A CRITICAL STUDY OF THE AUTHENTICATION REQUIREMENTS OF SECTION 2 OF THE COMPUTER EVIDENCE ACT NO.57 OF 1983

by

SIYABULELA XHANTI MAPOMA

submitted in part fulfilment of the requirements for
the degree of

MASTER OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF D P VAN DER MERWE

NOVEMBER 1997

STUDENT NUMBER: 789 - 096 - 6.

A CRITICAL STUDY OF THE AUTHENTICATION REQUIREMENTS OF SECTION 2 OF THE COMPUTER EVIDENCE ACT NO 57 OF 1983.

BY

S.X. MAPOMA.
DEGREE: LLM
SUPERVISOR:PROF D.P. VAN DER MERWE

SUMMARY.
The aim of this dissertation is to show the shortcomings of the Computer Evidence Act No 57 of 1983 , in so far as the requirements of authentication of computer generated documents before their admissibility as evidence in a court of law.

Key Terms.
Authentication ; Authentication requirements;Computer Evidence Act; Computer ; Computer print - out ; affidavit ; Computer evidence ; Admissibility ; Document ; Deponent.

" I declare that: ' A critical study of the authentication requirements of Section 2 of the Computer Evidence Act No 57 of 1983 ' is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

.....
SIYABULELA XHANTI MAPOMA

INDEX

1. DEFINITIONS:

In this paper,the following definitions will be used unless indicated otherwise.

(a) The 'ACT' means the Computer Evidence Act No. 57 of 1983.

(b) The 'Commission Report' means the South African Law Commission Report Working Paper 60 (Project 95),Investigation into the Computer Evidence Act 57 of 1983,1995.

© The 'Civil Proceedings Act' means the Civil Proceedings Act No 25 of 1965.

(d) The 'Criminal Procedure Act ' means the Criminal Procedure Act No 51 of 1977.

(e) 'E D I' means Electronic Data Interchange.

2. INTRODUCTION.

The Act[1] defines a 'computer' to mean any device or apparatus ,whether commonly called a computer or not,which by electronic ,electro- mechanical,mechanical or other means is capable of receiving or absorbing data and instructions supplied to it of processing such data according to mathematical or logical rules and in compliance with such instructions ,and of storing such data before or after such processing ,and of producing information derived from such data as a result of such processing.

The definition shows some lineal descent from antecedent statutes in the United Kingdom and South Australia. In Section 5(6) of the United Kingdom Civil Evidence Act of 1968, a computer is defined as any device for storing and processing information .Section 59 of the South Australian Evidence Act of 1929 defines a computer as a device that is by electronic,electro-mechanical,mechanical or other means capable of recording and processing data according to mathematical and logical rules and of reproducing those data or mathematical or logical sequence of them[2].

Computers nowadays are found in almost all facets if life. Information is stored by

---

1 Section 1(1)(iii) of Act 57 of 1983.

2 A St Q Skeen 1984 SALJ 675 at p 676

or on computers .Banks, businesses large and small use computers in their everyday dealings with customers.Children play computer games at home , some cars have on-board computers , schools have computer classes ,computers played no small role in the 1990 Gulf War,to cite a few examples.

In fact , modern society has become largely dependant on computers one wonders how man has survived for so long without them.

It therefore goes without saying that litigation will to some extent depend on computer- generated evidence.Crime will be also be committed using computers.However , it seems that our law of evidence in regard to computers is still lacking in this regard.

Various countries have laws which govern computer evidence as it relates to various aspects of their laws.We have in South Africa the Computer Evidence Act No 57 of 1983.

This Act was assented to on 4th May 1983.The Afrikaans text was signed by the President and its date of commencement was the 1st October 1983. The Act has subsequently been amended by the Computer Evidence Amendment Act No 59 of 1992.The latter Act was assented to on 4th March 1992,the Afrikaans text was signed by the President and the date of commencement was the 11th March 1992.

The Act is relatively short with only six sections and was enacted to provide for the admissibility in civil proceedings of evidence generated by computers and for matters connected therewith.

