

Journal of Information, Law & Technology

Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position

Prof. Murdoch Watney University of Johannesburg South Africa mwatney@uj.ac.za

This is a **refereed article** published on 28 May 2009.

Citation: Watney, M., 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 2009(1) *Journal of Information, Law & Technology (JILT)*, http://go.warwick.ac.uk/jilt/2009_1/watney

Abstract

Criminal courts the world over are on a daily basis faced with the question whether electronic evidence presented in criminal proceedings is admissible in evidence or not. In this discussion, the attention will focus on the rules governing admissibility of electronic evidence within the legal framework of the South African law of evidence. It will be argued that admissibility centers on establishing the type of electronic evidence, namely whether it is documentary or real evidence. Once the type of evidence is established, a two-phased procedure is applied, namely determining the admissibility of the electronic evidence and if admissible, establishing the evidential weight thereof. The South African common and statutory law governs admissibility of electronic law. The Electronic Communications and Transactions Act 25 of 2002 provides specifically for admissibility and evidential weight of electronic evidence. In the discussion, admissibility of electronic evidence is the functional equivalent of traditional evidence. No special rules of evidence govern electronic evidence. The South African law relating to electronic evidence is however, hampered by the lack of procedures governing the collection, storage and presentation of electronic evidence for purposes of criminal proceedings. Only once the latter is addressed, the environment relating to electronic evidence will successfully meet the challenges of the 21st century and fulfill its important role in proving crimes committed within an electronic medium.

Keywords

law of electronic evidence, electronic medium, admissibility, documentary evidence, real evidence, evidential weight.

1. Introduction to electronic evidence

A few years ago the Internet, cyberspace, information and communication technology and criminal conduct in cyberspace were regarded as science fiction, but today these are the realities that face countries in the 21st century. Most societies function within a physical and electronic medium. The electronic medium evolve around the use of information and communication technological devices such as computers, mobile phones, printers, iPods, digital cameras to name but a few.

The electronic medium, similar to the physical medium, creates many opportunities for the commission of crimes, such as phishing, 'identity theft', Internet child pornography and distributed denial of service attacks among many others. When a crime is committed, one of the parties in the subsequent criminal proceedings may wish to rely on information generated, distributed or stored on electronic devices such as spreadsheets, emails, text messages, databases and traffic data. Electronic information is often relevant in proving or disproving a fact or point in question relating to the guilt or innocence of the accused and as such, the information forms part of the totality of evidence before the court. This information constitutes electronic evidence and the rules of the law of evidence are applicable thereto in deciding its

admissibility. Galves and Galves (2007, p.9) states 'Technology can live up to its billing of making life easier and more efficient for all of us, despite how criminals may employ it, if we effectively use electronic evidence to prosecute those criminals and reduce the opportunities for technology to be used against us'. The question immediately arises as to whether the traditional law of evidence, which originates from a physical medium, has developed sufficiently to provide for the question of admissibility of electronically recorded and transmitted information. Although one may easily be seduced into believing that electronic evidence is trustworthy, reliable and easily admissible, challenges inherent to electronic evidence face most criminal courts in the electronic age (Solovy and Byman, 2007, p.1).

2. Sources of South African law of evidence governing electronic evidence

The focus in this discussion will be on admissibility of electronic evidence from a South African legal perspective. For purposes of this discussion, it will be assumed that the evidence was lawfully obtained, as evidence obtained unlawfully will in all probability be inadmissible. In this regard, section 35(5) of the Constitution of South Africa finds application. Section 35(5) states that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence render the trial unfair or will otherwise be detrimental to the administration of justice. The constitutional court stated in *Key v. Attorney-General, Cape Provincial Division* (1996 (6) BCLR 788 (CC)) '(b)ut there will be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted.'

The legal system does not always keep up with the pace of technological development. The South African law of evidence consists of common and statutory law. The need for legislative intervention was highlighted with the decision in *Narlis v. South African Bank of Athens* (1976 (2) SA 573 (A)). In this matter it was held that section 34 of the Civil Proceedings Evidence Act 25 of 1965 did not provide for admissibility issues relating to computer printouts. The section provided for the admissibility under specific circumstances of a statement made by a person in a document, but a computer was not regarded as a person. The Computer Evidence Act 57 of 1983 was thereupon placed on the statute book to regulate the admissibility of computer evidence. This act did not achieve its purpose mainly due to an over-cautious approach in placing a high premium on authenticity and reliability. As a result, a number of requirements had to be met before admissibility could be achieved. The Computer Evidence Act was also only applicable to civil proceedings, leaving criminal proceedings unregulated. Urgent legislative intervention was therefore required.

