Singapore Journal of Legal Studies
[1997] 130 – 184

COMPUTER OUTPUT AS EVIDENCE

This article discusses the new provisions in the Evidence Act that provide for the admissibility of computer output as evidence. In Part II of the article, the author describes and explains the operation of these provisions. And in Part III, the provisions are analysed in detail. It is contended in this article that the provisions represent an elaborate scheme for authenticating computer output as a precondition to its admissibility in evidence, that the distinction between computer output as real evidence and as hearsay continues to be useful in applying the provisions, and that the evidential device of authentication supersedes the distinction between primary and secondary evidence.

PART I: INTRODUCTION

THE legal profession in Singapore witnessed momentous events in the last two years in the area of computer output as evidence. In 1996, our Evidence Act,[1] which has been amended on very few occasions[2] over the past 100 years, saw substantial changes[3] to bring it up to date with technological advancements. Parallel amendments were also made to the Criminal Procedure Code.[4] Last year, too, saw the first cases being heard in our Technology Court,[5] where the Supreme Court has made available computers and other types of electronic equipment to facilitate the presentation of evidence in court. In the first case of its kind, *Las Vegas Hilton Corporation* v *Sunny Khoo Teng Hock,*[6] the High Court received and admitted evidence

1 (Cap 97, 1990 ed).

2 The last major change to the Evidence Act was in 1976 when Parliament adopted some of the proposals recommended in the UK Criminal Law Revision Committee Eleventh Report: Evidence (General) 1972 (Cmnd 4991). The other changes were relatively minor.

3 Evidence (Amendment) Act 1996 (No 8 of 1996). All further references to sections shall be to the Evidence Act and to the amendments introduced *via* the Amendment Act, unless the context indicates otherwise.

4 Criminal Procedure Code (Amendment) Act 1995 (No 38 of 1995), amending the Criminal Procedure Code (Cap 68). The Code is hereinafter referred to as the 'CPC'.

5 Supreme Court Practice Directions (1997 Ed), Part VII, paras 37-43, hereinafter referred to as the SCPD. This is set up in Court No 5 of the Supreme Court. See, *ibid*, at para 37.

6 [1997] 1 SLR 341. Video conferencing was also deployed in the case of *PP* v *John Martin Scripps* but no grounds of decision were delivered for this case.

via video conferencing from a witness in Las Vegas on the laws of Nevada.[7]

This breaknecking speed of change in a relatively quiescent subject for a traditionally conservative profession continues unabated in 1997. True to the Chief Justice's announcements in his Opening of Legal Year speech,[8] the Judiciary launched the Electronic Filing System project ('EFS')[9] on 8 March 1997.[10] The Academy Newsletter described the launch of EFS as a move "that would change the face of civil litigation, and make a paperless court a reality in about three years."[11]

With the EFS in place,[12] there are now two schemes devised by the Singapore judiciary to facilitate the presentation of computer output as evidence. These are the Litigation Support System for Presentations ('LSSP') and the Electronic Filing System. As currently devised, the EFS deals with the pre-trial process of filing and service of documents electronically,[13] while the LSSP deals with trial process of case presentation[14] and presentation of evidence.[15] However, in the absence of a Supreme Court Practice Direction to the contrary, it does appear possible to tender computer output as evidence outside of these two schemes, provided the evidence as tendered complies with the rules of evidence and rules of civil or criminal procedure.

7 *The Straits Times*, 21 December 1995.

8 Speech of the Chief Justice at the Opening of the Legal Year, 4 January 1997.

9 Three legal instruments are used to effect the EFS: the new section 36A of the Evidence Act, as inserted by the Evidence (Amendment) Act 1996, the new Ord 63A of the Rules of Court 1996, as inserted by the Rules of Court (Amendment) Rules 1997, and the Supreme Court Practice Direction No 2 of 1997, which is inserted as Part VIIA of the SCPD.

10 Singapore Academy of Law Newsletter, March/April 1997, at 1-6.

11 *Ibid*, at 1.

12 In this initial stage, only writs and their related applications come within the EFS. The related applications include summonses-in-chambers and summonses for directions, and the affidavits filed in relation to the writs and their attendant summonses, as well as the orders of court and judgments. See Ord 63A, r 1 and SCPD, para 43C(1). Thus other modes of commencement of proceedings such as originating summonses, motions and petitions as well as their attendant documents do not come within the EFS. See SCPD, para 43C(3) and (4).

13 Supreme Court Practice Direction No 2 of 1997, as incorporated into the SCPD as Part VIIA, and Registrar's Circular No 1 of 1997.

14 SCPD, para 41(5)(a)(i) (cause papers), (5)(c)(iv) (written submissions), (5)(c)(i) (submissions linked by "hyper-text" to other documents or other items of non-oral evidence), (5)(a)(ii) (electronic visual aids or multimedia presentations), (5)(a)(iii) (a combination of these techniques), (5)(c)(ii) (flow charts linking documents and other items of non-oral evidence), (5)(c)(iii) (a combination of hyperlinked submissions, flow charts, documents and items of non-oral evidence).

15 *Ibid*, para 41(5)(a)(i) (documentary evidence and non-oral items of evidence such as video clips or sound clips), (5)(c)(iv) (documents and non-oral items of evidence in electronic format). As explained in the previous footnote, these items of evidence may be electronically linked to flow-charts and submissions.

For the "paperless court" of the future to work, our rules of evidence must be equipped to deal with the reception of computer-generated output as evidence, since computer output will greatly supplant the traditional forms of evidence tendered in court. This article seeks to examine the legal foundations for the admissibility of computer output as "electronic evidence".[16] It will explain the admissibility provisions in Part II of the article. It is outside the scope of this article to deal with all the evidentiary aspects of computer output in criminal litigation. But as this article is founded on the Evidence Act amendments, which apply to criminal proceedings as well, much of the discussion is equally applicable.

Finally, the author analyses the provisions themselves in Part III of this article, and in the process, reviews some of the problems engendered by computer output as evidence and assesses the efficacy of the provisions in addressing with these problems.

PART II: ADMITTING COMPUTER OUTPUT

A. *Rules of Procedure* vs *Rules of Evidence*

A distinction must be drawn between using the LSSP and the EFS to present cause papers and submissions, and to tender documents and other non-oral evidence. The former are "documents" which go to the administration of the legal process ('administrative documents'). They do not by themselves "[prove or render] probable the past, present, or future existence or non-existence of the other."[17] The latter are documents that have independent probative value, and are not merely administrative in nature ('documentary evidence'). Stephen did define "evidence" in the Evidence Act to include "all documents produced for the inspection of the court",[18] which would *prima facie* include cause and submission papers. But this definition can

[16] The interest generated by amendments has spurred some secondary materials. The author is indebted to the authors of the following seminal articles on the Evidence (Amendment) Act 1996: Chin, "Recent Developments in the Law of Evidence: The Evidence Amendment Act 1996 – Part I" (hereinafter 'Chin I'); Charles Lim, "Recent Developments in the Law of Evidence: Computer Output, Technology Court and EDI Networks – Part II" (hereinafter 'Lim') and Chin, "Presenting Evidence in a Technology Court: Challenges for the Law of Evidence" (hereinafter 'Chin II'). All these are unpublished papers delivered at various conferences. The first two papers were delivered at the Academy of Law Seminar on 18 May 1996. The second paper was delivered at the Renaissance Courts Conference 1996 on 1 September 1996. The author understands from Mr Lim that his papers have been consolidated and will be published in the forthcoming issue of the Singapore Academy of Law Journal.

[17] Stephen, *A Digest of the Law of Evidence* (12th ed, 1936), Article 1, at 4.

[18] S 3(1), Evidence Act.

only be accepted at face value. Otherwise, there will be a failure to distinguish between procedure and evidence. Wigmore's five-stage classification of the judicial process makes this distinction clear: (i) the procurement of the parties' appearance before the tribunal ('Process'), (ii) the ascertainment of the subject of the dispute ('Pleading or Charge'), (iii) the attempt at demonstration by the parties of their respective positions ('Trial'), (iv) the determination of the dispute by the tribunal ('Verdict and Judgment'), and (v) the enforcement of the tribunal's determination ('Execution'). The rules of procedure control the first two stages of the judicial process, and the rules of evidence control the third stage of this process.[19]

Prior to the enactment of the Evidence (Amendment) Act 1996, there were no provisions in the Evidence Act which dealt with the rules of procedure for tendering administrative documents.[20] This distinction has however been coloured by section 36A, which states that the Rules Committee of the Supreme Court may make rules to provide for the "filing, receiving and recording of evidence and documents in court by the use of information technology". If one recognizes this dichotomy between administrative documents and documentary evidence, section 36A must be interpreted to refer to the making of rules of procedure and not rules of evidence. Though, for instance, section 36A(2)(a) permits the Rules Committee to make rules which can derogate from rules of evidence, this is only for the limited purpose of facilitating the use of electronic filing of documents. It is submitted that any rules so made will not derogate from the rules of evidence. Again, the rest of section 36A(2) sets out the circumstances of filing, sending and receiving of documents,[21] which have no counterparts in the rules of evidence that determine the admissibility of these documents.

It is useful to contrast the legal prescriptions in the Evidence Act for the EFS with the absence of similar mechanisms for the LSSP. Part VII of the SCPD certainly draws on the inherent jurisdiction of the court[22] to

[19] Wigmore, *A Treatise on the Anglo-American System of Evidence in Trials at Common Law* (3rd ed, 1940), §§1-2.

[20] It is certainly true that administrative documents can by themselves be relevant and thus "documentary evidence" *stricto sensu*. So judgments, orders or decrees of court are themselves relevant, wherein they have to be proved in evidence. See ss 42-46. Interestingly, the Evidence Act is silent as to the evidential value of judgments against which appeals have been lodged. Clearly the appellate court has to have cognizance of the lower court's judgments, orders or decrees. But such judgments do not fall cleanly within ss 42-44.

[21] S 36A(2)(b) deals with the sending and filing of "evidence or documents" and s 36A(2)(c) deals with the filing and receipt of such "evidence and documents".

[22] The first set of Practice Directions which relate to the use of the Technology Court was the Supreme Court Practice Direction No 2 of 1995, which preceded the 1996 amendments to the Evidence Act.

control the procedure of presenting and tendering of documents. But to admit these documents, the rules of evidence must still be satisfied. Conversely, parties cannot present electronic documents by way of the LSSP or EFS if such documents are inadmissible in evidence. Nothing in Part VII of the SCPD, and nothing in Ord 63A, permit the parties, by the use of the LSSP and EFS, to elide from the rules of evidence. In summary, the rules of evidence apply to the tender of documents and other non-oral evidence by way of computer output, regardless of whether the LSSP or the EFS is used.

B. *The Computer Output Regime under the Evidence Act*

The Explanatory Statement to the Evidence (Amendment) Bill[23] states that the 1996 Evidence Act amendments were sought "principally to facilitate the use of information technology and the admissibility as evidence of information stored or produced by the use of such technology." To this end, the original sections 35 and 36 of the Evidence Act, which were the only computer-related provisions in the Evidence Act prior to its amendment in 1996,[24] were repealed. In their place, five new computer-related provisions were inserted,[25] accompanied by two new definitions and a new illustration.[26]

1. *"Computers" and "Computer Output"*

The key provisions are the new sections 35 and 36, which provide for the admissibility and weight of any "computer output" (which is statutorily defined) produced by any "computer" (which is also statutorily defined). To generalise, the net effect of sections 35 and 36 is to require any "statement or representation … produced by a computer" ("computer output") or one which is "accurately translated" from such computer output[27] to satisfy the preconditions set out in section 35 before such computer output is admissible in evidence. These preconditions apply equally to both criminal and civil proceedings.[28] And they apply to all kinds of computer output – whether

[23] No 45 of 1995.

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

[25] Ss 35, 36, 36A, 62A and 68A.

[26] New definitions for "computer", "computer output" and a fresh illustration for computer-produced secondary copies.

[27] Taken from the definition of "computer output".

[28] See the Explanatory Statement to the Evidence (Amendment) Bill (No 45 of 1995), at 14. Hereinafter the "Explanatory Statement".

in audio, visual, graphical, multimedia, printed, pictorial, written or any other form.[29]

Interestingly, the statutory definitions of "computer" and "computer output" are not taken from the South Australia Evidence Act 1929,[30] upon which our sections 35 and 36 are modelled, but from the definition section of our Computer Misuse Act.[31]

(a) *What is a Computer?*

First, by the definition, computers have to be "data processing devices" which perform "logical, arithmetic or storage functions". This will, of course, include computers. But there are many other devices that process data.[32] Given the proliferation of microprocessor-controlled devices, many common household appliances such as TVs, VCRs, radios, CD players, telephones, pagers, air-conditioners, washing machines, refrigerators, and even day-to-day things such as cars,[33] "smart lifts", self-regulating central ventilation systems and "smart buildings",[34] photostatting and fax machines[35] can be considered computers because they all to some extent or another process and sometimes store information or data.

To cut down the scope of the definition, the definition itself sets out an exclusionary list that states that certain devices are not computers. So typewriters, typesetters and hand-held calculators are not considered

[29] S 3(1) – definition of "computer output". See also the Appendix.

[30] S 59a, as inserted by the Evidence Act Amendment Act 1990 (No 53 of 1972).

[31] Cap 50A, 1994 ed. The only difference being that the definition in the Evidence Act permits the Minister to prescribe devices that are not computers.

[32] For instance, Tapper in "Evidence from Computers" (1975) 4 Rutgers Journal of Computers and Law 324, at 394, considers filing cabinets and typewriters as devices for storing and processing information. This was based on the UK Civil Evidence Act 1968, *supra*, note 24, which defines a computer in s 5(6) as "any device for storing and processing information". This was the original definition used in the now defunct s 35(8) of our Evidence Act.

[33] While cars are largely mechanical devices, electronics have found a place in vehicle mechanics, *eg*, electronic ignition and automated braking systems or ABS.

[34] "Not so smart", *The Straits Times*, 7 March 1997.

[35] These office machines have devices that can control the way in which images are captured, transmitted and reproduced. For instance, some photostatting machines can digitally enhance photographs, magnify or reduce or even crop or edit images. Fax machines definitely process information by converting images and photographs into digital signals which are then converted into analog signals for transmission over phone lines. The converse process takes place when incoming faxes are received. In addition, some photostating and fax machines are programmable, *eg*, certain photostatting settings such as margin alignment, border erase, magnification can be stored for convenience. Fax machines can be programmed to dial certain numbers or lock themselves up after office hours.

computers by exclusions (a) and (b). Again, by statutory exclusion (c), devices "similar to" typewriters, typesetters or portable hand held calculators which are non-programmable[36] or which do not contain any data storage facilities are not considered computers. In addition, by exclusion (d), the list can be extended by Ministerial notification. The only caveat is that items on that list must be "such other device", which triggers the *ejusdem generis* rule. So the exclusionary list can only contain devices akin to typewriters, typesetters and calculators.

