specific admissibility provisions in the current sections 35 and 36 with the inherent flexibility of the presumptions. We think that it will be difficult to reconcile the utility and advantages arising from the use of flexible presumptions with the computer-specific provisions of sections 35 and 36. For that reason, we had explained in the Consultation Paper that Option 2 and Option 4 are opposite options for legal reform.[64])

34. Therefore, we are of the opinion that we have struck a balance in our Option 2 by not referring to any particular standards or particular procedure. Mr Gregory seems to concur with this approach.[65] The courts are always free to refer to applicable standards for retention of evidence. There is much to be said for national standards as setting best practice guidelines for document retention and evidence preservation. And we will encourage national standards bodies, computer societies and industry and business associations to do so. Obviously, where a party deviates from national or industry standards or guidelines, especially for that industry, that party has to answer to the courts and the opponent with his reasons for doing so. This process is part of the authentication process that we envisage. In this regard, we draw comfort from Mr Gregory's observations that where legislation refers to (and

---

62 *Annex 8*, at 75.

63 *Annex 7*, at 73.

64 *Consultation Paper*, at paras. 4.28 - 4.31.

65 *Annex 2*, at 36.

prescribes) standards, there is a tendency for parties and the industry to too closely associate the standards with the admissibility rules.[66] The industry should be encouraged to develop its own standards, but the law should give full support for such standards, where they are consistent with the objectives of trustworthy, authentic and reliable evidence.

35. In conclusion, the consultation exercise has reinforced our belief that the current provisions for computer admissibility are in need of reform and that the proposed Option 2 is an acceptable, if not the best, way forward.

36. Finally, we wish to take this opportunity to express our sincere gratitude to The Honourable the Chief Justice and the TLDG leadership for having entrusted this research project to us and for their continued support throughout the project. We also wish to thank all the respondents who have so graciously provided feedback on our Consultation Paper, and we hope that our efforts will make a positive difference to the development of the laws on electronic evidence.

Authors:

Daniel Seng

Associate Professor, Faculty of Law, National University of Singapore

Sriram S. Chakravarthi

Assistant Director, Singapore Academy of Law

December 2004

---

66 *Id*. at 37.

Appendix: Draft Evidence (Amendment) Bill

ARRANGEMENT OF CLAUSES

EXPLANATORY STATEMENT

EXPENDITURE OF PUBLIC MONEY

EVIDENCE (AMENDMENT) BILL

Bill No. 00/2005.

Read the first time on *2005.*

A BILL

i n t i t u l e d

An Act to amend the Evidence Act (Chapter 97 of the 1997 Revised Edition) to provide for the admissibility of electronic evidence in court proceedings and certain related matters.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

Short title and commencement

1. — (1) This Act may be cited as the Evidence (Amendment) Act 2005 and shall come into operation on such date as the Minister may, by notification in the *Gazette*, appoint.

(2) The provisions of the Evidence Act as amended by this Act shall apply to any judicial proceedings in or before any court which takes place on or after the commencement of this Act, and the court may make any order as it thinks fit to give effect to those provisions.

Amendment of section 3

2. Section 3 of the Evidence Act is amended —

(*a*) by deleting the definitions of "computer" and "computer output"; and

(*b*) by inserting immediately after the definition of "document", the following definition:

> "electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another;".

Amendment of section 9

3. Section 9 of the Evidence Act is amended by inserting, immediately after paragraph (*f*) of the *Illustrations,* the following paragraph:

> "(*g*) A seeks to adduce evidence against B in the form of an electronic record. The method and manner in which the electronic record was (properly or improperly) generated, communicated, received or stored (by A or B), the reliability of the devices and the cir-

cumstances in which the devices were (properly or improperly) used or operated to generate, communicate, receive or store the electronic record, may be relevant facts as authenticating the electronic record and therefore as explaining or introducing the electronic record, or identifying it as the relevant electronic record to support a finding that the record is, or is not, what its proponent A claims."

Repeal of sections 35 and 36

4. Sections 35 and 36 of the Evidence Act are repealed.

Amendment of section 64

5. Section 64 of the Evidence Act is amended by inserting, immediately after *Explanation 2* including the *Illustration* to that *Explanation*, the following *Explanation*:

"*Explanation 3.* - Notwithstanding *Explanation 2,* if a copy of a document in the form of an electronic record is shown to reflect that document accurately, then the copy is primary evidence.

Illustrations

(*a*) An electronic record, which has been manifestly or consistently acted on, relied upon, or used as the information recorded or stored on the computer system (the document), is primary evidence of that document.

(*b*) If the electronic record has not been manifestly or consistently acted on, relied upon, or used as a record of the information in the document, the electronic record may be a copy of the document and treated as secondary evidence of that document.".

Amendment of section 65

6. Section 65 of the Evidence Act is amended —

(*a*) by deleting paragraph (*b*); and

(*b*) by deleting paragraph (*c*) of the *Illustrations*.

Amendment of section 68A

7. Section 68A of the Evidence Act is amended -

(a) by deleting the words ", computer output or other explanatory material" in paragraph (1) and substituting the words "or other explanatory material, in electronic or other medium,"; and

(b) by deleting the words "in any form, including computer output;" in paragraph (3)(a) and substituting the words "in electronic or other medium;".

New section 81A

8. The Evidence Act is amended by inserting immediately after section 81, the following section:

"Presumptions in relation to electronic records

81A.—(1) Unless evidence sufficient to raise doubt about the presumption is adduced, where a device or process is one that, or is of a kind that, if properly used, ordinarily produces or accurately communicates an electronic record, the court shall presume that in producing or communicating that electronic record on the occasion in question, the device or process produced or accurately communicated the electronic record.

Illustration

A seeks to adduce evidence in the form of an electronic record produced by an electronic device or process. A proves that the electronic device or process in question is one that, or is of a kind that, if properly used, ordinarily produces that electronic record or document. This is a relevant fact for the court to presume that in producing the electronic record or document on the occasion in question, the electronic device or process produced the electronic record or document which A seeks to adduce.

(2) Unless evidence to the contrary is adduced, the court shall presume that any electronic record generated, recorded or stored is authentic if it is established that the electronic record was generated, recorded or stored in the usual and ordinary course of business by a person who was not a party to the proceedings on the occasion in question and who did not generate, record or store it under the control of the party seeking to introduce the record.

Illustration

A seeks to adduce evidence against B in the form of an electronic record. The fact that the electronic record was generated, recorded or stored in the usual and ordinary course of business by C, a neutral third party, is a relevant fact for the court to presume that the electronic record is authentic and accurate.

(3) Unless evidence to the contrary is adduced, where an electronic record was generated, recorded or stored by the opponent of the evidence but adduced by the proponent against that opponent, the court shall presume that the electronic record is authentic in relation to the authentication issues arising from the generation, recording or storage of the record by the opponent.

Illustration

A seeks to adduce evidence against B in the form of an electronic record. The fact that the electronic record was generated, recorded or stored by B, who opposes the relevance of the evidence, is a relevant fact for the court to presume that the electronic record is authentic and accurate.

(4) The Minister may make regulations providing for a process by which a document may be recorded or stored through the use of an imaging system, including providing for the appointment of one or more persons or organisations to certify these systems and their use, and for any matters incidental thereto, and an "approved process" in subsection (5) means a process that has been approved in accordance with the provisions of such regulations.

(5) Where an electronic record was recorded or stored from a document produced pursuant to an approved process, the court shall presume, unless evidence to the contrary is adduced, that the electronic record accurately reproduces that document.".

Transitional provision

9. Notwithstanding the repeal of section 35, the regulations made under the repealed section 35(5) and in force immediately before the commencement of this Act shall continue to be in force as if they have been made under section 81A(4).