The purpose of this paper is to critically study the shortcomings and strong points of the Act in relation to admissibility of computer generated evidence in civil proceedings and to the desirability of its application in criminal proceedings.

The South African Law Commission[3] in its report observed that when one studies the legal provisions and case law relevant to the admissibility of computer evidence in civil and criminal proceedings one inevitably comes to the conclusion that our law is unsatisfactory in this regard.

It appears that the Act , which was designed precisely to regulate b the admissibility of computer voidance in civil proceedings , does not fulfill its objectives.

In practice the Act finds virtually little or no application , the reason being the unattainable requirements which have to be satisfied before a computer print-out is admissible as evidence.

---

3 South African Law Commission,Working Paper 60 (Project 95)- Investigation into the Computer Evidence Act 57 of 1983,1995.

The Commission further observed that it is moreover undesirable for the admissibility of such of such evidence to be left to the interpretation of the existing provisions as the interpretations are not always uniform[4] . I could not agree more.

The problem of the onerous authentication requirements will also be looked into.

The relationship between computer generated evidence and the hearsay rule will be examined.

A brief discussion will be made on comparative law to see how our law compares with laws of other selected countries.

Is there a way in which the Act in its present form can be changed in order to make it adaptable to modern technology regarding computers ?

---

4 South African Law Commission Report,op cit,(Summary p iv) See also Allison Nyssens, " The Law of Evidence: On line with The Computer Age ? Evidence Law (1993) EIPR, p360-365 at p 360.

3. AUTHENTICATION.

Section 3 of the Act provides that

> "In any civil proceedings an authenticated computer print-out shall be admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible".

Section 1 provides that an authenticated computer print.-out means the documentary form in which information is produced by a computer or a copy or reproduction of it , and includes whenever any information needs to be transmitted , translated or interpreted after its production by the computer in order that it may take a documentary form and be intelligible to the court , a transcription , translation or interpretation of it which is calculated to have that effect , which must be accompanied by the authenticating affidavit which relates to it and by such supplementary affidavit or affidavits as may be required by Section 2 in connection with the authenticating affidavit.

The ' authenticating affidavit ' means an affidavit which authenticates a computer pit-out in compliance with Section 2.

For all intents and purposes , a computer print-out is simply a " document"

The Civil Proceedings Act defines a document as including any book , map , plan , drawing or photograph.[5]

Authentication is a condition precedent to admissibility and requires that sufficient evidence be produced to support a finding that the evidence in question is what its proponent claims.

The Act itself does not define a document. This means in actual fact that any map , plan , drawing or photograph which is generated by computer and property authenticated in terms of the Act will be admissible in civil proceedings.

On the other hand , the Criminal Procedure Act[6] defines a document as including " any device by means of which information is recorded or stored ", and further provides that the provisions of Section 33 of the Civil Proceedings Act (No 25 of 1965) shall mutatis mutandis apply with reference to criminal proceedings[7].

In *S v Harper and Another* [8], the court was of the view that the extended definition of ' document ' is clearly not wide enough to cover a computer , at any rate where

---

5 Section 33 Act 25 of 1965.

6 Section 221 Act 51 of 1977.

7 Section 222 Act 51 of 1977.

8 1981 (1) SA 88 (D & CLD) at p 95.

the operations carried out by it are more than the mere storage or recording of information.

I do not agree , for the simple reason that a computer by its nature and design records and stores information.Whatever it does afterwards is a result of such storage or recording of information and any print-out is part of the process involving storage and recording of information.

Both the Civil Proceedings Act and the Criminal Procedure Act do not mention "computer" in their definitions of " document" nor do they stipulate the manner in which any book , map , plan , drawing or photograph may be produced , for the Criminal Procedure Act provides for any "device".

In criminal proceedings therefore , a computer generated document or print-out would be admissible without the authentication required by the Computer Evidence Act.One would have thought that authentication of computer print-outs would be more of a requirement in criminal than civil proceedings for , inter alia , the standard of proof is greater in the former than in the latter and in most cases criminal proceedings usually affect the liberty of individuals.