The statutory relief came in the form of the Electronic Communications and Transactions Act 25 of 2002 (hereafter referred to as the ECT Act) which came into operation on 30 August 2002. It provides for various legal issues and not only for the admissibility of electronic evidence.

Section 15 of the ECT Act provides for the admissibility and evidential weight of a data message as electronic evidence. It is clear from the wording in section 1 that it sets out to facilitate rather than inhibit the admissibility of data messages as electronic evidence. Section 1 defines that a data message means data generated, sent, received or stored by electronic means

and includes (a) voice, where the voice is used in an automated transaction; and (b) a stored record. Data is defined as the electronic representation of information. It is in fact stated that a data message will not offend the best evidence rule on the ground that it is not in its original form. It is submitted that electronically produced data will not be subjected to a special set of admissibility requirements and the ordinary rules of evidence will apply (Schmidt and Rademeyer, 2006, pp.11-4).

3. A synopsis of the law of electronic evidence

As the normal (tradional) rules of evidence will be applicable to the admissibility of data messages, it is necessary to briefly consider the applicable rules of evidence. The means of proof are traditionally classified under three headings namely: witnesses, objects (real evidence) and documents. Technological advances have brought many new devices onto the market, some valuable in providing evidence. The products of these devices are sometimes regarded as real evidence and sometimes as documentary evidence. The current view is that it is real evidence unless it takes the form of paper or other material on which knowledge or thoughts are reproduced. It is the human source of the information that identifies it as documentary evidence. The rules of documentary evidence were especially designed to combat errors or inaccuracy flowing from human involvement in the document (Schmidt and Rademeyer, 2006, p.12-4). In the *S v. Fuhri* (1994(2) SACR 829 (A)) it was decided that the photograph of a vehicle whose driver had committed an traffic offence is real evidence, whereas in the *S v. De Villiers* (1993 (1) SACR 574 (Nm)) the court found that a computer printout containing information, where the information had a human source, is a document.

Although S v. Ndiki ([2007] 2 All SA 185 (Ck)) dealt with the admissibility of computer printouts before the ECT Act, Van Zyl made many relevant remarks pertaining to the admissibility of electronic evidence. The following remark was made by Van Zyl in S v. Ndiki:

'It seems that it is often too readily assumed that, because the computer and the technology it represents is a relatively recent invention and subject to continuous development, the law of evidence is incapable or inadequate to allow for evidence associated with this technology to be admissible in legal proceedings. A preferable point of departure in my view is to rather closely examine the evidence in issue and to determine what kind of evidence it is that one is dealing with and what the requirements for its admissibility are' [53].

Against the background of the *Ndiki*-case, one will have to look at the facts of a particular case and determine what type of evidence the data message represents. Once the type of evidence has been determined, a two-phased procedure will be applicable namely (i) to determine the admissibility of the electronic evidence during a trial-within-a-trial and if the evidence is found to be admissible, (ii) the evidential weight of the evidence has to be determined.

Phase 1: Determining admissibility of a data message as electronic evidence by means of a trial within a trial procedure.

Questions relating to admissibility of electronic evidence must be decided in a 'trial within a trial'. 'A trial within a trial' procedure reflects the South African exclusionary approach to evidence. Hofman (2006, p.1) states 'An exclusionary approach can mean a time-consuming

'trial within a trial' before a court decides whether to admit or exclude the evidence. On the other hand, an exclusionary approach can save time by not requiring a court to look at evidence on which it will not be able to rely.'

3.1 Documentary evidence

3.1.1 What is a document?

According to section 33 of the Civil Proceedings Evidence Act which is made applicable to criminal proceedings by section 222 of the Criminal Procedure Act 51 of 1977 (hereafter referred to as the CPA), the word 'document', apart from its usual meaning includes 'any book, map, plan, drawing or photograph'. Section 221(5) of the CPA states that document includes any device by means of which information is recorded or stored, and section 246 includes under that term 'any book, pamphlet, letter, circular letter, list, record, placard or poster.' Section 247 of the CPA also includes newspapers and periodicals as documents. In *Seccombe v. Attorney-General* (2002 (2) All SA 185 (Ck)) it was thus described: 'The word 'document' is a very wide term and includes everything that contains the written or pictorial proof of something. It does not matter of what material it is made.' A document would thus include electronic information.