EXPLANATORY STATEMENT

This Bill seeks to amend the Evidence Act (Cap. 97) to give effect to the recommendations of the Technology Law Development Group of the Singapore Academy of Law in its Consultation Paper "Computer Output as Evidence", September 2003 and the Final Report, December 2004. The Report recommended the adoption of a non computer-specific approach but to provide presumptions to facilitate the admissibility of certain electronic evidence. 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. In this approach, the existing rules in sections 35 and 36 will be repealed and will no longer regulate the admissibility of electronic evidence. Instead the existing rules providing for the relevancy and admissibility of evidence (such as hearsay, the best evidence rules and rules on authentication) will regulate the admissibility of electronic evidence in the same manner as any other item of evidence. The courts are given a wide discretion to call for evidence to authenticate the electronic evidence in any manner that the courts deems appropriate. By avoiding the prescription of express requirements, such as that under the repealed section 35, that the proponent of the electronic evidence has to satisfy before the evidence can be considered for admissibility, full flexibility is preserved.

Clause 1 relates to the short title and commencement. The amendments made in this Bill will apply to any judicial proceedings in or before any court which takes place on or after the date of commencement.

Clause 2 amends section 3 by deleting the definition of "computer" and "computer output" which are no longer necessary in view of the repeal of sections 35 and 36.

Clause 3 amends section 9 by inserting a new illustration. The expression "generated, communicated, received or stored" is adapted from the legal definition of an "electronic record" in section 2 of the Electronic Transactions Act (Cap 88). The references to "reliability of devices" and "circumstances in which the devices were used or operated" are intended to encompass all issues relating to the reliability of

the devices as well as the human or automated agents that use or operate the devices.

Clause 4 repeals sections 35 and 36. The existing rules in sections 35 and 36 will no longer regulate the admissibility of electronic evidence. Instead the existing rules providing for the relevancy and admissibility of evidence (such as hearsay, the best evidence rules and rules on authentication) will regulate the admissibility of electronic evidence in the same manner as any other item of evidence.

Clause 5 amends section 64 by inserting a new Explanation to the effect that if a copy of a document in the form of an electronic record is shown to reflect the "original document" accurately, the copy is primary evidence. The concept of "original document" is of little or no relevance in the context of electronic copies which are identical and perfect. This amendment recognises that electronic copies that are shown to reflect the contents of the original document accurately are original or primary evidence.

Clause 6 amends section 65 as a consequence to the amendment to section 64 made by clause 5.

Clause 7 amends section 68A of the Evidence Act as a consequence of deleting the definition of "computer output".

Clause 8 inserts a new section 81A which introduces four new presumptions in relation to electronic evidence.

Section 81A(1) prescribes an evidential burden similar to sections 146 and 147 of the Australian Commonwealth Evidence Act 1995. Section 81A(1) is a restatement of the common law *maxim praesemuntur omnia rite esse acta*, which is the presumption that mechanical instruments were in order when they were used.

Section 81A(2) prescribes a legal burden and is modelled along the lines of section 5(c) of the Canadian Uniform Electronic Evidence Act ("UEEA"). Section 81A(2) creates a presumption of reliability of

business records of someone who is not a party to the proceeding, where the proponent of the record did not control the making of the record. The concept of business records here is intended to include more than strictly commercial operations. It will apply broadly to enterprise records of organisations not devoted to making a profit, such as Government bodies or non-profit organisations.

Section 81A(3) also prescribes a legal burden and is modelled along the lines of section 5(b) of the Canadian UEEA. Section 81A(3) deals with an electronic record obtained by a proponent from an adverse party and used against that party. The record is presumed reliable. If it is not reliable, then the adverse party has the means to show the unreliability of the record and rebut the presumption, since that party was in control, at the material time, of the record-generation or record-keeping system.

Section 81A(4) defines an "approved process" in a manner consistent with the repealed sections 35(4), (5) and (10)(a). Section 81A(5), introduces the legal presumption consistent with the repealed section 35(10)(b) that a document produced pursuant to an approved process is presumed to accurately reproduce the contents of that document. The effect is that such an electronic record may be primary evidence of that document pursuant to Explanation 3 in section 64.

Clause 9 provides as a transitional measure the continuance of the regulations relating to approved process and certifying authority made under the repealed section 35(5).

EXPENDITURE OF PUBLIC MONEY

This Bill will not involve the Government in any extra financial expenditure.

Computer Evidence Bill.Version D-13 Dec 04

Annexes

Annex 1 : Response from the Singapore Police Force

1. First and foremost, I would like to express my sincere gratitude to the Technology Law Development Group for offering my department the opportunity to present our views on the above paper. It underscores the importance of regular reviews of laws governing the admissibility of evidence especially those of an electronic nature and is timely.

2. We have perused the paper and find that it is very comprehensive and addresses the relevant issues relating to computer output as evidence well. Upon extensive discussions, we are in favour of the amendments as proposed in Option 2. Option 2 adopts a technology-neutral approach that allows for flexibility in the rules of evidence to embrace future changes due to advent in technology. This is vital especially when the pace of development in both software and hardware is expected to increase exponentially in time to come.

3. Repealing certain provisions the Evidence Act will also cut down on some of the current work processes where prosecution of offenders is concerned. This, in turn, may speed up the prosecution process and save precious resources.

Mr Ng Seng Liang
Director CID
Singapore Police Force
3 December 2003

Annex 2 : Response from Mr John Gregory

1. Congratulations! It's a very competent and readable discussion. I hope you get useful feedback.

2. I am particularly interested in this topic, since I was the principal author of the Uniform Electronic Evidence Act ("UEEA") in Canada (with considerable influence from Don Piragoff of the Federal Department of Justice in Ottawa and Joan Remsu of the Federal Department of Justice). I think your discussion of the UEEA is fair and perceptive, though you sometimes discuss its consequences in ways that suggest to me that not all the consequences may have been intended!

3. You take the same position as we did in the UEEA that "electronic evidence does not require any change in the law of hearsay". The hearsay rule goes to the truth of the content of the evidence, not to its medium, and thus does not vary between paper and electronic records.

4. I should note that this view is arduously contested in Canada by one of our principal experts in the field, Ken Chasse (who wrote the Uniform law Conference of Canada ("ULCC")'s first paper on the subject in 1994). He and I have had many debates, online and in person, since the Uniform Act was adopted in 1998.

5. He takes the view that the essence of the hearsay rule is the reliability of the evidence, and that electronic records are subject to so much manipulation, or unintentional degradation, that it is no longer safe to rely on, in particular, the business records rule. It is too easy, he says, for businesses to alter their records, to keep two (or more) sets of books, as it were. So if the books are electronic, they should be subject to additional controls even for the business records/hearsay rule to apply. So far he has not persuaded me, but I have not yet persuaded him, either...

6. I suspect you are right in your general view that the essence of the issue of electronic evidence is the authenti-

cation of that evidence. We stayed away from that conclusion in the UEEA, however, for several reasons.

7. First, Canadian courts tend not to focus on authentication - they rather lump it in with hearsay or best evidence findings. I certainly didn't find much direct discussion of it, either in the case law or in the text books on Canadian evidence law. So the problem with e-evidence seemed to be more whether it was an original or not, so we focused on the best evidence rule.

8. Second, the test for authentication - that the proponent of the evidence present evidence capable of supporting a finding that the evidence was what it purported to be - seems to be fairly easy to satisfy, in the absence of dispute. Bringing in a witness to say under oath, "these are the records of our transactions from 2001 through 2003" satisfies the test. If no one disputes that, the witness does not have to go into more detail, really. The courts don't seem to pursue the witnesses if the other side does not. So we didn't want to set up additional hurdles to the admission of evidence than the courts had - we were trying to remove barriers, not create them.

9. Third, we did not want two sets of hurdles. We thought for a while of just abolishing the best evidence rule for e-records, on the ground that the notion of "original" was just not readilly applicable to them (or some of them - it clearly applies to an electronic image) - and in any event an e-original and an e-copy were usually identical (as you point out in your paper), so the function of demanding an original was not really advanced by requiring originality.

10. Then we thought better of it. We thought - and Don Piragoff was probably the source of the thought - that if e-records were considered to be less reliable, or more subject to manipulation and degradation than paper records (which they are in general, though they can be made more secure than paper with the right technology), then it made no sense to make them easier to admit than paper records.

Getting rid of the best evidence rule for them would have that effect.