As statutory exclusion (c) is rather narrow, many devices identified above would be considered computers by the Evidence Act if these devices produce output. For instance, while devices such as photostating machines and telephones rarely produce printouts, which is the lay person's understanding of "computer output", measurements from dials, meters and other indicators read off such devices would by the extended definitions of "computer" and "output" be considered "computer output". Presumably, the class of devices that should not be considered computers can be enlarged by way of Ministerial notification. To date, however, no such devices have been prescribed.

(b) *Data Storage and Communications Devices*

Secondly, the statutory definition of computers includes "any data storage facility or communications facility directly related to or operating in conjunction with" computers. "Storage facilities" would refer to devices for temporary or permanent storage of computer data such as memory banks, tapes and drives, and "communication facilities" would refer to input and output devices and devices enabling computers to interoperate with each other. Such "communication facilities" would include keyboards, mice, displays, printers, modems and other computer peripherals. This extended definition is presumably used to refute any possible argument that because information that is generated by computers is physically stored in or communicated to other devices, it will not be considered "computer output" as these devices are not computers.

[36] The Oxford English Dictionary defines "programmability" as "the property of being programmable." "Programmable" is in turn defined as "Of an apparatus or an operation: capable of being programmed." And "program (verb)" is defined as "To cause (a computer or other device) automatically to do a prescribed task or perform in a prescribed way; to supply with a program." In summary, "programmability" refers to the ability to instruct the device to operate in certain prescribed ways.

(c) *Inter-connected Computers*

Finally, the definition of a computer includes "a group of such inter-connected or related [data processing] devices." This extended definition of what constitutes a computer recognises that computers are seldom used in isolation, and information recorded in one computer can be stored or communicated to other computers. In addition, one computer can process information fed to it by another computer. However, according to the Explanatory Statement, this definition even goes beyond interconnected stand-alone computers within some physical proximity to one another, and extends to "local area or wide area networks, bulletin board services and even a global network of networks such as the Internet."[37] More will be said about the ramifications of this definition when the section 35 preconditions are examined.

2. *Computer Output as Direct Evidence and as Hearsay*

Where computer output is "tendered in evidence for any purpose whatsoever",[38] such output shall only be admissible "if it is relevant or otherwise admissible according to the provisions of this Act or any other written law" and it satisfies one of the three sets of preconditions.

(a) *Common Law Distinctions between Direct Evidence and Hearsay*

How is computer output relevant or admissible? At common law, a distinction is maintained between computer output tendered as admissible "real evidence", and as hearsay. If the output records the results of devices which are produced without human intervention, it is "real evidence".[39] On the other hand, if the output is a record of human assertions, depending on human perception and the supply of such information to the computer, it would be hearsay and inadmissible unless it falls within a hearsay exception.[40] This statement was judicially approved in *R* v *Spiby*[41] where Taylor LJ distilled this distinction into one of asking whether there was the involvement of the human mind. If there was no such intervention, the evidence was not hearsay as it was one directly recorded by the machine.[42]

[37] *Supra*, note 28, at 15.
[38] S 35(1).
[39] *Castle* v *Cross* [1985] 1 All ER 87, 90a.
[40] Smith, "The Admissibility of Statements by Computer" [1981] Crim LR 387, 390.
[41] (1990) 91 Cr App R 186.
[42] *Ibid*, at 196.

Thus in *R* v *Wood,*[43] the computer printouts of chemical analyses and calculations were admitted as real evidence.[44] The court drew a distinction between using the computer "to store information which it then regurgitates"[45] whereupon "there would be persons who independently of the computer had had personal knowledge of the information inserted and stored",[46] and using the computer as "a calculating computer.... This computer was rightly described as a tool. It did not contribute its own knowledge."[47] The court classified the printouts as the latter, and not the former, drawing analogies from mechanically-operated recording devices such as mechanical records of radar echoes, barograph records, clock operated cameras and cards from clocking-in and out machines.[48] In *Castle* v *Cross*[49] the court accepted the argument that in many cases, results from less sophisticated mechanical devices or instruments have been admitted into evidence. No distinction should be made between the fact that it is a sophisticated machine which depends on computer control and other less sophisticated mechanical devices and instruments.[50] So printouts from an Intoximeter used for measuring the amount of alcohol in a breath sample were ruled real evidence and admissible.[51] And again, in *R* v *Spiby*, computer printouts of calls made from a hotel room recording the details of the telephone calls for billing purposes were treated as real evidence and admissible without the need to satisfy any hearsay exceptions.[52]

While this distinction between computer documents as "real evidence" and as hearsay appears in theory to be a reasonably clear one,[53] can be a tricky one to apply in practice. The case which best illustrates this is *R* v *Pettigrew*.[54]

In *R* v *Pettigrew*, A was found in possession of three new £5 notes shortly after a burglary committed at the premises in a village. He was charged with burglary. To prove its case, the prosecution led evidence that the notes were part of a bundle of £5000 worth of notes sent from the Bank of England

43 (1982) 76 Cr App R 23.
44 *Ibid*, at 27.
45 In *Castle* v *Cross*, *supra*, note 39, at 92f, Kennedy J characterised this as the use of a computer "in respect of its memory function".
46 *Ibid*, at 28.
47 *Ibid*, at 27. See also *R* v *Minors; R* v *Harper* [1989] 2 All ER 208, 212e *per* Steyn J.
48 *The Statue of Liberty* [1968] 2 All ER 195, 196.
49 *Supra*, note 39.
50 *Ibid*, at 90.
51 *Ibid*.
52 *Supra*, note 41.
53 See also the English Law Commission Consultation Paper No 138, *Evidence in Criminal Proceedings: Hearsay and Related Topics*, paras 2.13-2.19.
54 (1980) 71 Cr App R 39.

to a Newcastle bank, parts of which were traced through the village bank to the possession of the burglary victim. To prove that the three notes were part of this bundle, the prosecution tendered a computer printout recording the first and last serial numbers of each bundle of 100 notes. The notes had consecutive serial numbers, but the Bank of England machine counting the notes was programmed to reject defective notes. The machine operator would feed the bundle of notes into the machine, and would record the first serial number of the bundle on a card. It was not stated in the judgment as to whether the printout also records the numbers of the rejected notes, but one leading commentator states that these were so recorded.[55] Otherwise the operator had no personal knowledge of the number of the last note in the bundle, as well as the numbers of the rejected notes.

Was this printout a hearsay statement? The Court of Appeal concluded that it was. However, since the operator had no personal knowledge of the numbers recorded on the printout, it did not fall within the hearsay exception in section 1 of the English Criminal Evidence Act 1965.[56] The printout was ruled inadmissible. Professor Tapper disagrees. He takes the view that the printout was partly hearsay and partly non-hearsay: the first number should be hearsay and the last number and the numbers of the rejected notes are non-hearsay, being the output of a device.[57] Professor Smith, on the other hand, takes the view that the printout is non-hearsay because there is an absence of human intervention.[58]

Both views are, with respect, plausible. The difference in their views lies not in determining whether the operator had personal knowledge of the first number, or whether the machine generated the first number without human intervention. The difference lies in whether the operator fed the first number into the machine, and whether the machine processed this number. It would seem that the operator did not input this number into the machine; he merely wrote it down elsewhere, but the judgment does not make this

[55] Smith, "The Admissibility of Statements by Computer" [1981] Crim LR 387, 388.

[56] S 1 reads: "In any criminal proceedings where direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, on the production of the document, be admissible as evidence of that fact if – (a) the document is, or forms part of, a record relating to any trade or business and compiled, in the course of that trade or business, from information supplied (whether directly or indirectly) by persons who have, or may reasonably be supposed to have, personal knowledge of the matters dealt with in the information they supply…" It is roughly similar to s 380(1), CPC.

[57] Tapper, "Reform of the Law of Evidence in Relation to the Output from Computers" (1995) 3 International Journal of Law and Information Technology 79, at 87. Tapper did go on to qualify himself by explaining that as this was the output of a technical device, it had to be "proved according to the normal rules for proving the output of such devices."

[58] *Supra*, note 40, at 389-390.

absolutely clear. One may then assume that the machine read this first number from the bundle of notes, in the same way as it read the numbers of the rejected notes and the last note in the bundle. So the different views espoused by Professors Tapper and Smith can be resolved as follows: was the machine operating as a data storage device in relation to the first number, or a data processing device? Some form of hybrid function may also be possible, *eg,* the operator inputs the first number, which the machine records and then verifies against its own reading of the first number. If the machine indeed behaved this way, perhaps Professor Smith's view is perhaps more accurate. This is all a question of the degree and extent of human intervention.

The English cases carried this common law distinction between real evidence and hearsay into the English legislation which requires computer documents to satisfy prescribed conditions to be admitted "as evidence of any fact stated therein".[59] This distinction was reasserted in decisions such as *R* v *Minors,*[60] *R* v *Spiby*[61] and *R* v *Neville,*[62] where computer documents admitted as "real evidence" were ruled to be outside of the legislation because it was felt that the legislation was intended to apply only to hearsay documents. However, this distinction was held to be an unnecessary one by the House of Lords in *R* v *Shephard.*[63] Lord Griffiths noted that "[it does not] make any difference whether the computer document has been produced with or without the input of information provided by the human mind and thus may or may not be hearsay.... It is surely every bit as important that a document produced by a computer and tendered as proof of guilt should be reliable whether or not it contains hearsay."[64] In other words, regardless of whether computer documents are tendered as evidence of the facts stated therein, as hearsay or as "real evidence", all such documents are inadmissible without first satisfying the legislative preconditions for admitting computer documents.

(b) *Removal of the Distinction in section 35?*

In Singapore, similar distinctions have been drawn between computer output as real evidence[65] and computer output as hearsay[66] in relation to

59 S 5, Civil Evidence Act 1968, *supra*, note 24, and s 69, Police and Criminal Justice Act 1984 (1984, c 60).
60 *Supra*, note 47.
61 *Supra*, note 41.
62 [1991] Crim LR 288.
63 [1993] AC 380.
64 *Ibid*, 384E-385G.
65 *PP* v *Ang Soon Huat* [1991] 1 MLJ 1, following *Castle* v *Cross*, *supra*, note 39.
66 *Aw Kew Lim & Ors* v *PP* [1987] 2 MLJ 601.

the old section 35, which uses language similar to the English legislation. It is to the credit of the legislative draftsmen of the new section 35 that they echoed the sentiments in *Shephard* that regardless of whether the computer output is real evidence or hearsay, because both types of evidence involve the use of the computer, there should be some form of guarantee of trustworthiness.[67] So the new section 35(1) states that it applies "where computer output is tendered for any purpose whatsoever." This approach cannot be faulted.

However, it is the thesis of this author that while section 35(1) does away with the "real evidence doctrine" which would have discriminated between the admissibility of computer output as hearsay and as real evidence,[68] sections 35 and 36 themselves require that the useful distinction between computer output as real evidence and as hearsay be retained. Among others, sections 35(4), (10) and 36(1) refer to the "original document", which presumes that the computer is used to record information, whereas sections 35(6)(b) and 36(4)(a) refer to the use of the computer both for the purpose of processing and storing information. Thus the mechanics of sections 35 and 36 appear to discriminate between computer output as records ("recorded output") and as processed information ("processed output"), even though the provision applies to both types of output. This author agrees with the approach in *Shephard* that the proponent of computer output should not be allowed to outflank the legislative provisions by contending that his output is real evidence. So sections 35 and 36 should apply to *both* processed output and recorded output – computer output as real evidence and as hearsay. But it does not mean that the provisions should apply *in the same way* to these two types of evidence. It does not detract from *Shephard's* approach to observe that the legislative provisions work differently in relation to the different types of computer output. They ought to! The usefulness of this distinction in relation to sections 35 and 36 will be identified in the various provisions in the rest of this Part of the article and explored in detail in Part III of this article.

3. *Effect of Failing to Satisfy section 35*

Section 35 provides three sets of preconditions as alternative avenues for admitting such computer output: the parties to the proceedings may expressly agree to the accuracy and authenticity of such computer output

[67] *Supra*, note 16, Chin I, at 4-5, para 12.
[68] *Ibid*, at 5, para 12.

("express agreement"),[69] the output is one produced by an approved process ("approved process"),[70] or the party tendering such output ("the proponent") tenders the requisite certificates to prove the proper operation of the computer and the corresponding accuracy of the computer output ("by certification").[71]

If the proponent fails to satisfy any of these preconditions,[72] the computer output will be inadmissible, even though it is otherwise admissible by some other rule of evidence. This is confirmed by the language of section 35(1) itself, which contains the emphatic expressions "unless otherwise provided in any other written law" and "such output shall be admissible if it is relevant or otherwise admissible … *and it is* – [the preconditions follow]". Thus, unlike the position in England where there is some controversy over the possibility that computer output may be admissible pursuant to the business records exception even though it does not pass muster under the computer statements exception,[73] the unequivocal language of section 35(1) has obviated this possibility. In other words, for computer output to be admissible in

[69] S 35(1)(a). Hereinafter loosely described as "an express agreement to admit computer output", or "to agree to make computer output admissible", though this is only an agreement not to dispute the accuracy and authenticity of the output, and not to make it admissible for all purposes and intents. In other words, parties may so agree, but the proponent still has to show that such evidence is admissible, *eg*, by a relevancy provision in ss 6-16, or that it is not hearsay.

[70] S 35(1)(b).

[71] S 35(1)(c).

[72] An interesting issue arises here: can the proponent who fails to establish that the computer output satisfies one set of preconditions seek to admit such computer output by proving that it satisfies another set of preconditions? In principle, there appears to be no reason why this is not possible, since these three sets of preconditions are clearly in the alternative. Furthermore, the language of s 35(1) is such that there is on its face no bar to the proponent seeking to admit evidence under the various preconditions in the alternative. The complication, however, arises because since the parties can expressly agree that such evidence be admissible by s 35(1)(a), by corollary, what they do not agree is inadmissible by s 35(1)(a). And they can also expressly agree that any evidence to which they did not expressly agree is inadmissible, or that such evidence is inadmissible by either s 35(1)(b) or (c). It is submitted that the courts should give effect to such agreements, especially since the court can give effect to agreements to admit such output, and the prohibitions against admissibility are but the mirror image of the permissible arrangements between the parties. However, since the effect of such agreements will be to derogate from rules of evidence, clear and unambiguous language is called for.