In my opinion , the best definition of " document" is the one provided for in Section 1 of the Documentary Evidence From Countries In Africa Act No 62 of 1993 , which

provides that " document includes any affidavit , certificate , record , photograph , book ,map, plan , drawing and any documentary recording or transcribed computer print-out produced by any mechanical or electronic device and any device by means of which information is recorded or stored."

This latter Act does not have the same kind of requirements that are required for authentication of a computer print-out as required by Section 2 of the Computer Evidence Act. To my knowledge it has not yet been decided whether a computer print-out emanating from a designated country would have to be authenticated as if it was originating from inside the country.

Some problems may arise if the foreign country documents would have to be authenticated in terms of Section 2 of the Computer Evidence Act . For instance , what would be the position if the foreign country's equivalent to our Computer Evidence Act does not have authentication provisions as we do , or if such country has no computer laws of any kind at all ? Another problem of authentication was highlighted by the South African Law Commission when it submitted that it was impossible to comply with Section 2 (1) (c)and (d) of the Computer Evidence Act.

The substance of the sections is that a computer print-out could be authenticated by means of an affidavit which should:

(c) describe in general terms the nature , extent and source of the data and instructions supplied to the computer and the purpose and effect of the processing of the data by the computer ,and

(d)(I) certify that the computer was correctly and completely supplied with data and instructions appropriate to and sufficient for the purpose for which the information recorded in the computer print-out was produced,

(ii) unaffected in its operation by any malfunctioning , tampering , disturbance , or interruption that could have had an effect on that information or its reliability.

The Commission would appear to have heeded the call by the Johannesburg Bar which submitted that a computer could not perform any tasks on its own , that it needed an operator and a programme in order to process data.Therefore accurate information would depend on the correct entering of data and the correct functioning of the programme as it was supposed to function and that a programme could consist of various modules ,each written by a different programmer, and then integrated with one another.

In most cases , the programme was used together with other commercial programmes of which the programmer of the first programme had no knowledge.

This state of affairs had the result that it was impossible to find a person who could comply with all the requirements listed.The Johannesburg Bar further submitted that although provision is made for a number of persons to be able to supply supplementary affidavits , the problem with this was that in terms of Section 2(5) (b) , the person who made the main affidavit had to examine the information as contained in the supplementary affidavits. It goes without saying that this would be too onerous a duty on any would-be witness.

The Bar had also submitted that complying with the provisions of the authentication requirements was not practical , that the requirements of Section 2 for the affidavits are too comprehensive, and , I should add , are cumbersome.This will inevitably lead to cutting of corners , making of inadequate affidavits by unqualified people,which would defeat the purpose of the Act.

Indeed , it is questionable whether the provisions of Sub - Sections (1) to (5) reflect an appreciation of the complexity of information systems and,in turn , whether they impose on the deponent of the authenticating affidavit a burden that can be realistically discharged.

Although Section 2 may not be peremptory as regards authentication having to be made by an authenticating affidavit , it is certainly peremptory about what has to be done in order to authenticate a print-out by an affidavit

The chances of any one individual's having the totality of the overview to enable him to perform these tasks adequately are remote , particularly in systems of any size and complexity. The knowledge , skills and experience required at each level are too diverse for one individual , and it is suggested that specialists in each area would have to act jointly if a report on the adequacy of the various systems of controls is to be at all authoritative.[9]

It is interesting to note further that the Act differentiates between an authentication affidavit relating to a computer print-out of a public institution and those of a private institution.The Act defines a public institution to mean,"... financial institution as defined in section 1 of the Inspection of Financial Institutions Act...,the Land And Agricultural Bank of South Africa...; any mutual building society as defined ...,or any deposit - taking institution as defined..." Private institutions are not defined.

Sub - section 2(3) provides that the deponent to an authenticating affidavit shall be some person who is qualified to give the testimony it contains by reason of:

(a) " his knowledge and experience of computers and of the particular system by which the computer in question was operated at all relevant times; and

(b) his examination of all relevant records and facts which are to be had concerning the operation of the computer and the data and instructions supplied to it".