11. Therefore we invented a substitute for the originality test for best evidence, which was the system reliability test. This came out of Ken Chasse's 1994 paper. (You probably know that Ontario has added a provision to its implementation of the UEEA, to say that besides the system reliability test, one can satisfy the best evidence rule for e-records by showing that a reliable encryption system was used. I am not sure I was right to have promoted this amendment, though, because one can argue that any encryption procedure is itself a record-keeping system - even if not a complete one - so the usual rule of the UEEA would apply to it anyway).

12. We did not want to have e-records subject to two special tests, one under the best evidence rule (the system integrity test) and another - in the statute or made up by the courts - under the need for authentication. For that reason we codified the authentication rule, to make it clear (we hoped, or at least I hoped) that it was not more demanding for e-records than for any other.

13. I was concerned as well that some of the American discussion of authentication dragged in very complex tests for e-records. I was aware that Canadian courts (and others) generally admitted electronic records, and I was not trying to change that practice. We were trying to set out some clear rules to prevent the whole system from collapsing when clever counsel started asking pointed questions about the authenticity or originality or in general the reliability of e-records that their proponent could not answer. So we tried to keep a tight focus on just what questions were to be asked about e-evidence. That also was a reason for creating the presumptions, which I will discuss in a minute.

14. For those reasons, the UEEA is written to focus on the best evidence rule and to pass over authentication as lightly as possible.

15. However, as a kind of safety net, we also provided (as you note in your [consultation] paper) that any foundation evidence adduced to support the system integrity test under the best evidence rule could also be applied, if need be, to any other admissibility test - authentication or (less likely) hearsay.

16. The presumptions were another way to keep the new rules from keeping out of court records that were typically getting in. The high water mark of admitting records is the *R. v. Bell* and *Bruce* case, reasoned in the Ontario Court of Appeal, with leave to the Supreme Court of Canada refused in 1981, I think. My director at the time I started this work had argued Bell and Bruce for the Crown, and I think he was still happy with it. (That was Doug Ewart, author of Documentary Evidence in Canada, still the leading if not the only text on the subject in our country).

    (Ken Chasse is inclined to fall back on the 1979 Ontario case of R. v McMullen, in which the court sets out a whole list of considerations to address before admitting e-records. Bell and Bruce rather superseded McMullen - perhaps not technically, but practically).

17. So I was getting a message from knowledgeable sources that getting e-records in was not a problem. I can't recall if I mentioned this in my 1997 consultation paper, but during the several years of developing this project, it is largely true to say that I never met a barrister who thought that e-records were a problem, while I never met a solicitor who did not think they were a problem! It's one thing to get particular records into court - it's another to advise clients when they can destroy their paper files because the electronic versions will be all they'll ever need.

18. Anyway, we did not want to create new and expensive barriers to e-evidence. So we limited the scope of the new rules (and tried to prevent them from spilling over into authentication), and we provided presumptions. The different formulation for the first presumption (s. 5(a) of the UEEA) was a late addition, from Don Piragoff.

19. I am not sure I read the Australian language of presumption much differently from ours, I must say. I do agree with you that our presumption is intended to be easily rebuttable - the opponent does not have to prove the contrary, just raise evidence to the contrary. After that, the parties are on their own - no presumption - and then one gets into the reliance on standards etc etc.

20. The presumption for one's own records is obviously inspired by the English statute, but as modified by the Stewart case, so an irrelevant misfunction was not fatal to admission. We were not thinking of what you call computer-generated evidence, as you rightly point out. A criminal law specialist in Ontario spelled out that difference to me, possibly after the adoption of the UEEA - but it does not seem to be a problem.

21. I do recall a conversation with a very senior Canadian barrister about the UEEA in draft, and he was not prepared to confirm to me that Canadian law knew any such presumption as English law had, that machines were presumed to function correctly. Certainly I did not feel that we could rely on such a presumption to support computer-stored records generally as evidence.

22. The machines that produce computer-generated evidence are not presumed reliable until the courts are very familiar with them. At present, breath-analysers are considered reliable, but one model was successfully attacked at a trial a couple of years ago - and of course the usual routine about custody of samples and expertise of operators needs to be gone through in each case. We had a similar debate when we were doing our law to support photo-radar speeding tickets. (I could send you an article I wrote on that subject - but unfortunately for the law (and for drivers, I think), the government changed and the new government (in 1995) scrapped the program before several interesting legal questions could be resolved about how the system operated.

23. The presumptions about the other party's records and third party records we just made up. Originally we had a presumption about any other party's records, but after thinking about the possibility of collusion - you submit my records and I'll submit yours - we limited it to adverse parties. I still think that's a clever one. Your formulation in Part IV of your Consultation Paper is however a good one - the presumption covers the generation of the record in the hands of the adverse party, but once the record comes into the hands of the proponent, the proponent has to account for its integrity. We had in mind mainly documents produced on discovery, though the rule is more broadly worded.

24. All that said, I return to my admission that probably the real issue is authentication. The question then is whether you need any special rule for authenticating electronic records. I am inclined to support your recommendation on that - *i.e.* Option 2 - no special hurdle, no special demand, but some qualified easing of barriers that might otherwise arise. I don't think I was aware of the English Law Commission's recommendations from 1995 till after we had completed the UEEA - if so, I thought there was good reason not to follow - including that we were not going down the full demanding, certificate-supported route that the English had adopted in 1988 - so the criticisms of the English rules did not apply to us (I thought).

25. I agree with your general approach, which is that people are becoming more comfortable with e-records as the years go by, and nervousness that appears in 1985 or even 1995 is dissipating. One sees this in e-commerce statutes too - compare early versions of what became the Model Law on Electronic Commerce to the final and early implementing statutes (like yours) to later ones (like ours - and even within Canada...). The main purpose of these statutes is probably to let lawyers relax, since their clients are out there doing e-commerce and making and keeping e-records anyway.

26. The question in my mind in the mid-90s, and still there to some extent, is how to prevent the need for full-scale technical defences of e-records once one makes an authentication question of them. The proper answer is probably that one should not prevent a full-scale inquiry if the records appear to need it. One can facilitate the passage of records that do not appear to need it, though - through presumptions, or through procedural means (we have a "notice to admit" process in our Rules of Civil Procedure by which one party tells the other a set time before trial what documents the party will produce, and if the other party does not object within a fairly tight time limit, no objection can be brought at trial).

27. We also referred to standards. Three comments - or maybe four - on standards

(i) The language is intended to be broad enough to cover a bilateral standard, *i.e.* an agreement between the parties. Earlier versions of the UEEA had an express permission for the parties to agree, but that was attacked, mainly by criminal lawyers, as improper, since the court had to control what it admitted and the parties could not change the law of evidence by private agreement. No doubt it works better for civil cases.

(ii) We were under pressure to allow for the use of a Canadian General Standard Board Standard on the Use of Electronic Imaging and Microfilm as Documentary Evidence - adopted in 1993 based on a 1988 standard on microfilm alone. We resisted any reference to that standard in the Act, for various reasons I could tell you about if you wanted to know - but the standards people were happy enough with the general openness to standards we put in. I don't think that changed the existing law, though - I think the courts were always free to refer to applicable standards.

(iii) The CGSB is now in the late stages of adopting a standard on electronic records as evidence. In principle it should be helpful to records managers to tell them what to think about to keep their records admissible. Much of its language seems derived from the UEEA, though, and the federal implementation of it. When I read your recommendation and its reminder of the Law Commission's recommendation, I wonder if the Standard is too closely wed to the UEEA - and perhaps the UEEA is not the guidepost it used to be. Nothing you can do about that, of course, and there is something I can do about it, since I am attending meetings of the drafting committee for the new standard. But you may be interested in the existence (forthcoming...) of the Standard.

(iv) You may be familiar with Quebec's law on this subject - there is some material in the Civil Code of Quebec (1994), including a business records rule (article 2770 or 2870 I think). The big statute, adopted in 2001, is the Act to provide a legal framework for information technology. You can Google it under that name and find it, or search the Canadian Legal Information Institute site for it (www.canlii.org). It has some language about what a document is, and the neutrality of the law between media, and the migration of information from one medium to another, etc, that is very interesting - which is not to say it has to be legislated for all purposes.... that Act also has some later sections (about s.60) on standards and their development and application.