[73] Ss 4 and 5, Civil Evidence Act 1968; s 68, Police and Criminal Evidence Act 1984 (1984, c 60) (hereinafter "PACE") and s 24, Criminal Justice Act 1988 (1987, c 38). See for instance the discussion in *R* v *Minors; R* v *Harper*, *supra*, note 41, at 212h-213c, 215c, 216c-d and *R* v *Spiby*, *supra*, note 41, 192. This problem has been significantly resolved by the House of Lords decision of *R v Shephard*, *supra* note, which ruled in favour of a cumulative approach.

evidence in Singapore, it has to be *both* relevant or admissible *and* it has to be admissible by section 35. Section 35(1) is, in other words, a cumulative, and not an alternative, requirement for the admissibility of any item of computer output as evidence.[74]

4. *Where Computer Output is not "Tendered in Evidence"*

Despite the breadth of the language of section 35, it is nonetheless possible for counsel to rely on computer output for his case but not tender it in evidence. Where computer output is not "tendered in evidence",[75] arguably section 35 does not apply. This possibility can arise where, for instance, the computer output is relied on by an expert in giving his expert opinion and is not put in evidence.[76] Such output is certainly relevant as constituting the grounds of the expert's opinion,[77] but need not necessarily be "tendered in evidence".

Similarly, when computer output is used as a document by a proponent's witness to refresh his memory,[78] the output is not *per se* tendered in evidence.[79] An interesting issue however arises here as to the interaction between sections 35 and 147. By section 147(4), the computer output used to refresh the witness's memory "may be made evidence in those proceedings" if the opponent cross-examines the witness on it.[80] The effect of making the document evidence is that it is admissible "as evidence of any fact stated therein".[81] In other words, section 147(4) reverses[82] the common law rule that a document is only admitted into evidence to show consistency in the

74 See Chin I, *supra*, note 16, at 2.

75 S 35(1).

76 *R* v *Golizadeh* [1995] Crim LR 232. See also the English Law Commission Consultation Paper No 138, at para 14.13.

77 S 53. One should also be quick to add more often than not, an expert has to prove the grounds of his opinion to substantiate his opinion, whereupon s 35 would have to be complied with.

78 Ss 161 and 162.

79 *Sophocleous* v *Ringer* [1988] RTR 52.

80 S 163.

81 S 147(4).

82 See the commentaries to clause 9, Explanatory Statement to the Evidence (Amendment) Bill 1975 (No 34 of 1975), *Singapore Parliamentary Debates, Official Report*, vol 34, cols 1246-1247, and the Criminal Law Revision Committee Eleventh Report: Evidence (General) 1972 (Cmnd 4991), at paras 166, 167, 232 and 257. S 147 was based on cll 33(1)(a), 33(2) and 36(4) of the draft Criminal Evidence Bill prepared by the said committee.

testimony of the witness.[83] If the opponent[84] wishes to make the output evidence, does he have to satisfy section 35? Does section 147(4) override the legal requirements of section 35? It would appear not, since the language of such a provision must, by section 35(1) itself, be quite specific, and section 147(4) was enacted before section 35(1).

If so, who has the legal burden of satisfying the preconditions in section 35 – the proponent or the opponent? It is the opponent who triggers the operation of section 147(4), but the opponent is unlikely to have the requisite information to meet, for instance, the certification requirements of section 35(1)(c).[85] It is submitted that the burden should be on the proponent to establish the section 35 preconditions even where it is the opponent who triggers the operation of section 147(4). There is no unfairness if the burden is cast on the proponent when it is the opponent who wishes to make the output evidence: it would be even more unfair to permit the proponent to elide from section 35 by the expediency of "admitting" computer output via the backdoor of "refreshment of memory", and to give him the right to veto the opponent who wishes to rely on section 147(4).[86] If the reason for relying on "refreshment of memory" is that the proponent cannot satisfy the section 35 preconditions, then this is best brought out in cross-examination in section 147(4). This interpretation may be procedurally awkward,[87] but it is submitted that it fairly reconciles sections 35 and 147(4).

Again, the same interpretation should for consistency be given to section 147(3) where the opponent wishes to prove a previous inconsistent or contradictory statement in a computer output made by the proponent's witness.

This interpretation reinforces the clear rule in section 35 that all computer output tendered in evidence for any purpose whatsoever has to satisfy its preconditions. In this regard, it is necessary to identify the various types of computer output that can be tendered in evidence.

83 *R* v *Virgo* (1978) 67 Cr App R 323.

84 Unlike s 147(3) where it is the opponent who puts the document into evidence, s 147(4) does not make it clear whether it is the proponent or the opponent who puts the document into evidence. However, the common law authorities have uniformly referred to the opponent who puts the document, or is required by the proponent, to put the document into evidence. See *Gregory* v *Tavernor* (1833) 6 C&P 280 at 281, 172 ER 1241 at 1242, *Senat* v *Senat* [1965] P 172 at 177, [1965] 2 All ER 505 at 511 and *R* v *Britton* [1987] 2 All ER 412, 414-415. In England, the equivalent rule in civil proceedings is statutorily provided for in s 3(1), Civil Evidence Act 1968, *supra*, note 24.

85 This is the most likely precondition to bring the output under, unless the proponent agrees not to dispute the authenticity and accuracy of the computer output under s 35(1)(a).

86 For the reasons indicated above, *ibid*.

87 Because it calls for the proponent to tender evidence of the s 35 preconditions during the opponent's cross-examination.

C. *Preconditions to Admissibility*

1. *Alternative Modes of admission*

As explained above, if computer output is tendered in evidence, the proponent has to prove[88] that one of the three alternative sets of preconditions for admissibility is satisfied. In other words, the proponent has to prove that there is an express agreement between the parties that satisfies section 35(1)(a), that the computer output is produced by an approved process by section 35(1)(b), or that there is no reasonable ground for believing the output to be inaccurate and that there is reasonable ground to believe that the computer was operating properly by section 35(1)(c). In this respect, section 35 is unique because it gives the proponent seeking to admit computer output a choice of the mode for admitting evidence.

It does not appear that section 35 requires the proponent to elect one out of the three modes of admission, since like other rules of evidence in the Evidence Act, the modes of admission are inclusionary in nature.[89] Thus on principle, there appears to be no reason why a party who tries but fails to prove the existence of an express agreement between the parties to admit the computer output, may not subsequently seek to admit the output by way of certification.

2. *Express Agreement*

By section 35(1)(a), the parties to the proceedings can at any stage of the proceedings, expressly agree not to dispute the authenticity nor the

[88] If the s 32 precondition cases reflect judicial approach to admissibility, the courts would want strict legal proof of one of these three sets of preconditions before computer output is admissible. See, in relation to the effect of failing to establish the s 32 preconditions: *Mohd Ghouse* v *The King* (1909) 11 SSLR 31, *Sim Tiew Bee* v *PP* [1973] 2 MLJ 200 and *Vaynar Suppiah* v *KMA Abdul Rahiim & Anor* [1974] 2 MLJ 183.

[89] At common law, the rules of evidence are exclusionary in nature. In other words, if evidence is relevant, it is *prima facie* admissible unless a rule of evidence such as the hearsay rule applies to render the evidence inadmissible. If the evidence is hearsay, the proponent cannot escape from the hearsay rule by showing that the exceptions of another exclusionary rule of evidence applies. One can found an argument that the overall effect of s 35 is exclusionary in nature, because computer output has to be *prima facie* admissible by any written law, and if the proponent fails to bring his evidence within any one of the three modes of admission, the computer output would be inadmissible. But it is submitted that even if s 35 is treated as an exclusionary rule, the alternative modes of admission must be treated as exceptions to the exclusionary rule, so the proponent can choose to bring himself within any one of the modes of admission.

accuracy of computer output. Expressed positively, the parties must expressly agree not to dispute both[90] the authenticity and the accuracy of the computer output. This deceptively simple provision lends itself to four further observations.

(a) *"Expressly agree"*

The use of the expression "expressly agree" appears to contemplate an agreement with express, and not implied, terms as regards the use of computer output in evidence. There are no authorities that have interpreted section 35 yet, but it is submitted that there can be a sufficient express agreement if section 35(1)(a) is incorporated by reference. The expression does not appear to refer to the need for a written agreement as opposed to an oral agreement. Thus the Explanatory Statement confirms that the agreement "need not be in writing and can be in any form but it must be an express agreement."[91]

Special rules of admissibility apply to express agreements for the admission of computer output in criminal proceedings. By section 35(2)(a), an express agreement can only be made between the prosecution and a legally represented accused. This is to "ensure that there is no room for any allegation that the prosecution tricked the accused into agreeing to admit such evidence."[92] This makes section 35(1)(a) agreements consistent with sections 376 and 382(1)(a) of the CPC.

A nice question arises where transactions are conducted electronically, and it is sought to prove by way of disputed computer output that there is a legally binding contract between the parties. It does not appear that section 35(1)(a) can admit such computer output to prove an express agreement between the parties for the purpose of proving the contract between the parties. In other words, the disputed computer output cannot bootstrap itself into admissibility by section 35(1)(a). However, this does not rule out the use of non-disputed computer output to prove this express agreement between the parties (*eg*, electronic login records or user access scripts which require the user to acknowledge that he agrees to be bound by certain terms and conditions of usage when he logs on) or the use of the other two preconditions to prove the express agreement between the parties.

[90] S 35(1)(a) is stated negatively; thus a valid s 35(1)(a) agreement must contain an express agreement by the parties not to dispute *both* the authenticity of the computer *and* the accuracy of its contents.

[91] *Supra*, note 28, at 15.

[92] Charles Lim, *supra*, note 16, at 1, para 5.

(b) *"Between the parties"*

Section 35(1)(a) is silent as to whether in multi-party proceedings, agreements need to be obtained between every party to the proceedings, or only as between the proponent and opponent of the evidence concerned. If section 35(1)(a) is interpreted to mean any agreement between any two parties, A and B who are plaintiffs can expressly agree to admit computer output for use in proceedings as against C. While the computer output has to be relevant or admissible by any written law in the first place, the safeguards introduced by section 35 can be elided by the expediency of procuring the agreement of parties to the same side in legal proceedings. Compounding this abuse is the fact that such an agreement can be reached at any time to the proceedings, *eg*, between A and B during the legal proceedings itself when C challenges A's computer output on the ground that it fails to pass muster under section 35(1)(c). Surely this cannot be allowed to take place. It is thus submitted that the expression "relevant parties" used in the Explanatory Statement[93] must refer to the proponent of the computer output, the opponent or the party against whom the output is sought to be used, and any party whose interest will be affected by the admission of the output. In most instances, this would probably mean that the agreement of all the parties to the proceedings should be procured. On this interpretation, where one "relevant party" disagrees, the evidence cannot be admitted in evidence, despite the concurrence of all the other relevant parties.

(c) *"At any time"*

Section 35(1)(a) confirms that the parties can agree to admit computer output "at any time". This can be before the contemplation of proceedings or the commencement of criminal investigations, or even during the proceedings themselves. Nonetheless, if the computer output is a hearsay statement which is made after the commencement of police investigations, even if it is admissible by section 35, it remains *inadmissible* by sections 379(1) and 380(3) of the CPC. This is because section 35 is a cumulative provision: the computer output must first be admissible pursuant to some other written provision of the law before it is required to satisfy section 35.

[93] *Supra*, note 28, at 15, which states that "in multi-party proceedings, it may happen that the court may decide that only the agreement of relevant parties need be obtained. The provision leaves this possibility open." The Explanatory Statement can be used as an aid to statutory interpretation. See s 9A, Interpretation Act (Cap 1, 1994 ed).

(d) *Rescission of the agreement*

By section 35(2)(b), if the express agreement not to dispute the authenticity or accuracy of computer output is vitiated for reasons of fraud, duress, mistake or misrepresentation, the section 35(1)(a) agreement is ineffective. It does not appear that section 35(2)(b) is intended to exhaustively prescribe the circumstances of rescission. So, for instance, a party may terminate the agreement by way of repudiation or breach of a condition or innominate term, thus bringing the primary obligation not to dispute the computer output to an end.[94]

It follows that there is a point in time in the proceedings when the primary obligation is discharged. This will be when the proponent tenders computer output in evidence and the opponent and the relevant parties do not object. Thus Professor Chin argues that this obligation is discharged when computer output is included as part of the Agreed Bundle without condition.[95] The decisions on this point have also held that the mere fact that documents in an Agreed Bundle have been tendered in evidence does not mean that the opponent agrees with what the documents purport to say or their evidential value. This rule that the opponent can still entitled to reduce or rebut the tendered evidence[96] is statutorily prescribed in section 36(5). This strengthens the argument made above by Professor Chin, since the inclusion of computer output as part of the Agreed Bundle will not prevent the opponent from adducing other evidence to rebut the computer output evidence.

But can a party *subsequently* object to the accuracy or authenticity of computer output on the ground that his failure to object arose from the respondent's fraud or misrepresentation? Professor Chin agues that where the output is unconditionally included in the Agreed Bundle, the agreement can no longer be rescinded.[97] It is respectfully submitted that this statement cannot be over-generalised. Where the output is included or tendered without

[94] *Photo Production* v *Securicor Transport* [1980] AC 827.

[95] Chin I, *supra*, note 16, at 3, para 7.

[96] *Yap Choo Hoo* v *Tahir bin Yasin & Anor* [1970] 2 MLJ 138 and *Goh Ya Tian* v *Tan Song Gou & Ors* [1981] 2 MLJ 317; approved and applied in *Tai Siat Fah & Ors* v *Lawful Personal Representative Of Badrul Hisham Bin Hashim* [1995] 2 MLJ 571 and *Chua Gek Kuon* v *Seow Chai Seng* [1992] 1 SLR 270. In *Ng Bee Lian* v *Fernandez & Anor* [1994] 2 SLR 633, TQ Lim JC extended the reasoning to its logical conclusion and held that where a document is included in the Agreed Bundle, there will be no further dispute as to the authenticity of the documents.

[97] Chin I, *supra*, note 16, at 3, para 7.

objections, it does not lie in the mouth of the opponent to terminate the agreement or to establish breach to reverse the effect of tendering the output. The primary contractual obligation not to object to the admission of the output has been discharged. But where the section 35(2) vitiating factors operate, the expression – "an agreement expressly made between the parties … shall not render the computer output admissible in evidence" in the provision makes it clear that the agreement will be avoided. Where an agreement is procured by fraud, surely policy will require that the appellant be permitted to raise subsequent objections to the accuracy or authenticity of the output even though he failed to do so initially. The court cannot permit itself to be used as an instrument of fraud. Similarly, in criminal proceedings, where the prosecution secures an agreement with the accused and so tenders the output in evidence without objections, the accused's counsel must surely be entitled to object on the grounds that the agreement violates section 35(2)(a). The considerations in section 35(2) will vitiate any agreement, and annul any failure on a party's part to object. They should apply, regardless of whether the output is included in the Agreed Bundle, conditionally or otherwise. This interpretation is also consistent with the well-established rule that inadmissible evidence does not become admissible because of the failure of counsel to object.[98]

However, it remains an open question as to whether the appellant may be estopped from contending that the agreement was obtained by means of fraud, distress, mistake or misrepresentation, in view of the clear language of section 35(2). This possibility of pleading estoppel is not mentioned in section 35(2) itself, though it is available as a defence by section 117.