---

9 J.T. Steele 1983 SALJ 505 at pp 508-509
See also A.J. Ebden 1985 SALJ 687 at pp688-791

Sub - section (6) provides that Sub -section (3) does not apply to an authenticating affidavit which:

(a) "relates to a computer print-out of a public institution produced in the ordinary and regular course of the public institution's business or activities from data and instructions supplied to the computer in the ordinary and regular course of such business or activities ; and

(b) is deposed to by an official or employee of the public institution who is qualified to and does certify that the computer print-out was so produced."

The need for authentication of computer print-outs is accepted as essential in a court of law. If the individual person who is the deponent to an authenticating affidavit were to be called as a witness as regards to what he had said,he would , of course , be subject to cross examination. In very few instances could he substantiate what he had stated on oath with any degree of confidence , for he could not be expected to have the required degree of thorough knowledge of the various systems and their controls.

The emphasis therefore , in Section 2 (3) (a) on the deponent(s) being qualified by reason of his knowledge and experience of computers and of the particular system by which the computer

in question was operated at all relevant times (whatever that might mean), would seem to be misguided.[10]

The Act does not indicate the kind of qualification required of the public institution official or employee.It seems , however ,considering that Sub-section 3 is not applicable,that the qualification requirement is relaxed when it relates to computer print-outs of a public institution.

From my view this relaxation is unwarranted.Firstly there is no need to differentiate between computer print-outs when it comes to their admissibility as evidence.

Secondly,public institutions affect and control our lives as much as private institutions do.In fact, public institutions have more control over our lives.After all,we don't choose to be governed and administered upon by certain government departments,we are born into it and have no choice in the matter.One need only think of the mass of information contained in the Department of Home Affairs' computers. At the touch of a burton one can be a citizen of the country or be a foreign national.At the touch of a burton one can be officially dead ,unmarried etc.

---

[10] J.T. Steele,op cit,at p 509.

These are matters of status and it seems to be desirable that any computer print-out which relates to such things would have to be authenticated by properly qualified persons when admissibility as evidence becomes an issue.

In my opinion, Sub-section 2 (3) should also be applicable to authentication of computer of computer print-outs of public institutions.

Anther shortcoming of authentication of computer print -outs in terms of Section 2 of the Act is realised when one considers its application in Electronic Data Interchange (EDI). EDI is the computer to computer exchange of business information in a standard format. It is paperless communication . It's most celebrated application is between two independent firms or trading partners.

EDI replaces the physical interchange of routine purchase orders , transportation orders, acknowledgements , invoices and cheque stubs. This creates problems in the law of evidence in connection with the increasing use of EDI, in that the vast majority of business transactions transactions take place without paper . A machine " talks" directly to another machine. Business is done and information is stored , mostly without human intervention .

The Act does not provide for such transactions. However , where information is recorded by means of mechanical means without the intervention of a human mind, the

record made by the machine is admissible in evidence provided , of course , it is accepted that the machine is reliable.[11]

In England , in cases where the computer merely functions as an automatic recording device or calculating machine , the print-out is treated as real evidence rather than documentary evidence.It is handled in the same way as a tape recording , film , video cassette or radar tracking.There must necessarily be corroborative evidence to prove reliability and relevance.[12]

Without legislation in respect of EDI computer generated print -outs , it certainly would be a heavy and onerous task for authentication of print-outs from the computers involved in the print-outs.

It has been said that ,whereas it seems appropriate for the physical computer print-out to be identified by means of an affidavit , it certainly seems inappropriate for the accuracy and reliability of its contents to be authenticated by this means , and that the preferable solution ,it is suggested , is for the physical identification , on the one hand, and the accuracy and reliability on the other hand , to be treated separately.[13]

---

11 T.C.Smith"The admissibility of Statements by Computer",Crim .L.R. (1981) p 387 - 391,at p 390.

12 South African Law Commission,op cit,at p 16-17.

13 J.T.Steele ,op cit,at p 510.

At this stage it is apparent that our law is still lacking as far as authentication of computer generated print-outs is concerned in relation to their admissibility as evidence.

4. IS COMPUTER EVIDENCE HEARSAY ?

The question might be asked whether unauthenticated computer print-outs must also in some instances be regarded as evidence which is admissible or must they be rejected outright as hearsay evidence. It might be also asked if authenticated computer print-outs are hearsay evidence or not. In other words , is a computer print-out , properly authenticated, reliable enough to qualify to be an exception to the hearsay rule ?