The rules governing the presentation and admission of documents differ depending on whether the document in question is a public or private document. There are two reasons why it is important to distinguish between public and private documents:

- a. A public document may be used to prove the truth of its contents, in spite of the hearsay rule. The hearsay rule is however applicable to private documents; and
- b. A public document is proved in a different way than a private document. Identification and proof of authenticity by a witness are not required, but only that the document is made available by the authorised custodian. The document therefore 'proves itself'. Secondary evidence of the contents is also admissible.

3.1.2 Public documents

A public document is a document made by a public officer in the execution of a public duty, which is intended for public use and to which the public has a right of access. Official documents usually require the signature or seal of an official. Sections 18 and 19(3) of the ECT Act allow for the electronic notarisation, certification and sealing of data messages. Section 18 provides as follow:

- '18(1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.
- (2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.
- (3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is

http://go.warwick.ac.uk/jilt/2009_1/watney

certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.'

Section 19(3) reads as follow:

"19(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method of form by which such document may be sealed by electronic means, the requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.'

An advanced electronic signature is defined in section 1 of the ECT Act as an electronic signature which results from a process which has been accredited by the Accreditation Authority in terms of the Act.

3.1.3 Private documents

Most documents are private documents. A private document is a document that is not a public document.

A party who wishes to rely upon statements contained in a document must ordinarily comply with the following four general rules namely:

- (i) the contents of a document may be proved only by production;
- (ii) the original document must be produced;
- (iii) evidence is normally required to satisfy the court of a document's authenticity; and
- (iv) the document may have to be stamped in accordance with the provisions of the Stamp Duties Act (this requirement is not applicable to criminal proceedings).

These rules only deal with the position where a court receives evidence to prove what a document contains. They are not concerned with whether statements of fact in a document can be used to prove that those facts are true (Zeffert, Paizes and St Q Skeen, 2003, p.685). If the probative value of a document is dependent on the credibility of a person other than a person who testifies about it, it will be hearsay and inadmissible unless it can be received under section 3 of the Law of Evidence Amendment Act (see par. 3.1.4 below).

The above-given rules are briefly outlined:

(i) Production

A data message can only be produced as evidence by using an output device such as a computer screen, printer or data projector. Section 17(1) of the ECT Act allows the production in an electronic form subject to the following conditions:

'17(1)(a) Considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.'

Section 17(2) states that the integrity of the information is maintained if the information has remained complete and unaltered except for (a) the addition of any endorsement; or (b) an immaterial change, which arises in the normal course of communication, storage or display.' Hofman (2006, p.7) states correctly that the reliability of a particular output device can be dealt with as part of the process of production, but that questions that need the testimony of a witness should for convenience purposes be dealt with as part of the authentication process.

(ii) Production of the original

Section 17 of the ECT Act allows a person who is required by law to produce a document to do so in the form of a data message provided the data message fulfil the requirements in the section about ensuring the integrity of the document (Hofman, 2006, p.7).

The rules of evidence require that, subject to certain exceptions, the original document must be provided as evidence (Zeffert, Paizes and St Q Skeen, 2003, p.686). Section 14 of the ECT act provides that a data message satisfies the requirements of original form if it meets the conditions in the section. Section 14 provides as follow:

- '14(1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if –
- (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsec (2); and
- (b) that information is capable of being displayed or produced to the person to whom it is to be presented.
- (2) For the purposes of subsec 1(a), the integrity must be assessed –
- (a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
- (b) in the light of the purpose for which the information was generated; and
- (c) having regard to all other relevant circumstances.'

For example, when an electronic file is retrieved, it must be shown that the computer system ensured the integrity of the original because 'digital technology makes it easier to alter the text of documents that have been scanned into a database, thereby increasing the importance of audit procedures designed to ensure the continuing integrity of the records' (as referred to in Solovy and Byman, 2007, p.3).

Section 15(1)(b) provides, however, for an exemption from the requirement of original form if the data message is the best evidence that the person adducing it could reasonably be expected to obtain.

(iii) Authenticity

Section 15(1) provides for the general admissibility of data messages. It is important to note that section 15(1) does not make every data message admissible and the wording of the section indicates that a data message may be inadmissible on grounds contained in other laws (Hofman, 2006, p.6).

The South African law of evidence requires that anyone who wants to use a document as evidence have to satisfy the court that it is authentic, in other words, that the document is what it claims to be. Due to its high degree of volatility, electronic evidence can easily be manipulated, altered or damaged after its creation and therefore authenticity must be proved.