3. *Approved Process*[99]

An "approved process" is a process that has been approved pursuant to regulations made by the Minister under section 35(5). To date, only one such process has been approved pursuant to the Evidence (Computer Output) Regulations 1996[100] – document imaging systems. Document imaging systems

[98] *Lim Yam Hong* v *Lam Choon* (1928) AIR 127, *Packiam* v *PP* [1972] 1 MLJ 247, *Malaysia National Insurance Sdn Bhd* v *Malaysia Rubber Development Corporation* [1986] 2 MLJ 124, *Cold Storage Singapore* v *Magistrate's Court of Chancery Court* [1992] 1 SLR 521, *Mui Bank Bhd Johor* v *Tee Puat Kuay* [1993] 3 MLJ 239, *PP* v *Tan Kok An* [1996] 1 MLJ 89; *cf Mui Bank Bhd* v *Alkner Investments Pte Ltd* [1990] 3 MLJ 385.

[99] For a detailed discussion of the approved process method for admitting computer output, please refer to Charles Lim's article, *supra*, note 16, at 2-3.

[100] S 93/96.

are computer systems that are capable of capturing, storing and retrieving or generating such images of documents recorded using this process.[101] Where it is proved that the computer output has been "produced in an approved process", it is admissible. The Evidence (Computer Output) Regulations prescribe the method for obtaining the due certification by a certifying authority that the document imaging system is an approved process.

Proof that the computer output has been "produced in an approved process" is twofold. First, the process that is relevant to the proceedings has to be identified as, or as part of, an approved process, by a certificate from the certifying authority. The certificate must be signed by a person holding a responsible position in relation to the operation or management of the certifying authority.[102] Secondly, there must be a certificate that the computer output is obtained from the approved process. This is to link the output to the approved process. The certificate must be issued by a person holding a responsible position in relation to the operation or management of the approved process.[103] With these certificates, the presumption arises that the computer output is an accurate reproduction of the original document until it is rebutted.[104]

It should be noted that the "approved process" route for admitting computer output appears to be available only where the computer is used as a record storage device. So the presumption in section 35(4) is one that the output "accurately reproduces the contents of the original document unless the contrary is proved". This is reflected in the Evidence (Computer Output) Regulations, which to date have only prescribed document imaging systems as approved processes.

4. *Certification*

(a) *No improper use and proper operation of the computer*

Where there is no express agreement between the parties and where the computer output is not produced pursuant to an approved process, the output is still admissible in evidence if the party tendering such output satisfies

[101] Regulation 2 read with para 2, First Schedule, Evidence (Computer Output) Regulations 1996.

[102] S 35(3).

[103] S 35(4). The certifier only needs to state that the requisite matters in s 35(3) and s 35(4) are true to the best of his knowledge and belief: s 35(9).

[104] S 35(4). A *prima facie* reading of s 35(4) that the presumption arises without a s 35(3) certificate is erroneous: s 35(4) requires proof that the output is obtained from an approved process, and this proof must be supplied by a s 35(3) certificate.

section 35(1)(c) and proves two preconditions. The first precondition, which is expressed in the negative, is that that "there is no reasonable ground for believing that the output is inaccurate because of the improper use of the computer, and that no reason exists to doubt or suspect the truth or reliability of the output" (the "no improper use" requirement). The second precondition, which is expressed in the positive, is that "there is reasonable ground to believe that at all material times the computer was operating properly" (the "proper operation" requirement).

(b) *"No reasonable ground for believing..."* vs *"reasonable ground to believe"*

The first precondition relates to disproving any improper use of the computer, and the second relates to proving the proper operation of the computer. The different phraseology of these preconditions is not unintentional. According to the Explanatory Statement to the Bill, the first precondition is "deliberately phrased in the negative to facilitate proof".[105]

This assertion however appears somewhat dubious, since it would appear more difficult to prove a negative than it is to establish a positive![106] The expression "no reasonable ground for believing" requires the proponent to rebut any possible suspicion that may give him some reason for suspecting otherwise. In addition, the second part of the first precondition requires the proponent to show that "no reason exists to doubt or suspect the truth or reliability of the output", which again sets a very high standard to be satisfied. Parallels may be drawn with cases which dealt with negative hearsay, which require evidence of a proper system of record keeping before the court would draw inferences from the absence of entries in maintained records.[107] This may be a matter of phraseology, but it is interesting to note that the Explanatory Statement indicates that it should be made more difficult to prove that the computer is operating properly than it is to prove that there has been no improper use of the computer. One would have thought that in practice, the converse is true – that it is more difficult to show that there has been no improper use of the computer, since, unlike the proper operation of computers, proper human usage is always difficult to reproduce

[105] *Supra*, note 28, at 16.

[106] Bradgate in "The Evidential Status of Computer Output" (1990) 6 *Computer Law and Practice* 142, 145-146 makes a similar point.

[107] *Patel* (1981) 73 Cr App R 117, *Shone* (1983) 76 Cr App R 72, *Muir* (1983) 79 Cr App R 153. See also s 9(3), UK Civil Evidence Act 1995 (c. 38).

and reconstruct empirically.

(c) *"A certificate signed by a person holding a responsible position …"*

To this end, the proponent can establish that the two preconditions in section 35(1)(c) have been complied with by relying on the certification mechanics spelt out in detail in section 35(6) to (8), or he can rely on other modes of proof.[108] By section 35(6), "a person holding a responsible position in relation to the operation or management of the computer system" can issue a certificate that complies with section 35(6) as "sufficient evidence of the matters stated in the certificate". The Act does not explain who this person is, but reading section 35(6) with section 35(7), such a personal should normally have "control or access over any relevant records and facts in relation to the production by the computer of the computer output". The Explanatory Statement explains that such a person is usually the systems operator or information systems manager ("sysop").[109]

(d) *"… did not have control or access over any relevant records and facts …"*

The sysop's certificate must (a) identify such output and describe the manner in which it was produced, (b) give particulars of the device involved in the processing and storage of such output and (c) deal with the matters mentioned in section 35(1)(c). In other words, the sysop must certify that to the best of his knowledge,[110] there has been no improper use of the computer and that the computer was operating properly at the material time. There is no doubt that the sysop is often the best person to supply details about the hardware he is maintaining. But sometimes the sysop may have his hands full. This problem is compounded by the fact that computer systems may be set up as networks, which may span large areas and be managed by many discrete entities.[111] Computers may in turn be connected to various storage or communication devices, over which the sysop may have only indirect control. So a sysop may not have complete knowledge of all the

[108] S 35(6) does not make it mandatory that the proponent tenders a s 35(6) certificate to establish that the conditions in s 35(1)(c) have been complied with. Nor does s 35(1)(c) so prescribe.
[109] *Supra*, note 28, at 16.
[110] S 35(9).
[111] Such a network may include the Internet. *Supra*, note 37.
[112] Professor Tapper makes the similar point in Tapper, "Reform of the Law of Evidence in Relation to the Output from Computers", *supra*, note 57, at 88 that it is difficult to find any one individual who is in a position to testify or certify to the proper operation of all

different components of the computer responsible for generating the computer output.[112] However, caselaw appears to have offered a pragmatic solution: the sysop is considered to have discharged his duties if he had made adequate inquiries about the proper operation of other computer systems over which he has no direct responsibility or control.[113]

Interestingly, the sysop is normally not the operator, nor does he have any direct supervision or control over the actual computer user. In a large business organisation, the sysop will set up the computer system, but it will be the managerial staff (not to be confused with the information system manager) who will supervise the data entry operators or clerical staff. It would be unlikely that the sysop has any actual knowledge of any improper use of the computer system, unless such improper use shows up in the computer's diagnostic, maintenance or audit records. As such, he would not be able to certify as to the proper operation of the computer, especially since a false certification subjects him to criminal sanction under section 35(11).

A possible solution is to note that since section 35(6) refers to a person who is responsible for "the operation or management" of the computer system, this expression is arguably wide enough to cover both a sysop as well as a management staff member. This interpretation however appears to be foreclosed by the Explanatory Statement's conception of "a person holding a responsible position" to mean a sysop and not a managerial staff member overseeing computer operators.[114] The Explanatory Statement goes on to state that "[m]oreover in wide area networks or large systems, one person alone may not have knowledge of the relevant computer output. The new section 35(7) therefore provides for a supplementary certificate to be signed by another person who had control or access to the computer system."[115] Thus the Explanatory Statement calls for the following distinction to be made. Where only one person oversees both the operation of the computer as well as its users, as in SMEs,[116] section 35(6) is to be used. In larger organisations, where joint responsibility is held by both the sysop

of the parts of the system. Also those occupying a responsible position in relation to the operation of a computer do not necessarily understand its operation any more than, or even as much as its operator.

[113] *R* v *Neville*, *supra*, note 62, where the English Court of Appeal simply held that the witness, who was from the phone billing company and gave evidence that the microfiche of the phone bill was accurate, had made adequate inquiries about the proper operation of a call-tracking computer operated by another company, the mobile phone operator.

[114] *Supra*, note 28, at 16.

[115] *Ibid*.

[116] Small and Medium-sized Enterprises.

as well as the management staff member, one party can tender a section 35(6) certificate, and the other, who has "control or access over any relevant records and facts",[117] can tender a section 35(7) certificate to supplement[118] the former's section 35(6) certificate.[119] Thus a managerial staff member, who would not be expected to have any knowledge as to the operation of the computer, but only its proper use, can so tender an "incomplete" section 35(6) certificate, to be supplemented by the sysop's section 35(7) certificate as to those matters not addressed in the section 35(6) certificate.[120]

Section 35(8) additionally provides that if there is no sysop or manager, or if there is an uncooperative sysop or managerial staff who refuses to tender either a section 35(6) or section 35(7) certificate, an expert who has been given access to the computer system can issue a certificate to address the section 35(6) requirements.[121]

It would also appear from the language of section 35(6) read with section 35(7) and (8) that the sysop and management staff need not state their belief as to the proper use or operation of the computer system from their actual knowledge. Instead, they can refer to and draw such conclusions from the relevant records and facts for which they had control or access. This means that they can technically certify as to matters that are hearsay to meet the

[117] It is unclear if this expression refers to the diagnostic, maintenance and audit records used by the sysop to establish if the computer is operating properly, or to the records and facts which form the input for the computer output. It does however appear that if the management staff is supposed to tender the s 35(6) certificate, since only he can most effectively deal with the requirement to establish the proper use of the computer as set out in s 35(1)(c)(i), the expression "relevant records and facts" must refer to the diagnostic, maintenance and audit records maintained for the computer. This interpretation is consistent with s 36(1) and (2), which seem to use the same expression in contradistinction to "the original document".

[118] S 35(7) does not make it clear that the s 35(7) certificate is to be a substitute for the s 35(6) certificate. Evidence from the Explanatory Statement suggests otherwise – that there be both a s 35(6) certificate and a supplementary s 35(7) certificate. Otherwise, in large organisations, it would not be possible for any one person to issue a s 35(6) certificate which meets all its requirements, because such a person will not have full knowledge that all the requirements have been complied with.

[119] It is unclear whether it is the sysop who should tender the s 35(6) certificate and the management the s 35(7) certificate, or it be the converse. The Explanatory Statement appears to contemplate the latter, especially since it refers to the person signing the s 35(7) certificate to be someone in charge of wide area networks or large systems.

[120] Any difficulty posed by what appears in s 35(7) to be a need for a supplementary certificate to comply with all the three requirements in s 35(6) can be resolved by interpreting the provisions to mean that different people can tender evidence to prove these different requirements.

[121] S 35(8). See also the Explanatory Statement, at 16, and Charles Lim, *supra*, note 16, at 4, para 17.

certification requirements.

5. *Effect of Admission*

(a) *Calling for further evidence*

Where admitted computer output is produced by an approved process, section 35(4) presumes such output to be an accurate reproduction. There are no similar presumptions for output admitted pursuant to an express agreement[122] or by way of certification.[123] Arguably a similar presumption should arise, as section 36(1) refers to the court which is "not satisfied" calling for further affidavit evidence[124] or oral evidence[125] as to the accuracy[126] of the computer output. This implies that the court is normally satisfied and no further evidence need be called. Where the court is not satisfied that the computer output accurately reproduces the relevant contents of the original document,[127] by section 36(1), it may exercise its discretion and call for further evidence. The further evidence[128] by way of affidavit evidence can come from the certifying authority, a responsible person in relation to the operation of the computer, the person who had control or access, or had been given such control or access, over the relevant records and facts, or a court expert.[129]

But further affidavit evidence can only be called for where the computer is used as a data storage device, because section 36(1) and (2) contemplate the circumstance where the computer output "reproduces the relevant contents of the original document", a clear reference to recorded output. Where the computer is used as a data processing device, the relevant provision to refer to is section 36(3), which applies to all computer output, and which gives the court the discretion to require "oral evidence be given of any matters

[122] S 35(1)(a).
[123] S 35(1)(c).
[124] S 36(2).
[125] S 36(3).
[126] S 36(1) read with s 36(3).
[127] S 36(1) and (2) only apply to computer output which reproduces the contents of the original document. S 36(3) however applies to all computer output.
[128] In *Shephard*, *supra,* note 63, Lord Griffiths opined that for s 69, PACE, *supra*, note 73, a higher level of technical expertise is required for a certificate since the certifier cannot be probed in cross-examination, but a testifying witness is there to be probed as to his adequacy of knowledge so a lower level of expertise is permissible. Thus a person who is actually testifying in court need not be as technically competent as the certifier.
[129] S 36(2).

concerning the accuracy of the computer output."

(b) *Weight of computer output*

Section 36(4) contains a statutory reminder that the weight of computer output has to be subjected to close scrutiny, "regard [being] had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the output." The court is urged to have regard to two factors in particular:

- the contemporaneity of the supply or recording of the input with the occurrence or existence of the facts dealt with in the input;[130] and

- whether the supplier of information or person involved in the processing of such information had any incentive or motive to conceal or misrepresentation the information.[131]

Unlike section 36(1) and (2), which applies only to recorded output, section 36(4) applies uniformly to both recorded output and processed output. Thus section 36(4)(a) requires the court to inquire as to whether the input "which the output reproduces or is derived from" was contemporaneous with the facts and section 36(4)(b) refers to both the "supplier of the information" and "any person involved in the processing of such information".