Is it in the interests of justice to allow authenticated computer print - outs as evidence in court ?

Because computer - generated records are hearsay , they are inadmissible as evidence unless they fall under an exception to the hearsay rule.[14] This is the general view.

Not all evidence is admissible in court .At common law, it is a fundamental rule that hearsay evidence is not admissible to prove the truth of the matter at hand.A statement made outside a court may only be admitted as evidence of the fact that such a statement was made. With limited exceptions , such a statement may

---

[14] Richard M. Long " The Discovery and use of computerised information.An examination of current approaches.Pepperdine Law Review. Vol 13.(405) 1986,at p 15.

not be offered to prove the truth of its contents[15]

A grey area exits in the law of evidence between the exceptions to the hearsay rule and the rules relating to the admissibility of scientific evidence[16]

In many instances the information recorded by the computer will be a statement of fact derived directly or indirectly from a human mind and then the hearsay rule will operate to exclude the evidence unless it can be brought within the terms of an exception to the rule.

Where information is recorded by mechanical means without the intervention of a human mind the record made by the machine is admissible provided, of course,it is accepted that the machine is reliable.

If the operator fed into the machine a series of messages written by himself or other persons which were incorporated in the print-out ,that document would be hearsay evidence if it were tendered to prove f acts recorded in the messages.[17]

---

15 Allison Nyssens,op cit ,at p 360.

16 A St Q. Skeen,1984 SALJ 675 at p 676.

17 J.C. Smith, "The Admissibility of statements by Computer" Crim.L.R. p 390.

Exceptions to the hearsay rule are based on the view that certain classes of hearsay evidence should be admissible regardless whether the evidence is reliable or not. The fact that a statement may be fair, clear, reliable and personable does not make hearsay evidence admissible.

The business records exception is based upon the premise that records kept and relied on in the normal course of business bear sufficient guarantees of trustworthiness to justify an exception to the hearsay rule.As the form of the records changes from manual to electronic, the inherent guarantees of reliability also change.Various methods of insuring reliability must be examined in light of these changes.The elements of the rule must be applied flexibly and with these considerations in mind.

In some situations, it may be necessary to rely upon the content of the statement itself as evidence of the witness's personal knowledge.In addition to the normal foundational requirements for business records, the admission of computerised records requires that a sufficient foundation of trustworthiness be established.[18]

---

[18] Pepperdine Law Review,op cit ,at pp 14-16

Computer generated evidence may either be real or documentary. If it is hearsay ,the the evidence should be subject to the normal rules governing hearsay evidence.[19]This is because the general principles governing the admissibility of all evidence also governs computer generated evidence.

The basic objection that can be taken to hearsay evidence obtained from a computer is that its veracity is not subject to testing by cross - examination.The answer is that computer generated evidence would be best evidence available and should , in view of the safeguards built into the Act , in the overwhelming majority of cases be accurate .[20]

The common law of hearsay no longer applies in South Africa now that Section 3 of the Law of Evidence Amendment Act No 45 of 1988 has come into operation.[21]

The latter Act provides as follows:

---

19 Allison Nyssens,op cit,at p 360.

20 A St Q .Skeen , op cit, at p 688-689.

21 L.H.Hoffmann & B.T. Zeffert - "The South African Law of Evidence" 4th Edition,Butterworths.p126.This Act came into operation on 3 October 1988.

'3 (1) Subject to the provisions of any other law, hearsay evidence shall not be admitted as evidence at criminal or civil proceedings, unless:

a) ....

b) The person upon whose credibility the probative value of such evidence depends ,himself v testifies at such proceedings;

or

c) The court ,having to :

I) ....

ii) the nature of the evidence,

iii) ....

iv) ....

v) ....

vi) any prejudice to a party which the admission of such evidence might entail, and

vii) ....

is of the opinion that such evidence should be admitted in the interests of justice .

(2) ....

(3) ....

(4) for the purposes of this section -

"Hearsay evidence" means evidence, whether oral or in writing, the probative value of which depends on the credibility of any person other than the person giving such evidence,..."