Section 15(4) of the ECT Act provides that a data message made by a person in the ordinary course of business, or a certified copy, printout or extract from such data message 'is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law,..., or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.' The copy, printout or extract is to be certified to be correct by an officer in the service of the person making the data message. Schmidt and Rademeyer (2006) points out that this section creates *prima facie* proof that the contents admitted will be considered proven until rebutted: an evidential burden is therefore placed on the party contesting the facts contained in it. Where a data message does not fall under this provision, it will usually be necessary to call the person who was responsible for the data message to establish its authenticity.

3.1.4 Hearsay

When a data message is used merely to establish the fact that information in it was sent, received or stored the law of evidence does not exclude it. Where a data message is however used to show the truth of its contents, the common law requires that the person responsible for the message should be available to be cross-examined about its contents. If this cannot be done, the data message is hearsay and will be inadmissible as doubt exists regarding the reliability of its content and not about the reliability of the technology used.

Section 3(4) of the Law of Evidence Amendment Act 45 of 1988 defines 'hearsay evidence' as evidence, whether oral or in writing, the probative value of which depends upon the credibility of a person other than the person giving such evidence. It will only be admissible if it qualifies as an exception to the hearsay rule as provided in the Law of Evidence Amendment Act (Hofman, 2006, p.9; Zeffert, Paizes and St Q Skeen, 2003, p.685). Section 3 of the Law of Evidence Amendment Act provides that hearsay evidence will be admissible as evidence in the following circumstances:

Section 3(1)(a) states that if the party against whom the evidence is to be adduced, agrees to the admissibility thereof,

Section 3(1)(b) provides that if the person upon whose credibility the probative value of such evidence depends, himself testifies; and

Section 3(1)(c) states that if the court is of the opinion that such evidence should be admitted in the interest of justice, the court must have regard to the following:

- a. the nature of the proceedings;
- b. the nature of the evidence;
- c. the purpose for which the evidence is tendered;

- d. the probative value of the evidence;
- e. the reason why the evidence is not given by the person on whose credibility the probative value of the evidence depends;
- f. any prejudice to a party which admission of such evidence may entail;
- g. any other factor which should in the opinion of the court be taken into account.

Van Zyl J remarked as follow in S v. Ndiki:

'If a computer print-out contains a statement of which a person has personal knowledge and which is stored in the computer's memory, its use in evidence depends on the credibility of an identifiable person and would therefore constitute hearsay. On the other hand, where the probative value of a statement in the print-out is dependent upon the 'credibility' of the computer itself, section 3 (of the Law of Evidence Amendment Act) will not apply [31].'

3.2 Real evidence

3.2.1 Graphics, audio and video

According to the traditional view, graphics, audio and video are regarded as real evidence. Real evidence differs from documentary evidence in that it is never excluded, it only has to be relevant. Once it is received, its authenticity, accuracy and interpretation may be disputed (Zeffert, Paizes and St Q Skeen, 2003, p.706). Zeffert, Paizes and St Q Skeen (2003, p.703) correctly states that real evidence is seldom of much assistance unless it is supplemented by the testimony of a witness to connect it to the issue.

Hofman (2006, p.16) however argues that graphics, audio and video that are in data message form should be treated in the same way as documents and states:

'This view (that graphics, audio and video are regarded as real evidence) is conceptually simple and appeals to those who dislike excluding any evidence. But it does not take account of the way graphics, audio and video are, to an ever-increasing extent, recorded, stored and distributed in digital form and fall under the definition of a data message. This means that graphics, audio and video now resemble documents more than the knife and bullet that are the traditional examples of real evidence. In data message form, graphics, audio and video are susceptible to error and falsification in the same way as data messages that embody documentary content. They cannot prove themselves to be anything other than the data messages and their evidential value depends on witnesses who can both interpret them and establish their relevance.

So long as South African law follows an exclusionary approach it would seem that graphics, audio and video that are in data message form should be treated in the same way as documents. Zeffert, relying on *Ramgobin*, submits that this is the only satisfactory way to guard against the possibility of deliberate or accidental changes in the data messages. To be admissible graphics, audio and video that are in data message form should be produced, be original in form and be authenticated. If the probative value of their content depends on someone who is not giving evidence the statutory hearsay rule and its exceptions should apply to them" (16) (references excluded).