(c) *Ancillary evidence*

Once computer output is admitted under section 35, evidence may be adduced to contradict or corroborate it. In addition, by section 36(5), evidence may be adduced to impeach or support the credibility of the person "by whom [the computer output] was made" or the person "by whom the information was processed". Again, section 36(5) does not discriminate between recorded output and processed output: in either case, the credibility of the supplier or processor of information may be impeached or supported. However, unlike section 160 of the Evidence Act and section 383(b) of the CPC, the scope of attack is limited, for no further evidence can be adduced if this person has been called as a witness and has denied the matter upon cross-examination. This must be because where the output is a record of

[130] S 36(4)(a).
[131] S 36(4)(b).

a statement, the person "by whom [the computer output] was made" is not necessarily the person who makes the statement contained in the output. The former may be a mere amanuensis for the latter.[132] However, where the first-mentioned person makes the statement as well as the output, and his statement is admitted pursuant to sections 32 and 35, section 160 necessarily overrides section 36(5) and permits an extended line of cross-examination for the purpose of impeaching his credibility. Where the output contains processed information, both the person supplying the information as the input and the person processing the output do not directly control the processed output. The output is at least one step removed from the direct engagement of these persons because the computer is processing the input to obtain the output. Hence the limited line of cross-examination which can be adduced pursuant to section 36(5).

PART III: LEGAL ANALYSIS

A. *Distinguishing between Proper "Use" and "Operation"*

Section 35(1)(c) makes a useful distinction[133] between the proper "use" of a computer and its proper "operation", a distinction maintained in the Evidence (Computer Output) Regulations for output admitted pursuant to an approved process.[134] There is no reason why the same distinction should not be made by the parties who have entered into an express agreement to admit computer output under section 35(1)(a).

It is submitted that the nature of the differences between the computer's proper "use" and its proper "operation" depends on whether the computer is used as a data processing device or as a storage device. As a storage device, the computer will be used for data input, and for extracting the

[132] *Jones* v *Metcalfe* [1967] 3 All ER 205, *R* v *McLean* (1967) 52 Cr App R 80.

[133] Bradgate, *supra*, note 106, at 146, submits that improper operation frequently overlaps with unauthorised use. But it is the view of this author that a distinction is maintainable, although this calls for a detailed examination of the purpose for which the computer is used, as demonstrated in the main text.

[134] For instance, in the First Schedule, para 5, a distinction is drawn in the data capture process between the committal of the document image in the computer, and the possibility for image editing, image enhancement and alterations to captured digital images. In para 6, for the image storage and management process, image integrity requires a proper backup and recovery of the image and image and data security. Similar concerns underlie image output in para 7. Considerations such as image, physical, environmental, system and application security, audit trails and image changing all deal with computer usage. The other considerations deal with the proper operation of the computer.

[135] *Supra*, note 48.

stored data to obtain the output. Where data input is automated eg like the automated film record of radar displays in *The Statue of Liberty,*[135] the "use" of the computer is arguably its "operation". The distinction between "use" and "operation" is clearest if the human operator uses the computer to input data, and the computer is then operated to record or store such information. Conversely, when the data is sought to be extracted, the computer is "used" by a human operator and the computer is "operated" to extract and retrieve such information. The "operation" element emphasises the mechanical functioning of the computer, whereas the "use" element emphasises the human operation of the computer.

If the computer is used to process information, its "use" and "operation" are necessarily more complex. Since a computer is used to process information, considerations as to its "proper use" include the circumstances and environment in which the computer is used, and the degree and extent of human intervention in its data processing. For instance, if a radar gun is used to measure the speed of moving vehicles, considerations as to its "proper use" will be factors such as whether the gun is used by an authorised person such as a police officer or by a person trained in its use, whether it was properly aimed at the speeding car and whether the officer was in a moving vehicle when he used the radar gun.

In addition, some devices require some initial settings before it can operate. But not all "uses" will affect the operation of the machine. If these settings are by way of calibration, they would affect the operation of the machine. Thus in *Mehesz* v *Redman*[136] the court described the use of standards containing known amounts of alcohol to calibrate the gas chromatograph used for measuring the amount of alcohol in blood sample, both before and after the use of the instrument for measuring the actual sample of blood in question.[137] By way of contrast, in *Castle* v *Cross,*[138] the court described eleven steps in the correct procedure for using the Intoximeter to measure the alcohol in the subject's breath sample. The operator is required to enter the operator's name, the subject's name and the subject's date of birth for such information to be shown on the printout. Arguably, while errors in entering such information will affect the Intoximeter's use, such errors would not affect the machine's operation. Again, though the output is inaccurate

[136] (1979) 21 SASR 569.
[137] *Ibid*, at 570-571.
[138] *Supra*, note 39, at 89e.

because it will show incorrect details such as the names of the subject and the operator, the output may nonetheless contain other information that would remain accurate. For instance, in *R* v *McKeown,*[139] the Intoximeter used by the police recorded a time that was at least 15 minutes slow.[140] The court took expert evidence that the clock mechanism in the Intoximeter was separate from the alcohol analyser unit in the Intoximeter and thus the error in the clock display as reflected in the erroneous Intoximeter printout, did not affect the operation of the analyser and hence the accuracy of the Intoximeter output in relation to its measurement of the blood alcohol level.

To generalise, the human "use" of the computer is separate from the "operation" of the computer, but the former may affect the latter, depending on the nature of the use, the mode of operation of the computer and the nature of the data recorded or processed.

B. *"Accuracy" and "Authenticity"*

So far, this article has avoided references to the term "authenticity", except in relation to section 35(1)(a) where it is provided that the parties may express agree not to dispute "the authenticity and the accuracy" of the contents of the computer output. Having explained the operation of sections 35 and 36, it is now opportune to examine the requirements of "authenticity and accuracy" in detail.

What exactly is this dual requirement of "authenticity and accuracy"? Section 35 is replete with numerous references to the term "accuracy". For instance, section 35(1)(c) sets out the two requirements needed for a certification of an accurate computer output: that the computer must not be improperly used (the proper use requirement), and that the computer was operating properly (the proper operation requirement). But section 35(1)(a) uses the expression "authenticity or accuracy". This seems to imply that "authenticity" and "accuracy" are two separate and independent requirements. It is submitted that these two requirements are very closely related to each other. Furthermore, if "authenticity" is given its proper interpretation (outside of section 35), an authenticated item of evidence is an accurate item of evidence. In addition, one should make the section 35(1)(a) conception of "authenticity and accuracy" coincide with that in

[139] [1995] Crim LR 69 reports the judgment of the Queen's Bench Divisional Court. The House of Lords has just delivered its judgment allowing the appeal from the Divisional Court. This judgment has not been reported at the time of the writing of this article.

[140] The court accounted for the actual 1 hour 15 minutes discrepancy by noting that this was due to the implementation of daylight saving time.

section 35(1)(c), because there is no reason to interpret the requirements any differently in the preconditions. If so, references to "accuracy" in section 35(1)(c) and the mechanics of the certification process should be interpreted with the concept of "authenticity" in mind.

1. *Meaning of Authenticity*

When the proponent tenders a piece of writing as evidence of its contents, the relevance of the writing "will frequently be logically dependent upon the existence of some connection between that writing and a particular individual."[141] And where an object is tendered instead, "an adequate foundation for admission will require testimony first that the object offered is *the* object which was involved in the incident, and further that the condition of the object is substantially unchanged."[142] In other words, the relevance of any item of evidence will depend on its authenticity, *ie*, "upon its being what it purports to be or what its proponent claims it to be".[143]

This author acknowledges that these expositions of what constitutes "authenticity" have been taken from the American jurisdiction, where this concept is very well developed.[144] But as the Australian Law Reform

[141] McCormick on Evidence, (3rd ed, 1984), at 686. This is often termed "authentication" proper. See Schiff, *Evidence in the Litigation Process* Vol II, (4th ed, 1993), at 1069.

[142] McCormick, *ibid*, at 667. This is often termed "identification" proper. See Schiff, *ibid*, at 1069. See also 7 Wigmore, Evidence § 2129 (Chadbourn rev. 1978), at 709, where Wigmore argues that the term "identification" presupposes two objects for which there is a need to determine whether they are identical and not separate objects, whereas "authentication" presupposes only one object.

[143] Morgan, *Basic Problems of Evidence* (1957 ed) Vol II, at 327. Hoey in "Analysis of The Police and Criminal Evidence Act, s.69 – Computer Generated Evidence", [1996] 1 Web JCLI (http://www.ncl.ac.uk/~nlawwww/1996/issue1/hoey1.html), takes the view that where it is alleged that alteration of records, digital or paper-based, has taken place, the document remains admissible and this is only a question of weight, not admissibility. With respect, this is an oversimplification. A forged record has no weight at all – its authenticity has to be established as a precondition to its admissibility. Such a view all but reinforces the warning issued by Wigmore, *supra*, note 142, not to admit documents whose authenticity is in issue.

[144] See Rule 901 – Requirement of Authentication or Identification, US Federal Rules of Evidence 1975.

[145] In *R* v *Governor of Pentonville Prison ex p Osman* [1989] 3 All ER 701, at 727, the court was inclined to the view that that before the judge can decide on admissibility, appropriate authoritative evidence must be adduced to describe the function and operation of the computer. In *R* v *Shephard*, *supra,* note 63, at 383, the House of Lords said that in the vast majority of cases, it is possible to discharge this burden by calling a witness familiar with the operation of the computer, and that it will be very rarely be necessary to call an expert to prove that the computer is reliable. These cases could be seen as elaborations of the "authentication" requirement.

Commission noted, "it is difficult to find an analysis by Australian or English writers[145] of the basis upon which evidence authenticating or identifying proferred [sic] evidence is required."[146] The Evidence Act suffers less from this problem. Stephen, who by his own erroneous reasoning, concluded that there should only be two classes of evidence – oral and documentary – because "the condition of material things, other than documents, is usually proved by oral evidence, so that there is no occasion to distinguish between oral and material evidence"[147] left for us extensive references to the need for authentication, though not referred to as such, in many sections of the Evidence Act.[148] But these relate primarily to the authentication of documents. For non-documentary evidence (or evidence in general), we have to rely on section 9, especially illustration (a). It is submitted that Stephen classified evidence of authentication under this section as "facts necessary to explain or introduce a fact in issue or relevant fact … or which establish the identity of any thing … whose identity is relevant, or fix the time or place at which any fact in issue or relevant fact happened or which show the relation of parties by whom any such fact was transacted." If this interpretation of section 9 is correct, Stephen's observations precede but coincide with those held by Wigmore[149] and Weinstein[150] that authentication is a condition precedent to admissibility.[151] This rule of evidence is now confirmed in the US Federal Rules of Evidence.[152]

2. *"Authenticity" in relation to Different Types of Evidence*

Wigmore convincingly argues that evidence that is not authenticated cannot be admitted because to do so will cause the trier of fact to unconsciously accept other aspects of the party's case, and that the trier of fact upon the proponent's production of the thing or document has a natural tendency to forget that the preconditions to its admissibility have not been met yet and thus the weakness of the proponent's evidence.[153] If authenticity

[146] Australian Law Reform Commission on Evidence: Interim Report No 26, 1985, vol I, at 548 para 979.

[147] Stephen, *An Introduction to the Indian Evidence Act*, at 11.

[148] Ss 9 (especially illustration (a)), 62(3), 69-92.

[149] 7 Wigmore, § 2129, *supra*, note 142, at 703. Wigmore terms the need for authentication as being based on "an inherent logical necessity".

[150] Weinstein and Berger, *Weinstein's Evidence* (1983), §§ 901–18 – 901–19.

[151] See also Michael & Adler, "Real Proof: I" (1952) 5 Vand LR 344, 362, where this is described as "the logical condition of the admissibility of real proof".

[152] US Federal Rules of Evidence 1975, Rule 901.

[153] 7 Wigmore, § 2129, *supra*, note 142, at 704. Paraphrased in the Evidence: Interim Report No 26, 1985, vol I, *supra*, note 146, at 548 para 980.

is a precondition to the admissibility of all evidence, authenticity means different things in relation to different types of evidence. Often, one forgets that non-documentary evidence such as corporeal objects or tangibles have to be authenticated as well. For corporeal objects or tangibles, authentication evidences the connection between the objects and the case ("identity"). It also assures the court of the substantially unchanged condition of the object between its seizure, its analysis and its eventual production, and that the evidence is not tampered with ("immutability"). Thus rule 901(4) of the US Federal Rules of Evidence suggests that authentication can be by way of "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."

Authentication as to identity can be illustrated by cases where there is a doubt as to whether the body of the deceased is the body of the victim of the offence,[154] or as to the identity of the deceased.[155] Authentication as to immutability can be illustrated particularly well by local jurisprudence in the area of "chain of evidence", in which the prosecution is required to prove that the exhibit was the subject-matter seized from the offender.[156] The need for authentication is especially material in drug trafficking cases, since discrepancies as to the weight of the drug and its quality will affect the nature of the offence as well as the possible sentence.[157] Similarly the "chain of evidence" must be show that the seized drug exhibit is not contaminated or mixed with the drugs seized from other accused,[158] which may affect the chemical analysis of the drugs. It must also establish the proper handling and management of the drug exhibits,[159] especially given the lapse of time between the seizure, the chemical analysis to which it is subjected and its eventual production at the trial.[160]

For processed results, where the device concerned is a scientific or

[154] *Fazal Din* v *Public Prosecutor* [1949] MLJ 123.

[155] *Teay Wah Cheong* v *Public Prosecutor* [1964] MLJ 21.

[156] *Abdul Rashid & Anor* v *Public Prosecutor* [1994] 1 SLR 119. Normally such evidence is not called: *Su Ah Ping* v *Public Prosecutor* [1980] 1 MLJ 75, unless a doubt as to the identity of an exhibit arises: *Teoh Hoe Chye* v *Public Prosecutor* [1987] 1 MLJ 220, *Lim Swee Seng* v *Public Prosecutor* [1995] 1 SLR 425 *per* Thean JA, *Lai Kam Loy & Ors* v *Public Prosecutor* [1994] 1 SLR 787.

[157] *Lim Swee Seng* v *Public Prosecutor* [1995] 1 SLR 425, *Lee Chee Meng* v *Public Prosecutor* [1992] 1 MLJ 322. This is so especially if there was a suggestion that the exhibits seized from other offenders may have been mixed with those seized from the accused, and there was no way of identifying and separating those exhibits from each other:.

[158] *Sia Soon Suan* v *Public Prosecutor* [1966] 1 MLJ 116.

[159] *R* v *Khoo Guan Teik* [1957] MLJ 128.