The Act gives some discretion to the court to admit or not to admit hearsay evidence. The Act further provides that the evidence may either be oral or written. Computer generated documents by virtue of their being in writing fall to be administered by this Act.

This Act should be read with Section 34 of the Civil Proceedings Act. Section 34 of the Civil Proceedings Act (which in terms of Section 222 of the Criminal Procedure Act applies mutatis mutandis, to criminal proceedings) creates a useful statutory exception to the hearsay rule as regards certain documentary evidence. The drafters of the legislation envisaged, however, that the makers of such documents would be natural persons who would be called as witnesses unless they were for various reasons unavailable or undue delay or expense would be caused[22].

Because our hearsay rules are now controlled by statute, it is my submission that,

---

[22] A.J. Ebden 1983 SALJ 545.

despite the problems of authentication , a properly authenticated computer print-out should be admissible as real n evidence.Presiding officers should exercise the discretion they have to call any oral evidence where it is apparent that the deponent of the authenticating affidavit is not well versed with the particular function of the computer about which he is testifying. Courts should lean in favour of presuming computer print - outs accurate and admissible rather than not.

5. THE BEST EVIDENCE RULE.

A document is an original if according to the substantive law and the issues raised in the trial, it is the document of which the contents have to be proved.[23]Therefore, no evidence is ordinarily admissible to prove the contents of a document except the original document itself.

The best evidence rule applies only when the contents of a document is directly in issue, and has no application where a document's contents serve merely to prove a fact a fact that is capable of being proved by means other than the document, thus a party is required to produce the original document only if he seeks to prove its contents.[24]

The best evidence rule has the effect that any party on whom it is incumbent to prove any act, matter or thing shall be bound to give the best evidence of which, from its nature, such fact, matter or thing is capable.[25]

Quite apart from the questions of hearsay and the rule relating to original

---

23 Hoffmann & Zeffertt," The South African Law of Evidence",op cit, at p 392.

24 Hoffmann & Zeffertt ,op cit, at p 392.

25 May, South African Cases and Statutes On Evidence,Fourth Ed,Juta Par 114,p67.

documents , the value of the best evidence rule is that it makes for certainty and reliability.[26]The rule has its primary application in proving the contents of documents.

It has been stated that ,although the application of the best evidence rule to computerised information presents some conceptual problems , the rule should not , however , provide a major obstacle to the admission of computerised evidence.

The " original" of a computer generated record is arguably the electronic pattern found in the computer's memory.A litigant could argue that a print-out represents a translation of this pattern into readable form, thus it is not the original and should be excluded.

However , this argument is weak because it is virtually impossible to understand computerised information without a print-out , unless one reads the screen of the computer , which for purposes of the law of evidence ,is not a document.

A litigant might also argue that where information in a computer has been input from paper records, these records themselves constitute the best evidence and should be produced.

In the U S A , THE Federal Rules take the position that the electronic pattern in a

---

[26] May,op cit,par 115 ,p 67.

computer's memory constitutes a "writing" and therefore defines a print-out as an "original" and the common law allows secondary evidence where the originals cannot be obtained, such as where paper records are destroyed in the normal course of business.

Where the computer record is merely corroborative , the best evidence is not involved ,and the transaction can be proven by other means.Where the evidence is based solely on the print-out, the print -out must be produced unless its absence can be adequately explained.[27]This seems to be the better view.Even though the scribbler's quill pens in original books have been replaced by magnetic tape, microfiche film and computer print-outs, the theory behind records remains the same and computer generated evidence is no less reliable than original entry books ,provided a proper foundation is laid[28]

Some evidence which is electronic in source , process and result with no human intervention in the process may be considered real evidence ,and presumed reliable.However ,it should not be forgotten that the mere processing of material through a computer adds nothing to its reliability and that in cases where the computer is simply observing facts ,collating information, etc,legislation is desirable because it specifies conditions for admissibility to ensure the reliability

---

27 Pepperdine Law Review- Computer Law [Vol .13:405,1986],pp 17-18.

28 McCormick On Evidence.3rd Ed.Edward C.Cleary(General Editor) at p 85.

of the information supplied.