28. All that (much) said, I am inclined to support your recommendations. I think your Option 2 makes much sense. You may need something to dispose of the best evidence rule, and your proposal is probably OK on that. I'm not sure our courts make as firm a distinction as you suggest between original and secondary evidence. (Quebec's statute makes such a distinction, in different language.) You may

have read the paper by Ed Tollefson for the ULCC in 1995 (all the papers are on the ULCC web site - that one in the Proceedings for 1995), who supported a distinction between original and duplicate, probably influenced by the American rules. Otherwise you could just say that a print-out is an original, for the purposes of the best evidence rule, if it is shown (or the contrary is not shown, or presumed...) that it reproduces what is in the computer.

29. After we had completed the UEEA, some barristers said it was a shame to focus so much on the best evidence rule, because the courts had basically stopped talking about it, They were just letting any evidence in, and dealing with questions of integrity etc as matters of weight. (Where were they during the years we tried to get some reaction out of the profession on the topic, you might well ask!) The 1996 paper for the ULCC, by Hamish Smith (on why one needed to legislate on the topic) had also made the point that courts were tending to move away from admissibility to weight. (And we decided very consciously in the UEEA not to say anything about weight, though we toyed with something like article 9 of the Model Law on E-Commerce, before deciding that the first part was wrong and the second part was self-evident.)

30. But then a couple of Canadian courts - or administrative tribunals - made a couple of big decisions based on best evidence principles, so I felt less bad about the UEEA...

31. I doubt that you need to do much to the definition of document. In our uniform statute to implement the UN Model Law, we speak of electronic documents, but we did not define document - we figured everyone knew what a document is... We did have one law firm complain that "electronic document" was a non-sense, but everyone else seems comfortable enough with it. (We stopped talking about "records" largely because the term is very hard to translate satisfactorily into French, and we adopt our uniform - and federal, and several provinces' - statutes in English and French. Also, archivists say a record is a document that is in a record-keeping system. The ISO has

some other definitions that become very confusing - the short of it is that there is no consensus among specialists, so legislation should probably just choose the street meaning.)

32. I have probably given you something on most of your questions, except the ones directly dealing with the Singapore legislation itself.

- **Should the rules be technology neutral?** Yes. (which doesn't prevent a presumption based on a secure e-signature, if you must. The federal law of Canada gives one, but in three and a half years since adopting their statute, they have not done a regulation to say what a secure electronic signature is.)

- **Should the definitions of computer and computer output be retained?** I doubt it - this question may be made unnecessary by choosing option 2. I am rather sorry we put the definition of computer system into the UEEA. This was mainly because such a definition was already in the Canada Evidence Act, which is where the UEEA was going to go, in its federal life. But I'm afraid it narrows the application of the Act unduly. (There is almost no case law on the various implementations of the UEEA – because it's admirably clear, or because it's irrelevant?)

- **Do the real evidence rule and hearsay rule continue to be relevant?** I think so - but they don't change because the evidence is electronic.

- **Should there be a provision for the admission of e-business records?** Not especially.

- **Should there be a provision to admit e-records as an exception to the hearsay rule?** No.

- **Can issues of reliability be dealt with as matters of authentication?** Largely yes (and this note and your paper have lots of the qualifications.)

- **Should the best evidence rule be retained?** Yes, for the reason we kept it. But you don't have to deal with it in as heavy-handed a way as we did in the UEEA - go with the American-inspired way you suggest in the paper. If it works, maybe we'll follow in a few years... (but getting uniform legislation is not fast work in Canada).

33. Good luck in your wrapping up this project. I am very interested in where you go from here, and what you hear in response to your consultation.

34. I would of course be happy to follow up on any of this discussion, if you would like. I am afraid I have presumed (in a non-legal way) upon your interest in the minutiae of the Canadian policy development. Probably you knew much of this already but did not find it necessary to reflect it in your paper.

Mr John D. Gregory
Toronto, Ontario, Canada
30 November 2003

Annex 3 : Response from Ms Yee Fen Lim

1. I must congratulate you on your excellent Consultation Paper "Computer Output as Evidence". It is a very thorough and useful analysis of the different regimes governing the area in many jurisdictions around the world.

2. The Options for Reform contained in Part IV is meticulously written and argued and very carefully thought out. I have to say that I personally think Option 2 would be the preferred option. I'm not convinced that Option 3 will indeed perform an effective function in responding to the needs of the business community in terms of business records. Option 4, whilst less of a radical change and espouses an incremental change approach is not in keeping with the international trend.

3. Options 1 and 2 embraces the technology-neutral approach that has been adopted in so many legal instruments that have responded to changes in information technology. Option 1 certainly allows for full flexibility but I wonder whether it is wise to have a change from a presently very prescriptive regime to one offering very little legislative guidance.

4. I congratulate you on the proposals outlined in Option 2. The adoption of the presumptions certainly would guide the business community, legal profession and judiciary in adjusting to the new regime. Further, there is existing bodies of law in jurisdictions such as Canada and Australia from which guidance can be drawn. Indeed, as you correctly pointed out in paragraph 4.18, the Canadian UEEA are an expanded version of the Australian Commonwealth Evidence Act, the Canadians having embarked on their law reform processes several years after Australia. The suggested presumptions in paragraph 4.22 without a doubt do simplify the admissibility issues, as they have done so in Canada and the reasons for their adoption in Singapore are extremely cogent.

5. Thank you for sharing with me your reform proposals - it has been a very interesting and enlightening read.

Ms Yee Fen Lim
Senior Lecturer in Law
Department of Law
Division of Law
Macquarie University
Sydney New South Wales

&

Visiting Professor
Centre for Asia Pacific Technology Law and Policy
Nanyang Business School
Nanyang Technological University
Singapore
17 November 2003

Annex 4 : Response from IBM Global Services – Asia Pacific

1. Computer evidence is not what we read, or what we see on the screen. Those are "views".

2. What is evidence is really ordered compilations of binary data, *i.e.*, zeroes and ones. These zeroes and ones are rendered by one or more computing process (which are themselves comprised of zeroes and ones) to become human readable. Read in their native format, one set of binary data is completely unreadable by human perception and therefore it's content, as well as time of creation (the when and the what, rather than the "who") is indistinguishable from any other set of binary data, including fraudulently manipulated or created data. Unless these zeroes and ones can be anchored and authenticated in some reliable way not under the control of human intervention, digital data, and computer output, is highly suspect.

3. There is vulnerability in current computing environments that may affect both admissibility as well as weight of digital evidence. That vulnerability is the insider control over time in the data generating system. Where insider control over network time exists, the capability for digital data fraud (manipulation, re-creation, substitution or alteration) exists.

4. Computer Output: We would submit that computer output is binary data, ordered sets of zeroes and ones, and nothing else.

   Current Admissibility Standards: Compliance with these conditions is accomplished by the certificate issued by an individual who is considered an "insider" to the data generation process.

5. Express Agreement: What if there is an express agreement between the parties as to the content of the evidence, but one party is not aware that the other has engaged in time-

base data manipulation. It may be that such fraud can never be discovered (especially if the fraudulent data is backdated and substituted for the true data)

6. Approved Process: In this method, a certificate signed by a person holding a responsible position in relation to the operation or management of the process certifies that the output (or data) is obtained from an approved process. The approved process still does not remove or otherwise inhibit the ability of an insider to engage in unauthorized time-based data manipulation, because the time is erroneously presumed to be fixed.

7. Proof of Operation and Accuracy: This method presents similar issues.

   Requirement One: No reasonable ground for believing output is inaccurate because of improper use, and that no reason exists to doubt or suspect the truth or the reliability of the. This requirement poses challenges in that the re-setting of time in a computer can be seen as an aspect of proper operation, but may involve improper use. Further, if an insider has engaged in improper time-based data manipulation, it will be impossible to ascertain after the fact what has been altered or tampered. In the United States, the Rite Aid lawsuit brought by the SEC noted that the original data that had been tampered and altered could never be retrieved or "audited".