[160] *Vinit Sopon & Ors* v *Public Prosecutor* [1994] 2 SLR 226, *Abdullah bin Yaacob* v *Public Prosecutor* [1991] 2 MLJ 237.

technical instrument, considerations of authenticity address the question of the description of the process which produced the result ("identification"), and whether the process produces an accurate result ("accuracy"). "Accuracy" here must entail a close examination of all the data processing steps – from choice of processes to input to actual processing to output. Hence rule 901(9) of the US Federal Rules of Evidence states that "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result" is authentication. These considerations meet concerns such as whether the instrument has been tampered with. Authentication also includes considerations such as whether the operators of these devices are affiliated to the parties to the proceedings.[161] For instance, where the event is contemporaneously recorded by a neutral third party using an automated instrument as the event happens, there is less reason to suppose that the evidence produced is suspect.[162] But where an instrument is used by a witness to take measurements or make observations from samples supplied by the proponent, there is good reason to subject the witness, the instrument and the entire observation process to closer scrutiny.[163]

Authenticating evidence tendered for documentary evidence serves to identify, *inter alia*, the source of the writing ("authorship"), the date and time of the writing ("chronology") and to ensure that the writing is not forged or tampered with ("accuracy"). The authorship and chronology coupled with compliance with the prescribed formalities (if any) will together evidence the document's due existence, execution and contents – its "genuineness". Hence in *Tsia Development Enterprise Sdn Bhd* v *Awang Dewa*, the court was fully justified in holding that authenticity is a precondition to a document's admissibility.[164] Though the court may, by section 138(2), permit a document to be conditionally admitted upon the proponent's undertaking to duly prove its authenticity, if the proponent fails to do so, the court has to exclude the document.[165] Our Evidence Act has a very extensive set of provisions designed to deal with the types of evidence authenticating the genuineness of documents.[166]

3. *Applying the Extended Concept of "Authenticity"*

[161] Evidence: Interim Report No 26, *supra*, note 146, at 549.
[162] Such as the radar film record in *The Statue of Liberty*, *supra*, note 48.
[163] See, for instance, *Abdul Rashid & Anor* v *Public Prosecutor* [1994] 1 SLR 119.
[164] [1984] 1 MLJ 301.
[165] *Ibid*.
[166] Ss 69-92.

The analysis above shows that a duly authenticated computer output is an accurate computer output. This is regardless of whether the computer output is evidence of information processed by a scientific or technical instrument, or as a substitute for writing. Where computer output is authenticated, the authenticating evidence will have to show the proper use and operation of the computer. Hence where section 35(1)(a) contemplates an express agreement as to "accuracy and authenticity", the expression is really tautologous if one reads it with section 9 and adopts the extended concept of "authenticity" as explained above: it is really an agreement not to dispute the authenticity of the computer output. One can use the case of *PP* v *Ang Soon Huat*[167] to illustrate this point. If the prosecution tenders a spectrogram – a computer output – to prove the nature and quantity of the substance seized from the accused,[168] considerations of the accuracy of the spectrogram will be that the spectrometer produces an accurate result, and that the spectrogram had not been tampered with to show a forged result. Authenticity will encompass these considerations, as well as considerations such as identifying the process which produced the result (mass spectrography), identifying who and what produced the spectrogram (the spectrometer produced the spectrogram and the identity of the operator of the spectrometer), and establishing when was the spectrogram produced (chronology). It is really quite hard separating these two sets of considerations of accuracy and authenticity: choice of processes, operators and usage obviously affect the accuracy of the output.

One cannot take the expression "[not to dispute] the accuracy of its contents" in section 35(1)(a) to mean that the parties agree not to dispute the contents of the output. Otherwise, by section 60, the facts stated in the contents need not be proved and the computer output need not be admitted. If it were otherwise, by section 36(5), the opposing party cannot tender evidence to contradict the output or impeach the credibility of its maker. Also, by section 36(1), there would be no grounds for the court to call for further evidence if it is not satisfied as to the accuracy of the computer output, or by section 36(4), to estimate the weight to be given to such evidence, and by section 35(10), there can be no dispute that the original document is not the same as the computer output. This shows that "accuracy" here must be understood in the sense of "authenticity". If the parties agree not to dispute the authenticity of the output, it is still open to them to dispute the facts represented in the authenticated output.

By examining section 35(1)(b) and 35(1)(c) in more detail, one can see that this is a harmonious interpretation of the section 35 preconditions. So

[167] *Supra*, note 65.
[168] That it is diamorphone, and that weighs 18.77 grammes.

where computer output is admitted pursuant to an approved process, the Evidence (Computer Output) Regulations require the imaging system to ensure image integrity and to disallow any changes to be made to the digital image of the document.[169] Where changes are made to the digital image, steps have to be taken to ensure that the new changes can be distinguished from the original digital image.[170] These are clearly requirements of authentication.

Perhaps it is for the same reason that section 35(1)(c) fails to mention the need for "authenticity", because in establishing that there is no improper use of the computer, that no reason exists to doubt or suspect the truth or reliability of the output, and that the computer was operating properly, the proponent is in effect establishing, in some respects, the authenticity of the output. As previously explained, interpreting "authenticity" to encompass "accuracy" has the beneficial effect of rendering section 35(1)(c) consonant with section 35(1)(a). Such an interpretation also explains why section 35 is made to supplement all other admissibility provisions, in that computer output which is *prima facie* admissible under any written law has to be further authenticated before it is actually admissible. In addition, it explains why section 35(10) states that "any computer output tendered in evidence under this section" has to be "duly authenticated" before section 35(10) applies.

It is submitted, however, that establishing the proper use and operation of the computer by section 35(1)(c) will not establish all the various aspects of the authenticity. Authenticity encompasses other elements such as identification, authorship and chronology. But perhaps there is no lacuna in section 35(1)(c): if one is reminded by section 35(10) that computer output has to be "duly authenticated", this can be additionally established pursuant to the need to show that "no reason exists to doubt or suspect the truth or reliability of the output" spelt out in section 35(1)(c)(i) itself, as a requirement over and above the requirement of proper use. And arguably, this expression is also wide enough to permit the court to consider not just the output itself for accuracy, but also the input which goes into making the output.[171] In fact, section 36(4)(a) mandates that the court examine the contemporaneity of the input to assess the weight of the output. In addition, one can supplement section 35(1)(c) with section 9, the generic authentication

[169] Para 6(a), (b), First Schedule, Evidence (Computer Output) Regulations 1996.
[170] *Ibid*, para 5(h).
[171] Bradgate, *supra,* note 106, at 145, makes the point that the means of supply of information to computer and accuracy of input cannot be ignored for purposes of assessing the authenticity of the output.

provision in the Evidence Act, to ensure that computer output is "duly authenticated". All these provisions operate together with section 167, to permit the court to call for authenticating evidence, "in order to discover or to obtain proper proof of the relevant facts."

C. *Computer Output as Stored Records*

Today, computers are used both as data storage devices and as data processing devices. In the business community, computers are primarily used as data storage devices to store records which were previously kept in documentary form. It is assumed that computers are reliable data storage devices.[172] And rightly so, for modern forms of data storage are extremely reliable,[173] and these devices also deploy various processes to track errors in data recording and storage.[174]

So where computers are used as data storage devices, one can validly assume that computers operate properly. The proper "use" of the computer appears more significant than its proper "operation". In fact, where the human "use" element is ignored, computers have such an aura of trustworthiness that output generated from such computers is often assumed to be accurate. This has certainly led Steyn J to observe that "the failure of a computer, or a software programme, may occasionally result in a total failure to supply

[172] Some forms of computer output are really "processed" information. For instance, modern computers operate in the form of computer networks where data concerning a particular individual or entity are actually digitally reconstituted from physically and digitally discrete databases maintained by different computers. The modern "client-server" model of data computing draws heavily on this paradigm. Digital imaging is also arguably data processing, since analog images of documents have to be digitally converted. For these forms of computer output, both sets of considerations in relation to the authentication of computer output as stored records and as processed results must apply.

[173] The CD-R, or recordable CD-ROM, is a data storage device like a CD containing a layer of organic chemicals, instead of a layer of aluminium, which can be "burnt" by a laser to record information. The CD-R has a shelf-life of almost 30 years. Hard disks, which are the main secondary storage media for most computers today, have a Mean-time Between Failure ('MTBF') rate which runs into hundreds of thousands of hours. An MTBF of 100,000 hours translates into a continuous use of a hard disk for almost 12 years before it fails. However, all these presuppose that the data storage devices are kept in the proper environment.

[174] Numerous mathematical methods are now deployed to ensure the integrity of data once it is recorded in digital form. These range from the very simple such as parity checks to Cyclic Redundancy Checks to detect even one error in thousands of bits of information, or Reed-Solomon Error Correction codes that actually allow errors to be mathematically corrected. See generally, *Dr Dobb's Journal*, Issue 261, January 1997, at 30 for a discussion of Reed-Solomon codes, and Issue 5/92 for a discussion of Cyclic Redundancy Checks.

the required information, or in the supply of unintelligible or obviously wrong information. It will be a comparatively rare case where the computer supplies wrong and intelligible information…"[175] In *US* v *Vela,*[176] the court echoed similar sentiments: it considered computerized records more reliable than the "average business records" because they were "not even touched by the hand of man".[177] But section 35(1)(c) correctly reminds us that the common law presumption of *omnia praesumuntur rite esse acta* and the extravagant judicial statements above are incomplete and are actually misleading because accurate computer output depends not just on the proper operation of computers, but also on the proper human use (or abuse) of computers.[178]

1. *How Data is Stored*

Thus distinguishing between the human "use" of the computer and the "operation" of the computer as a data storage device will assist the parties and the court in deciding whether such output is adequately authenticated. It is submitted that where the computer output is tendered as evidence of the contents of the original document, the court should have regard to the following considerations:

(i) what is the nature of the information and the circumstances in which such information as indicated in the output is supplied to the computer, *eg*, lapse of time between the facts stated and the

[175] *R* v *Minors and Harper*, *supra*, note 47, at 214a-b.
[176] 673 F.2d 86 (5th Cir, 1982).
[177] *Ibid*, at 90.
[178] In fact, this impregnable aura of reliability can often be abused by operators who make alterations to electronic records, and the digital nature of electronic records in fact makes data alteration very simple and in fact untraceable if insufficient security safeguards and audit trails are put in place. All digital records are really stored in the form of ones and zeros in their various manifestations eg presence/absence of current in electronic circuits, presence/absence of pit in CDs, presence/absence of magnetic field in tapes and other forms of magnetic media. As a norm in the use of information technology, the inherent "alterability" of digital records means that altered records will override existing records, and generally there will be no traces of the existing records left. The error-correction and error-trapping mechanisms explained above do not assist, since these alterations will necessarily result in the updating of these error-correction and error-trapping data inserted into the digital records themselves to reflect the altered records. This is so unless separate records are kept of these error-correction and error-trapping data, *eg*, by way of audit trails.
[179] S 36(4)(a).

actual supply of such information to the computer,[179]

(ii) whether the supplier of the information had any incentive or motive to conceal or misrepresent the information so supplied,[180]

(iii) whether such information is properly recorded in the computer for retrieval purposes,[181]

(iv) whether such information has been manipulated or altered through improper use of the computer,[182]

(v) whether the computer is operating properly when such information is retrieved or extracted from the computer,[183] and

(vi) what are the circumstances in which such information is retrieved or extracted from the computer by way of the computer output.[184]

Out of these six steps, only steps (iii) and (v) involve the operation of the computer – the "material times"[185] on which the computer must be operating properly are at the time of recording and at the time of retrieval. Of course, the computer must ensure data integrity in the interim. Steps (i), (ii), (iv) and (vi) all involve opportunities for human misuse of the computer.

Authenticating computer output as records requires the court to ascertain their authorship, chronology and accuracy. Most written documents will bear a signature, or carry on their face signification of authorship such as handwriting. It accords with sound business sense to sign written documents and records, whereupon the signature becomes an inherent part of the document. However, digital records commonly used in most industries in business have to be specially designed to carry significations of authorship – authorship information is not normally maintained for computer records. And authorship in digital records can refer to the supplier of information or the recorder of such information – they are rarely the one and same person. For instance, in a business accounting system with a very large database of accounting records, the authorship of each entry will be different,

[180] S 36(4)(b).
[181] S 35(1)(c)(ii) read with s 35(6)(b).
[182] S 35(1)(c)(i).
[183] S 35(1)(c)(ii) read with s 35(6)(a).
[184] S 35(6)(a).
[185] S 35(1)(c)(ii).

depending on which clerical staff keyed in which entry. But the clerical staff may obtain the information from some other source. In practice, many digital records in businesses do not contain authorship information, since it is perceived, rightly or wrongly, that such information takes up unnecessary valuable digital space, which could be used for other, more valuable, non-authorship information such as descriptions and prices. Reimposing authenticity will refocus the computing industry's attention on the need for authenticated digital records.

In addition, the chronology of a digital document can be very difficult to establish. As a general rule, computers maintain digital records together with the dates and times of creation. But there are different levels of details in which chronological information is kept: the time of creation, modification, printing, deletion, and the time for each record or for the entire database as a whole. Furthermore, chronological information for computer records can be kept separately from the digital records themselves, so such information can be altered to give digital records the appearance of age without affecting the contents of the documents themselves.

Also, to refer to the chronology of computer output is very awkward, since computers used as data storage devices seldom produce the output contemporaneously with the happening of the event recorded. There will inevitably be time lags between perceiving the event in question, the supply of information describing the event, the recording of such information and the output of such information. These time lags provide opportunities for fabrication of output. And unlike written documents that can age with time because of their physical and tangible existence, and thus can be forensically tested for forgeries, digital records are inherently mutable, intangible and timeless. Digital records can be falsified to make them "age", just as their contents can be altered or fabricated, without being easily detected.

Requiring computer output as records to be authenticated seeks to refocus the court's attention on all these concerns, if the court bears in mind the way in which data is stored in computers.

2. *Admitting Output under the Evidence Act*

This analysis demonstrates that when parties choose to expressly agree that their computerised business records be admissible in evidence pursuant to section 35(1)(a), their agreement not to dispute the "authenticity and accuracy" of the output should optimally encompass all these material steps, with especial emphasis on those steps that involve human intervention. Parties engaged in more contentious matters may wish to limit the admissibility of computer output by expressly prescribing parameters for one or more of the steps of data storage. For instance, as to step (i), the parties may agree that only certain types of information recorded within a certain

time from its occurrence by certain people shall be admissible. As to steps (ii) and (iv), the parties may agree that only certain neutral parties shall handle the input and maintenance of the computer records, or that the records be kept in escrow. And as to step (vi), the parties may agree that where the evidence is sought to be tendered for purposes of legal proceedings, it shall be extracted from the computer in the presence of legal representatives from both parties who shall each receive a copy of the computer output. Computer output produced under such constraints is, by express agreement, authenticated, in the interests of both parties.