It has also been observed that the tendency of modern courts is to interpret the best evidence rule in as benevolent a manner as possible[29]It seems that the best evidence rule ought not to be insisted on where the evidence is not challenged;it should,where the court is of the opinion that better evidence could , without any great practical difficulty , be produced and the court feels it is not safe in accepting lesser evidence.[30]

The courts should be given a wide discretion on the matter.If the computer print-out is not of great probative value , and the court is of the opinion that the print-out should be admissible,the print-out should be ruled as the admissible original without authentication.There must be some relaxation of the law on computer print -out admissibility.If the court sees no prejudice to the other party, no objection is made and on weighing the probative value thereof , the print-out should be admissible as the best evidence.

---

29 May , op cit,par 119,p 69.

30 May ,op cit,par 120,p 70.

6. CONCLUSION.

There is nothing inherently unreliable about information stored electronically in a computer's memory for a period of time before a print-out is made. The amount of time between input and print-out could possibly have a bearing on reliability; a longer period may increase the possibility of errors or tampering. However, the duration of time passage alone should not prevent computer records from being admitted.[31]

Colin Tapper had this to say about the provisions of Section 5 of the Civil Evidence Act of 1968, which relates to the admissibility of a document produced by a computer:"...they have attracted some criticism, mainly on account of their needless complexity and their failure to cater for the single most common cause for the inaccuracy of computer output, namely inaccurate input."[32]

The same cannot be said about our own Act and its provisions ,for it provides that

"A computer print-out may be authenticated ... by means of an affidavit which shall

---

[31] Pepperdine Law Review.Vol 13[405] 1986 at p 15.

[32] As quoted in the South African Law Commission Report,op cit,p 18.

(a) ...

(b) ...

(c) ...

(d) certify that the computer was

(I) correctly and completely supplied with data and instructions appropriate to and sufficient for the purpose for which the information recorded in the computer was produced;

(e) certify that no reason exists to doubt or suspect the truth or reliability of any information recorded in or result reflected by the computer print-out."

The Act further provides that it shall suffice that the certifications required by paragraphs (d) and (e) have been given to the best of the knowledge and belief of the deponent to the authenticating affidavit.

Though this may be difficult and sometimes impractical, at least the Act attempts

to cater for the authentication of input.This may not always be practical , as the input may be impossible to verify.The information from which the input is derived may be lost, destroyed or unavailable;the person who fed information into the computer may be untraceable , may be dead or may be available but unable to remember what happened. Would the deponent then be able to say that to the best of his knowledge no reason exists to doubt the or suspect the truth or reliability of any information recorded in result reflected by the computer print-out ?

Would the deponent , in the absence of the person who put in the information ,rely on his trust of the capabilities of the absentee and hope no mistake or errors were made ?

Computers today are used in schools ,business and in almost every sphere where some form of record has to be kept.The conservative look with which our legislation and therefore our courts view evidence of documents generated by such computers means that our law is generally suspicious of records of documents generated by machines which control , record and store most transactions in the world today.

If one takes into account the extent of the use of computers and related devices in modern society , and in particular the fact that the business world relies to a large scale on information produced by computers and related devices ,then one marvels

that the judicature is almost over - cautious in admitting documents produced by such devices as evidence in legal proceedings . The law could at least be expected not put unnecessary obstacles in the way of the proof of facts contained in documents produced by such devices.It appears that in this regard there is a need for for simplification of the rules of the law of evidence with regard to documentary evidence.[33]

One of the reasons for this conservative approach might be the one stated by Parker[34], that, " technology is concentrated among the young ,and older people control the judiciary and legislative process.The laws are written by those who don't fully understand technology and where it is going.In turn,the technologists don't understand the ethical issues, resent the incursion of constraining penal statutes , and feel that it is an indication of society's distrust ,which certainly is..."

But do we really need the authentication requirements as set out in Section 2 of the Act, which are there for use in civil proceedings only and do not include criminal proceedings ?

Section 2 is also arguably not even sufficient for authentication ,because the deponent to an authenticating affidavit need not have personal knowledge of the

---

[33] South African Law Commission Report, op cit, p 53,Ch 5,par 5.3.