   Requirement Two: Reasonable grounds to believe at all material times that the computer was operating properly. Again, a computer may operate properly, but the time-based manipulation and vulnerability (i.e., re-setting the system clock) is a predicate to what is commonly accepted as proper operation.

Questions:

8. What is meant by a "time-stamp" in 3.86? We respectfully submit that there is much confusion as to the meaning of this term. Legally it may mean one thing, but in the technology world it could have three meanings. The "time-stamp" could be a time-mark, a time stamp, or a trusted time stamp. Each has far reaching implications for authenticating the "when" and the "what" of electronic data. For instance, if this is merely an unencrypted data string, or is an encrypted data string containing time from an untrusted source, then it is not a "time-stamp" per se, but a time-mark, and easily changed by the data generator.

9. In [paragraph] 3.90, it is mentioned that integrity considerations include the requirement that the object that is involved remain substantially unchanged when it presented, and that it is relatively impervious to change. If electronic data can be shown to be easily prone to change, would it then be considered inadmissible under Singapore law?

Proposed Options to Amend S35 & 536

10. It is our position that Option 2, which would provide a non-computer specific approach but provide presumptions to facilitate admissibility of electronic evidence, and Option 4, which would ease the rules of admissibility, fail to take into account the intrinsic vulnerability of currently generated electronic data. This vulnerability exists for both enterprise, the government, as well as private or small business user electronic data generating environments.

11. If altering, substituting, deleting, modifying, or re-creating backdated originals is as easy as setting the computer clock back in time (and it is), then any admissibility and authentication schema must include some provision for either a showing by strong testimonial proof, or by technology which provides such authentication without need for human intervention. Further, such technology, which

authenticates content as a function of time irrespective of testimony, should by imbued with a much higher degree of reliability, weight, as well as admissibility as compared with electronic content which has not been so authenticated.

Ms Judy Kon
Strategy & Engagement Executive
EBO IBM Global Services Asia Pacific
27 November 2003

Annex 5 : Response from the IT Committee and the Electronic Litigation Committee, Law Society, Singapore

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

2. The point to be made is that the time is right for a review of the rules of evidence relating to admissibility of computer output. lt is not necessary to determine whether there is presently a higher standard for admissibility, contrary to the equivalence principle. Further, it may be difficult to apply any equivalence principle, as that would presuppose the existence of traditional rules of evidence that can be equated with those relating to the admissibility of computer output as computer output. See further the final answer to the list of questions.

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

4. Again, the rules of admissibility should be reviewed with a view where possible to facilitating the admissibility of electronic evidence. At this juncture, section 35 has not fully been tested by the courts, but we need not wait to see whether section 35 unnecessarily interferes or limits the admissibility of electronic evidence to undertake the review. In our opinion, however, section 35 may be unduly restrictive and should be reformed. At the same time, if there are changes to be made to the law, transitional provisions should be made to ensure that previously admissible electronic evidence do not suddenly somehow become not admissible, unless there is a deliberate policy to do so.

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

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

8. Definitions should as far as possible be technology neutral and in this respect, it may be less important what term is used if the term is defined clearly.

9. Should the definition of the term "document" in the Evidence Act be revised to include electronic records?

10. No, unless a thorough review of the law is undertaken. For one, including electronic records within the definition of "document" may subject electronic records to the rule of evidence relating to primary and secondary evidence, which rules may not be fully appropriate for electronic evidence.

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

12. Unless electronic evidence merits special treatment, the hearsay rule and the real evidence rule should continue to be applied. It may, however, be difficult to see how electronic evidence may be admitted as real evidence, when by definition real evidence precludes human intervention. At least at this stage of technology, they would invariably be human intervention.

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

14. Only if there are similar exceptions made in the case of paper business records. The point to be made is that once record (whether physical or electronic) is admitted for the authenticity of its contents, the same hearsay rules should apply.

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

16. Only if there is a similar exception for other comparable evidence.

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

18. No, as reliability (in the sense of the likely truth of the contents) is somewhat distinct from authentication.

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

20. Yes, but with exceptions made to recognise that they can be other forms of electronic evidence which may be as good as what may be regarded as the best electronic evidence.

21. Should sections 35 and 36 of the Evidence Act be the subject of legal reform? lf 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?

22. The rules of admissibility should only govern admissibility of computer output as computer output. This is in contrast with admissibility of computer output per se, whatever the purpose that the computer output is sought to be admitted. The difference between the two formulations is that in the former, for the proposed rules of admissibility to govern, there must exist the purpose of admissibility as computer output as computer output, whereas in the latter, such a purpose need not exist (and the rules relating to admissibility apply automatically on the basis that it is computer output).

23. Accordingly, say two parties following negotiations reduce their agreement into an electronic document that is printed out. Subsequently, when a dispute arises, one of the parties seeks to produce the physical printout. lf the former formulation is adopted, the printout that is sought to be admitted into evidence as a physical document in the

ordinary way would not be subject to the additional rules relating to admissibility of computer output, since the computer output (i.e. the printout) is not sought to be admitted as computer output but as a document itself. lf the latter formulation were adopted, the rules for admissibility of computer output would govern on the basis that the printout is computer output.

24. To further illustrate the point, say that the original printout is lost, and what is sought to be admitted is a further printout, on the basis that it is identical to the original. In such a case, the rules relating to computer output should govern.

25. We submit that the latter formulation should be rejected, as if computer output is not sought to be admitted as computer output, it should not be subject to the rules relating to computer output. This is because there would otherwise be a mismatch between the rules governing admissibility of computer output and the admission computer output that is not sought to be admitted as computer output. To take the example in the previous paragraph, if the computer printout is subject to the rules, it would mean for example that the authenticity of the physical printout ought to be tested on he rules for admissibility of computer output (and not for the admissibility of documents), such as that it was printed out by a properly working computer etc. Consequently, all computer printouts may be subject to the rules for admissibility. Given the pervasive use of computers, this may be undesirable and at any rate unnecessary.

26. In addition, one should not be overly concerned that computer output sought to be admitted for purposes other than computer output may be too easily admissible if the rules relating to admissibility of computer output do not apply to them. This is because if a person seeks to admit computer output other than as computer output, their admission must be justified or consistent with other rules of evidence governing their admission. For example, com-

puter output that is sought to be admitted as a document must satisfy the rules for admissibility of documents. As a further example, if tests are conducted by experts using computers, and the printout of the results of such tests are exhibited (in the expert report) and utilized by the expert in reaching his conclusions, the rules relating to admissibility of expert evidence, in particular that relating to the grounds for expert opinion, would govern.

27. We would add that the technique of determining whether the rules of evidence should apply depending on the purpose for which the evidence is tendered is a technique that is not unknown. lt is a technique used in the area of hearsay evidence, in that the hearsay rules only apply where the purpose of the hearsay is admitted for the purpose of proving the truth of its contents.

28. We would accordingly suggest that the review should proceed on the basis that the rules of admissibility to be devised relating to computer output should only govern computer output sought to be admitted as computer output. One incidental benefit of such an approach is that the rules relating to admissibility of computer output can be tailor fitted to the situation where the rules are intended to apply, i.e. when the evidence is sought to be admitted as computer output.