The Evidence (Computer Output) Regulations similarly address these various steps of data storage.[186]

Where the proponent elects to admit computer output via the certification process of section 35(1)(c), the proponent may ease his authentication burden by closely supervising the proper use of the computer. As this is a managerial problem rather than a sysop problem, managerial controls such as user access privileges, issuance of passwords to authorised personnel, maintenance of a log of users and a set of secure computers for certain transactions, system and password security, limited physical access and even more sophisticated schemes such as data encryption and digital signatures will all contribute positively to the certification process. Controls such as those outlined above allow the certifier to provide details such as the identities of the supplier and recorder of information, chronological information such as the date and time of data entry, and the proper use of the computer.

For the sysop, because the computer is merely used as a data storage device, the proper and reliable operation of the computer is actually more easily established, by way of the principle of *omnia praesumuntur rite esse*

[186] See the First Schedule of the Evidence (Computer Output) Regulations 1996.

[187] In *R* v *Shephard*, *supra*, note 63, the House of Lords rejected the use of this presumption, but only because s 69(1)(b), PACE, *supra*, note 73, requires the proponent to show that the computer was operating properly by way of a mandatory certificate. However, it is not mandatory to use certificates to prove the preconditions in s 35(1)(c), so there may be some room for the presumption to operate in relation to s 35(1)(c)(ii). Also, all that the proponent has to establish in s 35(1)(c)(ii) is that there is reasonable ground to believe that at all material times the computer was operating properly.

[188] 7 Wigmore, §2131, *supra*, note 142, at 712-714; Morgan, *supra*, note 143, at 327. Thus in *R* v *Governor of Pentonville Prison ex p Osman*, *supra*, note 145, the court inferred the proper functioning of the computer from the fact that the computer printout contains no internal evidence of malfunction and is retained as part of business records. Similarly, in *R* v *Mather* [1991] Crim LR 285, it was argued that where a computer produces inaccurate results, that is almost likely to be detectable or result in the processing of erroneous data. Surely these statements must only refer to the errors in the operation of the computer. It is humanly possible to forge a computer output to show completely false information, yet it may look perfectly authentic.

acta.[187] Evidence that the computer is operating properly can be established by way of circumstantial evidence.[188] Thus the court can infer that the computer is operating properly at the material times if there is evidence before the court that the computer is operating properly just before or after the material times. The regular proper operation of the computer, unlike human use (or abuse), is something which can be empirically duplicated and demonstrated.

3. *The Rule against Hearsay*

Where computers are used as data storage devices, they are used to record information or facts perceived through human intervention. The computer does not "contribute its own knowledge". It is thus right and proper that the hearsay rule, whose objective is to ensure that out-of-court statements by the maker do not go untested, should apply equally to output from such computers as it applies to other forms in which such statements are recorded. If the output contains an out-of-court assertion by the maker, unless the assertion is admissible by way of a hearsay exception, the fact that it is tendered by way of computer output should not make any difference as to whether the hearsay rule applies. For the same reason, dangers associated with hearsay statements are equally to be found in computer output: the perception, memory, veracity and accuracy of narration of the maker cannot be tested in cross-examination if his statement is admitted.[189]

Some authors have however argued that there should be no need to authenticate computer output as hearsay statements once the statements themselves are admissible pursuant to a hearsay exception.[190] Reference is commonly made to the business records exception,[191] in that business records are in effect admitted on the basis of reliability and necessity. It is argued that business records are reliable because the statement maker would use such records for the management of his business, and they are necessary because there are no records otherwise kept of business activities. However, it is submitted that evidence of authentication highlights some additional and unique problems with computer output that are not necessarily taken into consideration when the business records exception is applied. If one considers the six steps set out above, the business records exception clearly cannot manage issues such as whether the recorded information has been improperly manipulated or altered, whether the computer is operating properly when recording, storing and extracting such information, and under what

[189] Morgan, *Some Aspects of Proof under the Anglo-American System of Litigation* (1956), Chaps 4-6.
[190] See Bradgate, *supra*, note 106, at 142, 146.
[191] S 32(b). The US equivalent in the Federal Rules of Evidence 1975 is Rule 803(6).

circumstances is the information extracted from the computer (steps (iv) to (vi) respectively).

It has been said, however, that since the rules of evidence are always alive to the possibility of fabrication of documents, and that computers used as data storage devices are presumed to be operating properly, computer records pose no unique problems to the business records exception. But it has been convincingly shown that step (iv) is really the Achilles' Heel of computer output.[192] The problem with manipulation or alteration of computer records is that unlike documentary records, such manipulations or alterations are almost invariably untraceable.[193] This is inherent in the nature of electronic records. While the business records exception does not preclude the opponent from challenging that the output has been manipulated or altered, often the opponent will encounter many difficulties in so establishing, because he does not have easy access to the proponent's computer system nor does he have knowledge of its usage policy. Having only the business records exception in effect casts the evidential burden on the opponent to challenge the authenticity of electronic records. This is really an unfair burden, because the opponent is at an information disadvantage, as explained above.[194]

The effect of section 35 is to reverse the burden and place it on the party who is in the best position to supply the requisite information as to the proper use and proper operation of the computer. For the reasons advanced above, this must be correct. So our business records exception, section 32(b), must be applied cumulatively with section 35 to admit hearsay business records.

One caveat is however in order. The business records exception in section 32(b) generally applies to statements made by the maker who has himself personal knowledge of the matters so recorded. But where the matters are recorded using computers, the person who supplied the information ('the supplier') is not necessarily the recorder or maker of the output. There may be an intermediate, documentary record by the supplier that will be entered into the computer system by an operator. Alternatively, the supplier will report the matter to the operator who will then enter such information into the computer. Such digital records will be second-hand or multiple hearsay and are inadmissible. So the fact that they are computer output actually hinders their admissibility, because section 32(b) appears to only admit first-

[192] Peritz, "Computer Data and Reliability: A Call for Authentication of Business Records under the Federal Rules of Evidence", (1986) 80 NWULR 956.

[193] See discussion in main text at *supra*, note 85.

[194] As explained above, this would be so unless additional security measures are put in place to ensure data integrity.

hand hearsay. Three exceptions are, however, possible: the first is where the computer record is actually secondary evidence of the intermediate documentary record, and the second is where the record as output is made pursuant to section 380, CPC, which permits multiple hearsay records to be admitted, as long as they are recorded under a duty. The third solution is where the supplier reads over and verifies the information keyed into the computer by the operator, whereupon the record is considered to have been made by the supplier.[195] These three exceptions must be clearly elucidated when digital business records are sought to be admitted.

D. *Computer Output as Data Processing Results*

Computers which are used as data processing devices[196] can be classified into the following categories: devices which accept human-supplied input and produce output, self-contained data processing devices which obtain input or take recordings from the environment without human intervention, and a hybrid of the two. Illustrations of each category of devices can be found in the various cases. The first category is used in *R* v *Wood*[197] where the computer is used to compute the quantity of metals given certain readings from other instruments. In *The Statue of Liberty*[198] where the radar device automatically records on film the radar images without human intervention, the device clearly falls into the second category. An illustration of a device that falls into the third category is the Intoximeter featured in *Castle* v *Cross*[199] where the operator keys in particulars of the subject and the operator into the Intoximeter before using it to measure the breath sample of the subject,

[195] Subject to the rules in *Jones* v *Metcalfe* and *R* v *McLean*, *supra*, note 132.

[196] In a sense, it is true that all data storage devices are also data processing devices, since data is never stored in the computer in the same form as it originally took in the form of input but is converted (read "processed") into digital form (if it is not already in that form) and then stored. So photographs, images and sound all have to be "digitized" before they can be stored digitally. The process of "digitization" is really a data processing step. The distinction between data processing and data storage devices may really be one of degree, but it is submitted that one way of concluding that digitization devices are really data storage devices is to note that such devices are designed to reproduce data in as accurate a manner as possible. So there is a presumption that such devices are operating properly as data reproduction devices, and that most of these devices do not permit human manipulation after the data is digitized. This, however, is a presumption which can be rebutted, *eg,* there are digital cameras which permit images to be manipulated before they are sent for printing.

[197] *Supra*, note 43.

[198] *Supra*, note 48.

[199] *Supra*, note 39.

[200] *Supra*, note 54.

and the output records the names as well as the computed alcohol amount. The device used in *Pettigrew*[200] is arguably also a device that falls into the third category, since the operator is actually required to record the serial number on the first note in the bundle, and the computer counts the bundle and records the serial numbers of the first and last notes as well as the numbers of any rejected notes.

Computers can be used both as data recorders as well as data processors. And in practice, the two different uses can produce a single output. In *Shepherd*, the House of Lords rightly observed that even for a supermarket till receipt, the receipt contains both recorded as well as processed information.[201] The provenance of each type of information and each different computing devices have to be separately established. The House of Lords noted that the till receipt is generated by the till machine plus the central computer housed within the supermarket premises: both together constituted the relevant computer. The price for each product is recorded information – based on the price information retained by the central computer, and the total price is processed information – based on the addition of the prices of all the products. The name of each product listed in the receipt is both processed and recorded information, since sometimes the operator keys in the identity of the product manually; for other products, the till device reads the UPC[202] from the product, and matches that against its internal database of names of products.

While this distinction may be criticised as being unduly technical, it does permit the court to easily resolve the problem faced by the House of Lords in *McKeown*[203] where the Intoximeter output contains inaccurate time information, but accurate breath alcohol readings. As a whole, the output is inaccurate, but the output is still a valuable piece of evidence.[204] The time information is clearly recorded information,[205] whereas the reading information is processed information. One does not affect the other. On this basis, the House of Lords admitted the output. The authenticity analysis

[201] *Supra*, note 63.

[202] Universal Product Code – the bar code found on most retail products, which is used to identify the product concerned.

[203] *Supra*, note 139.

[204] This led Professor Tapper to note the distinction between the accuracy of the document produced by the computer and the accuracy of the statement contained therein: though part of document that is inaccurate has no connection with part sought to be relied on, such a document ought to remain admissible. *Supra*, note 57, at 85.

[205] There was evidence before the court that the machine had been set to the wrong time, and there was no evidence to suggest that the machine recorded the wrong time because of the improper operation of the time unit in the Intoximeter.

yields the same results: the authenticity of the document (in terms of its origin and circumstances of production) and the authenticity of the reading (in terms of the proper operation of the Intoximeter) are not disputed. The authenticity of the document (as to its time of production) is established by extrinsic evidence. The authenticity of the document as a whole is established, and the document should be admitted.

1. *How Data is Processed*

This categorisation readily lends itself to an analysis of the following steps involved in using computers as data processing devices:

(i) what is the nature of the input and the circumstances in which the computer takes such input from the environment,[206]

(ii) whether human-perceived input is supplied to the computer,

(iii) whether the supplier had any incentive to conceal or misrepresent such input,[207]

(iv) whether the computer and the computer program are operating properly in processing such input to produce the required results,[208]

(v) whether the computer or the computer program is manipulated or altered to produce the desired results,[209]

(vi) whether such results are stored or is the output generated contemporaneously, and

(vii) if so, the circumstances in which the results are retrieved or extracted from the computer and the output generated.[210]

Again, the "use" and "operation" analysis greatly assists us in identifying the various dangers associated with computer output. Steps (i), (iv), (vi) and (vii) directly engage the proper operation of the computer. Steps (ii),

[206] S 36(4)(a).
[207] S 36(4)(b).
[208] S 35(1)(c)(ii) read with s 35(6)(b).
[209] S 35(1)(c)(i).
[210] S 35(6)(a).

(iii) (v) and (vii) all involve some human intervention, and thus give rise to opportunities for computer misuse.

2. *Admitting Output under the Evidence Act*

Where parties choose to expressly agree not to dispute the "authenticity nor accuracy" of output from computers used as instruments, because such output is treated as "real evidence" and admissible as such,[211] the parties ought to exercise caution in agreeing that all such output be authenticated. Output as real evidence, unlike output as records, do not have to pass through the filter of the rule against hearsay. Furthermore, the accuracy of the output may largely depend on the nature of the input, which has to be closely scrutinised. So as to step (i), the parties may wish to confine computer output admissible by express agreement to only certain kinds of clearly identifiable input and to certain kinds of computers that are used for specific purposes. As to (ii) and (iii), where human input is required, the agreement may require such information to be supplied by neutral third parties, and that such information be independently verifiable.[212] The parties will require information as to the proper operation of not only the computer, but also its computer programs, and that the computer and its programs are not modified without notice to the other party.[213] It ought to be noted that the definition of a "computer" in the Evidence Act does not encompass its computer programs, even though one would have thought that the accuracy of output depends more upon the program than the computer, since the program is really a set of human instructions to the computer to operate on the input, and programs are known to contain errors in coding and in operation. However, this ought not to prevent the court from adopting the general rules of authentication, and requiring authentication of the programs that operate the computer.

As regards step (vi) and (vii), where the results are not contemporaneously generated from the computer, the same concerns with computers as data storage devices should be addressed, since computers which store processed results provide the opportunity for data manipulation and tampering.

[211] There is some difficulty in admitting computer output as real evidence in the Evidence Act, especially since such output invariably takes the form of documents. See YL Tan, "Making Sense of Documentary Evidence Pt II" [1994] SJLS 111 at 119 *et seq*. This is because s 3 defines documentary evidence as all documents produced for inspection by the court. Professor Tan has suggested that one solution is to interpret this definition narrowly, to mean documents produced for the purpose of inspection only, and not for the purpose of admission into evidence.

[212] S 59b(2)(b), South Australia Evidence Act 1929.

[213] S 59b(2)(e), South Australia Evidence Act 1929.

Output from computers operating as data processing devices are not admissible by section 35(1)(b), since by section 35(4), such output has to be a reproduction of the contents of an original document.

Where a proponent seeks to admit output by certification by section 35(1)(c), as explained above, the certificate will contain a serious lacuna if it only authenticates the proper operation of the computer, but not the proper operation of the software as part of the computer.[214] As a technical matter, this probably comes within the purview of the sysop or technical manager. In addition, the proponent will have to offer evidence not only as to the proper use of the computer as spelt out in section 35(1)(c) but also that accurate input has been properly fed into the computer, either by way of automated operation[215] or by way of input by some authorised person who supplies the necessary and independently verifiable data to the computer. In addition, some computers have to be calibrated before measurements can be taken. These details will address steps (i) to (iv), which represent the data processing process. Steps (v) to (vii), which represent the data management process, can be addressed by way of evidence as to the handling and management of the computer after the input has been taken and after the results have been processed.

3. *Word-processed Documents?*

Are word-processed documents processed computer output or recorded computer output? Or are they not computer output at all? In *R* v *Blackburn; R* v *Wade*[216] the Court of Appeal inclined to the view that such documents are better regarded as produced by a human being with the aid of a computer, and are thus not computer output.