[34] D.B. Parker"Fighting Computer Crime",Scribners ,1983 at p 240.

subject matter of the transaction.It is further not necessary that the deponent was the custodian at the time the record was made, or that the deponent was employed at the time the record is produced or personally involved in the production of the print-out.

The nearest the section goes in this regard is to require " an official or employee of the public institution who is qualified to and does certify that the computer print-out was so produced".[35]

The official or employee must be

(a) of the public institution,and

(b) qualified.

The Act does not state the meaning of "qualified".Therefore a Minister of a Government Department in terms of this section can presumably, and I dare say , wrongly " authenticate" by affidavit a computer print-out even though he knows nothing about computers.

The veil of suspicion with which computer generated evidence is seen in terms of Section 2 (1) - (5) is pierced by Section 2 (6) , making Sections 2 (1) -(5) less meaningful.

---

[35] Section 2 (6)(b) of the Act.

One might argue that the authentication requirements of Sections 2 (1) - (5) are therefore the protection against the admissibility of tampered -with computer evidence.But where is the protection for those affected by computer generated evidence from public institutions when it is so easy to authenticate a print - out in terms of Section 2 (b) ?The different and preferential treatment of public institution computer print - outs is not desirable. Public institutions as well as private institutions' computers do the same thing and their computer print - outs should be treated the same.

Although the Act does not specifically require someone learned in computer workings for authentication purposes, it is obvious that the deponent who authenticate must have some knowledge of computers when one considers that the deponent must inter alia, " describe in general terms the nature ,extent and sources of the data and instructions supplied to the computer, and the purpose and effect of the processing of the data by the computer"[36], and certify that the computer was "unaffected in its operation by any malfunction , interference, disturbance or interruption which might have had a bearing on such information or its reliability".[37]

---

[36] Section 2 (1) © of the Act

[37] Section 2 (1) (d) of the Act.

It is thus my submission that the authentication requirements of Section 2 are too comprehensive and to a large extent difficult to put into practice and should be simplified.The Act should further be amended to make it applicable to both civil and criminal proceedings.After all, criminal proceedings often involve the liberty of individuals and it would be better that if there is any strict application of authentication requirements it should be in criminal proceedings.

The South African Law Commission has also recommended that there was no reason why computer related information should be suspect and that it ought to be made at least prima facie acceptable by means of legislation.[38]This recommendation is sound.

In S v de Villiers,[39] the court also stated that it was necessarily envisaged that because of the development of modern commerce ,and the necessity to store records relating to large sums of money and large numbers of people ,special provision would have to be made ,making evidence admissible that would not be able to be subject to the ordinary rigorous test of examination.

It has been suggested that there are numerous benefits to be derived from the presumption of accuracy of computer data,and that current dependence upon computing systems has

---

38 South African Law Commission Report ,op cit,p 129.

39 1995 (1) SACR 574 (Nm) at 579 a-c.

grown to such a point that laws must progressively acknowledge their roles and capabilities,[40] and that by removing the requirement for evidence as to the working accuracy of a particular device or process, the cost and time involved in litigation will be reduced.Further, the legislation supports the common law position thereby providing greater uniformity in this area of law[41]. I agree.

It is thus my submission that computer generated print-outs should be admissible in the same way as any other documents, and that if the word " document" is given its ordinary grammatical meaning, that would be a step closer to such admissibility, both to civil and criminal proceedings.

The court, in S v de Villiers,[42] said " It seems to me therefore that it is correct to interpret the word 'document' in its ordinary grammatical sense and that once one does so the computer print - outs themselves are admissible in terms of Section 221 (Act 51 of 1977).Once that situation has been achieved ,then it seems to me that the thrust of the attack upon the admissibility of these documents disappears ..."

---

40 Lynda Crowley -Smith " Should Computer data be presumed accurate ? Monash University Law Review (Vol .22,No 1 '96) pp 166-173 at p 172.

41 Lynda Crowley - Smith ,op cit, at p 173.The Legislation referred to is Australian Legislation.

42 Op cit at p 579 c.