29. In a situation where computer output be is sought to admitted as computer output, we would suggest:

a. A broad principle admissibility depending on accuracy, authenticity and reliability of the output, and for computer output to be admitted when they satisfy these requirements. In clear and obvious cases, the courts should additionally be allowed to exercise discretion to admit the evidence. For instance, what may be sought to be admitted is a digital photograph with which no controversy whatsoever arises on the facts. In such circum-

stances, the court should be allowed to admit evidence without any formality of admitting the evidence as computer output.

b. For certainty but without prejudice to the broad principle for admissibility, there should be various "safe harbours" where computer output would be admitted. Where the evidence satisfy the requirements of a "safe habour", they should be admitted unless it can be shown by the party resisting admission that they do not satisfy the broad principle for admission outlined in the previous paragraph. Such "safe harbour" grounds could include the current ground for admissibility of documents produced in an approved process, but with an appropriate review with a view to liberalisation. One reason why the "approved process" ground for admission should be retained is that the Evidence (Computer Output) Regulations has been accepted by the IRAS in its guide for "Keeping of Records In Imaging System". The abolition of the provisions for approved processes may result in the evidential rules for admissibility and the rules governing retention of records that the IRAS guide is concerned with, being out of sync. The "safe harbours" could also include instances where they are sanctioned processes for retention of documents that are prescribed in order to meet statutory obligations of retention. The IRAS guides for "Keeping Machine-sensible Records & Electronic Invoicing" and "Keeping of Records In Imaging System" would fulfill such criteria to be "safe harbours".

c. They should continue to be a ground for admission of electronic evidence by agreement of the parties.

d. Express provision should be made to allow as a separate specific ground of admissibility, the admissibility of computer output via expert evidence.

Mr Andrew Chan Chee Yin

IT Committee and Electronic Litigation Committee of the Law Society (Views expressed do not necessarily represent the views of the Law Society, Singapore)

28 November 2003

Annex 6 : Response from the Supreme Court, Singapore

Introduction

1. Rapid advancements in information technology pose new challenges to the rules of evidence and necessitate the need for review of the existing legal framework relating to the admissibility of computer output (as set out, inter alia, in sections 35 and 36 of the Evidence Act). Accordingly, having conducted a survey of the computer output admissibility provisions in selected jurisdictions (Canada, the United States, the United Kingdom, Australia, South Africa, India and Malaysia) and identified the existing inadequacies and limitations in Singapore's current approach, the 2003 consultation paper ("paper") of the SAL's Technology Law Development Group ("TLDG") proposes four options for reforming Singapore's current approach toward the admission of electronic evidence.

2. In a nutshell, the TLDG's view is that rather than continue with sections 35 and 36, it is preferable to adopt a "technology-neutral non-computer specific" approach to admit electronic evidence. Among other reasons, computer output is no longer confined to computer printouts and scanned documents but extends to electronic records generated and stored by a wide range of data processing, storage and transmission devices such as electronic organisers, mobile phones and digital cameras. The TLDG further proposes the use of presumptions to facilitate the admission of electronic evidence, as set out in greater detail in Option 2.

Options for Reform

3. The options for reform 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.

Each of these options are described more fully in turn.

Option 1. Non-computer specific approach

4. This approach, which is similar to that in the US Federal Rules of Evidence and the new UK approach (a mixture of statutory provisions and common law rules), is based on the principle of non-discrimination which requires that electronic evidence be treated no differently from evidence not in electronic form. Accordingly, sections 35 and 36 will not regulate the admissibility of electronic evidence; instead, the existing rules providing for the relevancy and admissibility of evidence will apply to admit electronic evidence in the same manner as any other type of evidence. The following changes to the Evidence Act will have to be effected:

    - Repeal the computer specific provisions (sections 35 and 36) and the computer specific definitions (in section 3) of the Evidence Act.

    - If necessary, expand the scope of the term "document" defined in section 3 to include electronic records, or redefine the term "evidence" to include such "electronic records".

    - Modify the best evidence rule (sections 35(10),65 and 66 of the Evidence Act) to require production of "original" copes of electronic documents where the copies are electronically identical to the original, but

admitting such "copies" only where the reproduction measures reproduce the "original" accurately.

5. Option 1 involves judicial assessment of, and discretion in, assessing electronic evidence to address issues of hearsay, authentication and best evidence. The courts are given wide discretion to call for authenticating evidence in any manner it deems appropriate, rather than prescribing the express requirements that the proponent of the electronic evidence must satisfy before the evidence can be considered for admissibility. As such, there is a great deal of flexibility. So, for instance, where the evidence is from a reliable and trustworthy source or there is little room for dispute that it is reliable, the court can more readily admit the evidence with little or no supporting evidence to authenticate it. Further, this option does not envisage any specific provisions to deal with considerations of weight, as such issues can be adequately dealt with as issues of authentication. In any event, even if a piece of evidence is found to be authentic, it is always open to the court to attach little weight to it. In summary, although there are plainly advantages to adopting Option 1, it does not afford any guidance as regards the proper use and admissibility of electronic evidence. Flexibility is achieved at the expense of certainty.

Option 2. Non-computer specific approach with presumptions

6. Option 2 is similar to Option 1. In addition, it is recommended that there be specific evidentiary (as opposed to legal) presumptions to facilitate the admissibility of certain types of electronic evidence. The rationale is that some types of electronic evidence are inherently more reliable than others, so rules should exist to facilitate their admissibility. More precisely, such electronic evidence will be those that are more readily authenticated than other types of electronic evidence.

7. Several advantages flow from the adoption of this approach. First, it combines the technology-neutral

approach of Option I with the recognition of the need for specific rules to facilitate the admissibility of electronic evidence in certain circumstances. It achieves this by focusing on the issue of authentication of such evidence. Second, the proposed presumptions (see infra) provide for ease of admissibility of electronic records by ensuring that in most cases, the authentication requirements as to admissibility of electronic business records (which will form the majority of electronic evidence adduced in evidence) are readily satisfied. Third, the use of presumptions avoids the formalism of compliance with statutory preconditions to admissibility such as the certification process (which often have little,, if any. bearing on the authentication issues before the court).

8. Apart from serving indirectly as a form of transition from the existing legal regime, this option also has the additional advantage of the desired certainty and predictability for businesses or organisations with electronic records.

9. The recommended changes to be effected pursuant to Option2, in addition to those listed under Option 1, are as follows. They involve the introduction of three new illustrations to section 9 of the Evidence Act to provide for three evidentiary presumptions:

- 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.

- Electronic evidence generated, recorded or stored in the usual and ordinary course of business by a neutral third party is presumed to be authentic.

- Where an electronic device or process is one that, or is of a kind that, if properly used, ordinarily produces that electronic record or document, it is presumed that the

electronic device or process produced that electronic record or document.

Each of these presumptions is to stand unless evidence sufficient to raise doubt about that presumption is adduced. The first presumption (also known as the "adverse party rule"), for example, is based on the notion of control; the party who has control over the generation, recording or storage of electronic records is the best party to prove authenticity. The onus is on that party to show that his record keeping system is unreliable. With regard to the second presumption, also known as the "neutral third party rule", there is an assumption that a neutral third party is less likely to have reasons to fabricate evidence in favour of either the proponent or the opponent. Such a third party would invariably have produced the evidence independently of either the proponent or the opponent.

Option 3. Business records approach

10. The business records approach provides a mechanism for the easy admissibility of business records in general, which will include electronic business records as stored records. Business records are, of course, already admissible pursuant to section 32(b) of the Evidence Act as an exception to the hearsay rule. This option envisages 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.

11. The objective is to provide an easy admissibility mechanism for the records maintained in electronic form by the business community. As most electronic records admitted in evidence are business records, and many organisations have expended resources to computerise their operations and store business records in electronic form the Supreme Court is a case in point), Option 3 acknowledges this reality and responds to the needs of these organisations. It also recognises that business records are generally presumed to be inherently reliable.

12. However, in the view of the TLDG, this approach lacks utility. First, its scope is rather narrow as it applies only to records retained in the course of business and not to non-business documents. For the latter category, the general rules of evidence remain applicable. This approach fails to provide rules and offers no guidance for dealing with electronic non-business records such as personal e-mail and chat-room logs. Second, since the provision envisages a "three-in-one" rule, the proponent of a business record will have to satisfy certain prescribed statutory conditions to ensure general reliability and integrity of the record. Proof of this may take the form of a certification process, which is not ideal. Among other things, a certificate gives no assurance as to the correctness and reliability of the contents of the business record so certified, for example where there is manifest error evident on the face of the record. Third, as this option is premised on the business record falling within the business records exception as proof of its authenticity, it has no application to business records that are real evidence.