Professor Tapper disagrees. He takes the view that this ruling, by way of *obiter*, is not correct, and that the document is a computer output. Professor Tapper reasons that if a computer is merely treated as a inert tool without

[214] The difficulty with this reasoning is that "computers" has been defined in the Evidence Act to mean hardware, and not software. Thus Bradgate, *supra*, note 106, at 144, argues that the definition of computers, which is a definition of hardware, should include software. But the definitions in our Evidence Act have to be interpreted contextually. See s 3(1). Thus arguably, the concept of proper operation in s 35(1)(c) encompasses the software that causes the computer to operate properly.

[215] For instance, by not operating the computer in extreme conditions, or by operating the computer beyond its specifications.

[216] The Times (1992) 1 December.

[217] *Supra*, note 57, at 86-88. Professor Tapper also points out that, for instance, computers can spell-check documents, and so documents produced using a word processor with spell-checking should be considered processed computer output.

a will or consciousness of its own, there would be no distinction between computer-generated and computer-stored output, since human beings in effect cause such output to be produced.[217]

Professor Smith takes the opposite view that *R* v *Blackburn; R* v *Wade* is correct because the computer is merely used as a tool. Professor Smith contends that if the human author reads the printout of his word-processed document to verify its contents, he authenticates it. The document is not a computer output and the computer is treated as a mere tool. But if he does not read his printout, the document is a computer output.[218] With respect, it is difficult to see how reading what is clearly a computer-produced document converts it into one not produced by a computer. The printout remains clearly a document produced by a computer operated as a data storage device.

These problems are engendered because specialised provisions with preset authentication conditions are enacted for admitting computer output, and technically, word-processed documents are computer output. What is required is more flexibility in the authentication provisions. Word-processed documents require a bare minimum of authentication. Since authorship, date of production of the output and data fabrication are never really in issue, the only question is the accuracy of the reproduction of the digitally recorded document in printed form. As to this, even a simple glance at the printout will suffice as circumstantial authenticating evidence that the printout is an accurate one. Also, where spell-checkers are used, currently, software spell-checkers are not smart enough to automatically correct spelling for us. The computer operator is required to confirm or ignore the recommended spell check for each word. He authenticates the operation of the computer and its software in this respect. Again, authentication is not really in issue.

So if word-processed documents are considered computer output, it should be relatively easy satisfying even the certification requirements, though it would appear to be a totally unnecessary hassle. In such circumstances, it is quite likely that even the opponent may express agree not to dispute its authenticity. Once the admissibility provisions are satisfied, additional copies of the document would be treated as secondary evidence and admissible by section 65.

E. *Computer Output as Direct Evidence*

[218] Smith, [1993] Crim LR 295, at 297.

A discussion of the various ways in which computer output may be used would be incomplete without identifying a third category of computer output where the computer is neither used to store data nor to process results. This is the case where the computer and its records are direct evidence of the transaction in question. This is best illustrated with the case of *R* v *Ewing*.[219]

In *R* v *Ewing*, A was charged with uttering forged instruments with intent to defraud. The prosecution's case was that A had altered a warrant for £30 to £1,130, and had paid it into an account that he opened at a bank, from which he subsequently drew £1,130. To prove the payments into and out of the account, the prosecution tendered a computer printout of the account, showing the transactions concerned. The Court of Appeal treated the printout as hearsay, but held that it fell within a hearsay exception[220] since the bank teller who fed the information into the computer could not reasonably be expected to have any recollection of such information, though a diligent search could have identified such a teller.[221]

Professor Smith disagrees. He takes the view that the printout can be, but need not always be, hearsay. If the teller, by keying the appropriate keys, actually credited the account, the printout would prove that the account was credited because the computer records would be the thing done. It would not be hearsay but direct evidence. However, if the teller was merely recording a fact, *eg*, that the account had been credited with a sum by way of direct bank Giro, then the record would be hearsay and so would the printout, since the crediting of the account preceded the actual record itself.[222] On this basis, the view is taken that digital records of on-line electronic transactions such as Electronic Data Interchange transmissions ('EDI') ought to be regarded as real evidence since the electronic documents do not just record the agreement – they constitute the transaction and *are* the transaction documents.[223]

What is the treatment of the Evidence Act in relation to such electronic records? These records are surely relevant and *prima facie* admissible. Evidence required for their authentication is the same as that for objects: evidence has to be adduced to show that they are the records in question, *eg*, because they constituted the transaction in question. In addition, they must be authenticated, *eg*, that they have remained unchanged and have

[219] [1983] QB 1039.
[220] S 1, UK Criminal Evidence Act 1965 (c 20), which is roughly similar to our s 380, CPC.
[221] *Supra*, note 219, at 1051.
[222] Smith, [1983] Crim LR 472, 473. Steyn J (as he then was) in *R* v *Minors; R* v *Harper*, *supra*, note 47, at 212, has ventured, *obiter*, his agreement with this view.
[223] Bradgate, *supra,* note 106, at 147.

not been tampered with since the event in question. Thus an express agreement by section 35(1)(a) must so state. And where the records are sought to be admitted by way of certification by section 35(1)(c), the proper use and proper operation of the computer for the purpose of effecting such transactions must be certified, in addition to the other considerations of authentication.

F. *Secondary Evidence*[224]

So far, the legal analysis has not addressed the question of whether the output concerned is primary or secondary evidence. The general rule[225] is that where the document itself contains contents which are to be proved, primary evidence of the document (the "original document") must be tendered, unless the proponent satisfactorily explains the failure to produce the original document to the court.[226]

This rule is deceptively easy. A document can be "any matter expressed or described upon any substance".[227] So where the computer is used as a data storage device because information is directly recorded into the computer, the primary document[228] itself is the digital record.[229] The output of this document can take different forms – it can be a visual representation on the monitor display, or a computer printout.[230] The output is secondary evidence, since by section 65(b) and illustration (ba), it is a copy made from the original document, the digital record, by an electronic or electrochemical process.[231] If there is an intermediate written record of the

[224] For reference, please consult Evidence: Interim Report No 26, *supra*, note 146, at paras 174-177, 319-324, Morgan, *supra*, note 143, at 327-332, and Martin, *Basic Problems of Evidence* (6th ed, 1988), at 433-460.

[225] S 64.

[226] Morgan, *supra*, note 143, at 332.

[227] S 3(1).

[228] Bradgate, *supra*, note 106, at 145, notes that a "document" of a computer can refer to the disc/computer's memory or the printout.

[229] This is implied in illustration (ba) to s 65, which refers to all other copies such as printouts etc as secondary evidence where they are copies retrieved from the storage device.

[230] See definition of "computer output".

[231] This would be apt to describe for instance visual displays, which are caused by the conversion of electronic digital signals into analog signals for the visual display, which in turn converts the electronic analog signals into visual information by the electrochemical interaction between the electron beam (representing the analog signals) and the chemical phosphors on the screen display. Similarly, laser printouts are produced by an electrochemical process involving the use of microprocessors to control lasers which write or clear electrostatic charges on the drums of laser printers, before toner powder is spread on the drum and chemically fused with the paper.

information, before such information is transcribed into the computer, the digital record is actually secondary evidence by section 65(c) as a copy made from the original.

Where the computer is used as a data processing device, the results are often stored in the computer's memory repository (which may be temporary memory or permanent memory) before it is generated in the form of output. Technically, the output is secondary evidence, since the primary document in question is the stored information in the memory of the computer, and the output is produced from the original copy in the computer's memory by electronic or electrochemical means.[232]

And again, where the computer output is tendered as direct evidence, the output is actually reconstituted from the digital signals which constitute the transaction in question. The signals themselves, being transient, are usually captured in permanent form in various storage devices. As reconstituted information by way of electronic and electromagnetic processes,[233] the output must be secondary evidence for the same reasons.

As demonstrated above, the distinction between an original document and a copy is highly illusory for computer output. Illustration (ba) to section 65, which is inserted pursuant to the Evidence (Amendment) Act 1996, attempts to cut through all these complexities: it states that where the output satisfies section 35, it is secondary evidence. The effect of illustration (ba) is to reverse the ruling of Chan Sek Keong J in *Aw Kew Lim* v *PP*[234] that a computer printout made from a digital database is an original document and if tendered, will be primary evidence.

If these amendments to section 65 are considered alone, it would appear that it is not any easier for the proponent to tender computer output as secondary evidence, since such computer output still has to comply with

[232] S 65(b).
[233] *Ibid*.
[234] [1987] 2 MLJ 601.
[235] If the rules as to secondary evidence are considered in isolation in relation to computer output, the proponent is most likely to succeed in establishing s 67(c), that "the original has been destroyed or lost", since this would be the case with most ephemeral digital records, especially processed output, and s 67(d), that the original, in the form of data storage devices, is "of such a nature as not to be easily movable". It must be pointed out however that s 67(d) is often applied in relation to documents such as inscriptions on tombstones and writings on walls. But it is submitted that a pragmatic view should be taken where it can be shown that the data storage devices are not easily extracted from the computer systems they are connected to and transported to the physical premises of the court, given the fragility of these devices, the need to reconnect these data storage devices to computers for display of their contents and the total inconvenience caused as opposed to the production of a printout generated in-house from these devices.
[236] *Loh Shak Mow* v *PP* [1987] 1 MLJ 362.

the rule in section 66 that documents must be proved by primary evidence unless the proponent can bring himself within the exceptions in sections 67 and 68.[235] This is so especially since the courts often require strict proof by the proponent that the conditions for admitting secondary evidence in sections 67 and 68 have been satisfied.[236] However, it is provided by section 35(10)(b) that any computer output admitted and duly authenticated by section 35 "shall not be inadmissible as evidence of the proof of the contents of the original document merely on the ground that … it is secondary evidence." Illustration (ba) to section 65 in turn states that "a copy of a document in the form of a print-out, or image on a monitor screen, retrieved from a … storage device … is secondary evidence of the document if it is shown that the copy … satisfies the conditions providing for the admissibility of such output." The effect of section 35(10)(b) read with illustration (ba) is that where a printout or image on the monitor is duly authenticated as computer output by section 35, it is irrelevant that it is secondary evidence!

Hence once computer output is admissible by section 35, even if it is secondary evidence by section 65, and it remains admissible, and there is no need to satisfy sections 67 and 68. In other words, computer output authenticated by section 35 is admissible regardless of whether it is primary or secondary evidence. Where computer output is authenticated for accuracy, the dangers associated with admitting secondary evidence such as slight mistakes in reproduction which may make vast differences in meaning, and opportunities for fraud[237] are already resolved in favour of the proponent. The presumption is that it is an accurate reproduction of the contents therein, and so there is no need to establish a satisfactory explanation for the failure to produce the original document, whatever and wherever that may be.

PART IV. CONCLUSION

Computer output as evidence is gradually receiving acceptance in Singapore. With innovative and forward-looking schemes like the Technology Courts and the EFS, our judiciary has provided the legal fraternity with the tools and the incentive to exploit the use of computer output as evidence. However, the use of computer output as evidence should not detract from the interests of justice and fairness in the admission of evidence. This article seeks to demonstrate that the evidential foundations for judicial scrutiny of computer output as evidence have been put in place by our legislature are forward-looking, progressive and fair. This is achieved by an extended concept of

[237] Morgan, *supra*, note 143, at 332.

"authentication" as applied to computer records in sections 35 and 36. The provisions are cumulative, apply to all forms of computer output, and apply regardless of whether the output is used as hearsay evidence or as real evidence. In addition, the requirement of authentication is permitted to supersede the distinction between primary and secondary evidence.

One may criticise the provisions as being unduly technical. For instance, distinctions are made between output as stored records, as processed results and as direct evidence, and between the proper operation of the computer and proper usage of the computer. The discussion above also shows that the provisions also apply to all forms of output from any data processing device, and this includes even word-processed documents. It has been suggested that the issue of the trustworthiness of computer output should be resolved simply as an issue of its authentication.[238] This is in effect the current position in the United States Federal Rules of Evidence. While such an approach has the advantage of flexibility, it appears inevitable that this approach requires detailed prescriptions of the different aspects of authentication. Where these are generic authentication provisions, they will in turn have to be transposed onto the context of computer output to suit the nuances of computer technology.[239] Hence the South Australian provision from which our section 35 has been modelled sets out a series of authentication factors to be considered in relation to computer output.[240]

Given that computer generated output is still relatively novel, there is clearly utility in prescribing detailed rules as to the nature of the authentication required. Of course, there is always the danger that the detailed rules may yield lacuna. It is the thesis of this author that if one applies the conception

[238] Bradgate, *supra*, note 106, at 145.

[239] See, for instance, Bradgate, *ibid*, at 146, where he notes that there are three aspects to authentication of computer output: accuracy of the original recording of information – which may be doubted; the data stored may be altered, either deliberately or negligently, upon authorisation or be unauthorised, or accidentally due to poor storage, system failure, viruses, and other environmental factors; finally lack of clear means for signing documents. The author very pessimistically notes that as foolproof authentication of computer record is rarely possible, there should be no reason for imposing conditions on admissibility.

[240] South Australian Evidence Act Amendment Act 1972 (No 53 of 1972). See, in particular, s 59b(2)(a) to (g). These considerations range are: the correct programming of the computer and its regular usage, systematic preparation of input data, no reasonable cause to suspect any departure from the system or any error in data preparation, no computer malfunction or alterations to the computer mechanism or processes, proper keeping of records by a reasonable person and no improper processes, procedures or inadequate safeguards in computer use.

of authentication as properly understood, sections 35 and 36 can be read with section 9 to ensure that there is adequate authentication of computer output. But as computers gain wider acceptance, and as lawyers and the courts alike become more familiar with electronic output, many of the authentication requirements will become more easily established, and will accordingly take on less significance.[241] Technology is gradually becoming alive to the legal requirements of proof. Implementations such as electronic security, data encryption, electronic identification as well as digital signatures all go a long way towards easing and simplifying the task of authentication. Currently, these implementations are not commonplace, but as businesses and corporations begin to better understand the need for authentication, and as these technical implementations mature and see widespread usage, it may then be time for us to re-examine the model in the Federal Rules of Evidence. By then, however, our provisions will have successfully served their purpose – to focus the attention of the courts, the business community and the information technology industry on the importance of authentication, to point out that it was technology which created the problem of unauthenticated computer output, and to ensure that it will be technology which will assist us in solving the same problem.

DANIEL SENG KIAT BOON*

[241] Whereas computer hardware was notoriously unreliable in the day and age of mainframes and minicomputers, with improvements in technology, computers are today reliable devices for storing information (although one can safely say that computer software has not reached that same level of reliability yet).

* LLB (NUS); BCL (Oxon); Lecturer, Faculty of Law, National University of Singapore. The author wishes to thank Professor Chin Tet Yung and Mr Ho Hock Lai for sharing their views with this author. The author also wishes to thank Senior Assistant Registrar Mr Christopher Tang and Assistant Registrar Miss Mavis Chionh for their assistance in supplying the author with the necessary Practice Directions. The customary epilog, however, must apply, in that all errors and omissions are clearly the author's, and remain the author's.