13. If adopted, the existing rule in section 32(b) must be modified to state that where written statements of relevant facts are relevant facts pursuant to that section, notwithstanding sections 9, [35], 65, 66 and 67, they may be proved by the production of a document 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 existing approach

14. Option 4 is similar to the computer specific approach in sections 35 and 36 of the Evidence Act, and 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 proposed amendments to the statutory provisions therefore take these issues into account and provide a structured

and elaborate mechanism that prescribes the preconditions for the admissibility of electronic evidence. The mechanism will serve as an instructive guide to the proponent of the evidence and the court as to the evidentiary issues to be considered when admitting the evidence.

15. The TLDG is not in favour of this option, as it indiscriminately assumes that all electronic records are unreliable and prone to error. However, it accepts that the value of this approach is in its instruction to the proponent and the court.

16. What is proposed are incremental modifications to the existing sections 35 and 36. Three modes of admissibility will supplement rather than exclude the existing common law rules of admissibility of electronic evidence. The revised section 35 will state the broad principles relating to the authentication of computer output, but the three modes of admissibility will be "inclusionary" and "descriptive". Not "exhaustive" and "prescriptive". The recommended changes 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.

- 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 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.

- Modify and revise section 35(6), (7) and (8) to provide that an affidavit made by any qualified person in relation to the computer output may be, tendered to authenticate such output. The court will retain the dis-

cretion to decide if the maker of an affidavit is such a qualified person to make the affidavit so tendered.

- 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; and
  - where a compliant certificate is issued pursuant to section 35(6), (7) or (8) (as modified), it shall be presumed. unless the contrary is proved, that the output is authentic.

17. The objective of making incremental modification to section 35 is to ensure that the complex and cumbersome process of certification is simplified, and captures the current practice in many cases. Option 4 is the opposite of Option l: it achieves certainty and predictability, but at the expense of flexibility.

Comment

18. In *Lim Mong Hong v Public Prosecutor* [2003] 3 SLR 88, the learned Chief Justice noted that section 35 of the Evidence Act was a reflection of the way our laws of evidence have had to adapt to the realities of modern business practices. His Honour also observed that computers today play a pervasive role in society and with the increase in computerisation of records, it is to be expected that more and more computer output will be presented in evidence. Indeed, this was a prescient observation as more forms of electronic evidence are increasingly accepted and used in a variety of contexts.

19. That *Lim Mong Hong* is to date the only case authority dealing with the admission in evidence of computer output, however perhaps illustrates the underdeveloped state of the law on this area in Singapore. Several questions arise - Do the courts have so much confidence in relying on electronic evidence that they see no need to apply the rules in

sections 35 and 36 of the Evidence Act? Do counsels think it is unnecessary to raise issues of, say, hearsay or authentication, or can it be characterised as collective ignorance of the law? Are these issues at all important?

20. The decision in *Lim Mong Hong* makes it clear that the court was mindful of the underlying rationale of section 35. Reference was made to the statement of the Minister for Law, Professor Jayakumar, at the second reading of the Evidence (Amendment) Bill, that the amendments "strike a balance between guaranteeing the reliability of evidence produced by such technologies and ensuring that the admissibility of such evidence is not hampered by' complicated conditions and procedures." This was to be achieved by requiring those who wish to adduce computer output into evidence to establish that it will be safe for the court to rely on such evidence. Plainly, this approach was a manifestation of the fundamental distrust of all forms of electronic evidence.

21. Since then, advancements in software and hardware technologies, the exponential growth in usage of the Internet after the passage of the amendment Bill, and indeed the widespread acceptance of computer output (broadly defined) in the business community, necessitate revising the current approach and perhaps rethinking this distrust. The perception that all forms of electronic evidence are unreliable and prone to error is no longer valid, although issues of integrity and authenticity remain. In this regard, Option 1 may not be suitable for adoption. In the US, for instance, email which cannot be verified (for example, where there is no digital signature) is treated with some degree of skepticism, but the courts have the benefit of a significant pool of case law with precedential and instructive value. In comparison, Singapore courts lack such a fund of experience to guide them. Hence, Option 2 aptly strikes a balance between flexibility on the one hand and predictability on the other. That it focuses on the issue of authentication means that a court need not rely on presumptions of system integrity where there is some other evidence to suggest that the electronic evidence produced or generated

by the system is reliable. Conversely, a data input error independent of the record keeping process or a manifest error such as a double entry will vitiate the presumption of an authenticated electronic record. For the foregoing reasons, we respectfully concur with the view of the TLDG and submit that Option 2 would be the best course for Singapore.

Mr Foo Chee Hok,
Deputy Registrar
Supreme Court of Singapore
2 January 2004

Annex 7 : Response from Drew & Napier LLC, Singapore

1. We refer to the Technology Law Development Group's ("TLDG") Consultation Paper ("Consultation Paper") on Computer Output as Evidence.

2. The Consultation Paper requested for comments and feedback on Sections 35 and 36 of the Evidence Act ("EA"). We appreciate the opportunity to share our views with TLDG and our response is set out below.

3. In summary, we agree with the position that Sections 35 and 36 raises the admissibility standards admitting electronic evidence in a manner that is unnecessarily inconvenient. Consequently, we agree that the EA should be amended so that electronic evidence may be admitted more easily.

4. We are not in favour of repealing Sections 35 and 36 altogether. These provisions were enacted to ensure that any electronic evidence sought to be admitted is not hearsay and is reliable. This is an important safeguard and must remain in place to ensure the integrity of electronic evidence.

5. Our view is that a variation of Option 2 is the most appropriate reform moving forward.

Sections 35 and 36 create unnecessary and burdensome admission standards

6. We agree with the TLDG's submission that the requirements under these provisions, particularly Sections 35(1)(a) to (c), make the admission of electronic evidence burdensome.

7. Given the wide definition of "computer output", just about every conceivable form of electronic evidence will be captured by Section 35 if it is tendered in court as evidence. We share the TLDG's view that this produces an undesirable result because of the prevalent use of elec-

tronic communications, computers and other devices in this day and age. Our experience confirms this view.

8. First, we note that the use of Section 35(1)(a) to admit electronic evidence is not common, largely because an agreement to admit electronic evidence is almost never discussed between parties at the time an agreement is negotiated or entered into. When the parties' relationship has deteriorated to the point of litigation, an agreement to admit electronic evidence is, not surprisingly, less than forthcoming. Moreover, as pointed out in paragraph 3.25 of the Consultation Paper, in the case of criminal proceedings, an accused is unlikely to agree to admit electronic evidence under Section 35(1)(a).

9. Second, Section 35(1)(b) has hardly come under judicial scrutiny since it would appear that only IRAS has an "approved process".

10. This leaves Section 35(1)(c) as the most commonly used provision for the admission of electronic evidence. However, as the TLDG pertinently pointed out, Section 35(1)(c) imposes several requirements to be satisfied, the cumulative effect of which is a burdensome process to admit even the most trivial and mundane electronic evidence. As a result of practical experience, we have previously encountered considerable difficulty in seeking to adduce computer output in our courts. In one such instance, our clients were French and the computer printout came from our client's head office's computer system in France. The data system administrator was also in France. In order to adduce the computer printout, we had to call a witness here just to say the system was functioning and to testify as to the reliability and accuracy of the system/output.

11. As such, our view is that the EA ought to be amended to relax the rules and "hurdles" imposed by Sections 35 and 36, and to permit the easier admission of computer output as evidence.

Repealing Sections 35 and 36 altogether

12. Computer devices will become more prevalent in future. Business processes and individual lifestyles will be increasingly computerized. The ubiquity of computing devices in our everyday lives inevitably means that it will become more and more common to rely on computer output as evidence in court.

13. As such, our view is that the time has come to recognize that there is no reason to treat computer output any differently from other forms of documentary evidence and to get over the mistrust of computers. By analogy, where authenticity of a document is not admitted, there are already established precedents to adduce expert evidence (such as the calling of handwriting analysis experts to give evidence on the authenticity of signatures and handwritten documents). In the same way, there is no reason why a computer systems expert would not be able to give evidence as to the authenticity of emails and other forms of electronic communications.

14. In support of this view, our experience is that litigating parties are now trying to take a more sensible approach by agreeing on the authenticity of documents that are in the form of emails and printouts etc. We believe a large part of the reason stems from the desire to avoid the cumbersome and onerous procedure under Sections 35 and 36. Clearly the trend is to move away from these provisions.

15. Our experience and reasons in these paragraphs 6 to 14 above are tempting reasons to support sweeping reforms such as Option 1.

Sections 35 and 36 are necessary safeguards

16. Having said that, we are not in favour of repealing Sections 35 and 36 altogether.

17. In our view, shedding our suspicion of computers completely and repealing these provisions altogether, is a risk. In time to come, parties and courts alike may accept com-

puter evidence without a blink, disregarding the fact that computers, as devices, may occasionally fail to function as it was designed or suffer from bugs and other errors etc and therefore produce a result that is manifestly wrong. This is where the philosophy behind Sections 35 and 36 become relevant.

18. Sections 35 and 36 were enacted to test the veracity of computer output as evidence and it is essentially a provision instituted to exclude computer output that is hearsay and/or computer output that is unreliable. While we agree that the provisions should be amended to be less burdensome, it should not be relaxed to the point that hearsay or inaccurate computer output finds itself admitted without check.

19. We take our cue from the TLDG's distinction between computer output as real evidence and computer output as hearsay.

20. We agree that for the purposes of the EA, evidence may be produced by electronic devices that store information and electronic devices that process information.

21. In the case of the first category, we accept that the hearsay rule must apply to computer output emanating from such devices because the information produced from such devices were input by humans in the first place. This is classic hearsay and the person who input the information must be subject to cross-examination. The computer output cannot be taken at face value since it was not the computer *per se*, that produced the information in the output.

22. In the second category of devices, the devices operate with little or no human intervention and as such, the output is in fact the "product" of the device itself. In this respect, we agree that the output made by such computers will not amount to hearsay. For example, where a computer applies an algorithm to produce a result, the result ought not to be regarded as hearsay.

23. However, we disagree with the TLDG's view in paragraph 3.53 that where an electronic device is "programmed to process information, and the evidence adduced is that which has been processed by the computer...the fact that such devices and the information recorded therein are electronic in nature is hardly a bar to their admissibility as real evidence".

24. In our view, apart from testing the a computer output for hearsay, Sections 35(1)(b) and 35(1)(c) also test the reliability of the information produced by the computer device, in the same way a witness is tested by way of cross-examination. Just as the reliability of a human witness' observations may be questioned, so too the reliability of the computer device and how it arrived at its output may also be questioned.

25. To our mind, this is not an issue of authentication. Neither is it an issue of integrity in the sense that the computer information may have been tampered with etc. This is an issue of whether the computer was functioning in the manner it was designed to, in order to produce the objective output/information we believe it will. If we are to trust that the output/information is accurate, we must first establish that the computer was operating properly. In this respect, we note that the focus of Section 35(1)(c)(i) is whether the output is "inaccurate because of improper use of the computer" and whether any "reason exists to doubt or suspect the truth or reliability of the output". Further, Section 35(1)(c)(ii) questions if the "computer was operating properly" and if it was not, whether "the accuracy of the output was not affected by such circumstances".

26. We would further submit that there is no breach of the equivalence principle in this respect. This is because even non-electronic evidence may be tested for its veracity in court. For example, the credibility of a human witness who testifies in court is open to cross-examination. In the same manner, the credibility of the computer device may be tested. To reject the computer device's output on the basis that the device was faulty is not different from impeaching

the credibility of a blind witness's testimony that he saw the accused at the scene of crime. Therefore, there is no breach of the equivalence principle because like non-electronic evidence, computer output, even if relevant, may be tested for veracity in court. So, although all evidence must be relevant, the fact that Section 35 further requires the computer evidence to be admissible via at least one of Sections 35(1)(a) to 35(1)(c) is really not an additional requirement.

27. Therefore, we see that in cases where the computer device acts as a storage device, there is a risk that its output is hearsay, and that the device may not be operating properly so that its output is not accurate. In the case where the computer output acts as a processing device, there is a risk that the computer is not operating properly so that its output is not objectively accurate.

28. In order to ensure that computer evidence is not hearsay, and that it is reliable, we would submit that there must remain some form of safeguard in the EA.

A middle-ground solution

29. In order to mitigate the burden created by Sections 35 and 36, we considered the possibility of narrowing the definition of "computer output" so that computer output in the form of business and other records may be excluded. In the same vein, we also considered the possibility of expanding the business records exception in Section 32(b) to include computer-type output. In either of these ways, commercial litigation will not be subject to the additional "hurdles" imposed on it whenever computer output is adduced under Section 35.

30. However, there are several reasons why we are of the view that it would be impractical to attempt to narrow the definition of "computer output" or expand section 32(b). First, we are not convinced that the hurdles presented by Sections 35 and 36 should only be relaxed in favour of commercial litigation only. The fact that Section 35 is burden-

some afflicts all forms of civil and criminal proceedings too. Creating an exception for only business records merely means that Section 35 will no longer discriminate against business records but will continue to do so in respect of all other forms of electronic evidence. Secondly, by drawing the distinction between business record-related computer output and other types of computer output, the result would be merely to shift the debate from "whether Section 35 should be repealed" to "what is a business record-related computer output".

31. In fact, it is precisely due to the ubiquity of society's increasing dependence on computing devices that we have reason to believe the definition should either be retained or be expanded, but certainly not narrowed. As mentioned in paragraphs 16 to 28 above, there needs to be a safeguard against the risk of computer output that is in fact hearsay or is unreliable. The prevalent use of computers and other similar devices both for processing and storing information and documentation means that submission of evidence in court will likely appear in the form of one computer output or another. And in such event, it ought to be necessary to be able to test the veracity of such computer output.

32. In our view, a variation of option 2 - in the form substantially similar to Section 5 of the Canadian UEEA - is, on balance, the most appropriate option for reform. We agree that the rules providing for the admissibility of computer evidence under Sections 35 and 36 are unduly burdensome. As such, they are better replaced by a set of evidential presumptions instead. However, for reasons stated above, we do not agree with the adoption of a non computer-specific approach and for the EA to remove any provision explicitly providing-for the admissibility of computer output. In our view, the notion of computer output as well as the existence of a provision to be able to test the veracity of computer output may be retained. The use of a set of presumptions will significantly reduce the burden of any party seeking to adduce computer output as evidence. To retain the concept of computer output and a provision testing the veracity of the same is a necessary safeguard.

33. Neither do we agree that the presumptions should only be confined to authentication presumptions. We would suggest that there be a presumption in relation to the fact that the computer system and the record keeping system is operating properly at all times. The TLDG, at paragraphs 4.16 and 4.17 of the Consultation Paper notes that Section 5 of the Canadian UEEA has such a presumption but it is more akin to a restatement of the general rule of authentication in Section 35(1)(c) of our EA. In our view, while the TLDG is correct to point out that such a presumption is not very different from our current Section 35(1)(c), the difference between the Canadian UEEA provision and that under our EA, is that the party adducing computer output as evidence needs to affirmatively show that the computer system was operating properly and that the output is reliable. In contrast, the Canadian UEEA presumes this to be so, which is a far more expedient and convenient process.

34. However, we agree that the second and third presumptions under Section 5 of the Canadian UEEA should be adapted into our EA.

35. Therefore, our position in terms of an option for reform would be to retain a computer-specific provision for the admissibility of computer output but to relax the current rules by substituting them with a set of presumptions similar to Section 5 of the Canadian UEEA instead.

36. We trust the above feedback will be helpful to the TLDG.

Mr Andrew Ong
Director
Drew & Napier LLC
5 January 2004

Annex 8 : Response from the Criminal Justice Division, Singapore

1. I've been asked to give CJD's formal response on the 4 suggested Options. CJD is in favour of Option 2. We feel that this Option would obviate the need to have formal admissibility rules when computer output is sought to be admitted. It does not stop the defence from mounting valid challenges to such evidence.

Mr Jaswant Singh
Attorney-General's Chambers
13 January 2004