It appears from case law and academic discussion by authors such as Zeffert, Paizes and St Q Skeen (2003, pp.704-706) that depending on the circumstances graphics, videos and digital photos may be dealt with as documentary evidence. In *S v. Motata* (Johannesburg District Court case number 63/968/07 (unreported)) the accused was charged with *inter alia* driving a

motor vehicle whilst under the influence of liquor. After the accused allegedly crashed into the boundary wall of a residential property that belonged to the complainant, the complainant in the matter made certain audio recordings on his mobile phone and took some photos on the scene of the accident with a digital camera. The audio recordings were later transferred from the mobile phone and stored on the complainant's laptop. At the time of the trial, the original audio recordings were no longer available and the admissibility of the audio recordings came to be decided. The court found that the audio recordings were documentary evidence and ruled it to be admissible.

3.2.2 Other real evidence

Other real evidence would for example be a computer programme utilised for the collection of traffic data. The logical approach to follow would be to ask for what a computer program or traffic data is being used, to establish and to treat the admissibility question accordingly.

For example, a computer program is a form of data message. It has at some stage of its existence a human author and for this reason, it could be treated as a document. On the other hand a computer programme is usually only presented as evidence to show how it works. In this case a computer programme is the functional equivalent of a piece of equipment and should be treated as real evidence (Hofman, 2006, p.17).

Phase 2: Once electronic evidence is admitted, the presiding officer has to decide what evidential weight to attach thereto

3.3 Establishing the evidential weight of electronic evidence

When giving judgement, the court must decide what weight to attach to the evidence when evaluating the totality of the evidence. Guidelines and presumptions assist the presiding officer.

The following guidelines will assist the presiding officer:

Section 15(3) provides for the following guidelines to assess the evidential weight of data messages:

- '15(3) In assessing the evidential weight of a data message, regard must be had to-
- (a) the reliability of the manner in which the data message was generated, stored or communicated;
- (b) the reliability of the manner in which the integrity of the data message was maintained;
- (c) the manner in which its originator was identified; and
- (d) any other relevant factor.'

Hofman (2006, p. 18) suggests that in using these guidelines a court will probably need some expert help to understand technical procedures such as encryption, hashing and backing-up that may be used to secure data messages. Later on courts may begin to take judicial notice thereof.

Section 13(2) of the ECT Act provides that data messages and electronic signatures that do not qualify as advanced electronic signatures carry evidential weight.

The ECT Act creates the following presumptions:

Section 15(4) creates a rebuttable presumption in favour of data messages made in the ordinary course of business (see par. 3.1.3 (iii)).

Section 13 provides for the use of an electronic signature in the place of a standard holographic signature and distinguishes between electronic signatures and advanced electronic signatures. Section 13(4) provides that where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved (see par. 3.1.2).

Section 13(5) provides that if the parties to an electronic transaction do not require a signature, the responsible person's 'expression of intent...is not without legal force and effect merely on the ground that (a) it is in the form of a data message; or (b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent...can be inferred.' If the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an 'advanced electronic signature' in terms of section 13(1) is used. The following important reservations are applicable in respect of section 13, namely that this section does not apply to the Wills Act 7 of 1953, the Alienation of Land Act 68 of 1981 and the Bills of Exchange Act 34 of 1964. As a result, wills, contracts for the alienation of immovable property or for the long-term lease in excess of 20 years of immovable property, as well as bills of exchange, cannot be executed and 'signed' in electronic form.

4. Conclusion

In the *Ndiki*-case, Van Zyl (p.13) states 'Finally, in dealing with computer evidence it must be recognized that computers are not infallible and that the dangers inherent in this type of evidence must be acknowledged and the necessary safeguards put into place.' Cognisant of the dangers inherent to data messages, a data message may qualify as either documentary or real evidence and the rules of evidence applicable to the specific kind of evidence should find application after determination of the kind of evidence at hand.

The suggestion that the admissibility of data messages should be regarded as *sui generis* in the sense that neither the traditional evidentiary rules applicable to documents nor real evidence should govern it, but a hybrid of the evidential rules applicable to documentary and real evidence, is not supported. No special rules of evidence should govern the admissibility of information in electronic format. Hofman (2006, p.4) is correct when he states that differential treatment between information in electronic and written format will either result in discriminating against those transacting electronically or give them an unfair advantage. One should bear in mind that South Africa modeled section 15 on the corresponding article 9 of the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce with Guide to Enactment 1996 (Hofman, 2006, pp.2-5). Many other countries have incorporated the Model Law into their domestic law. Although Hofman (2006, p.4) indicates that the Guide does not list article 9 as one of the articles that embodies a functional equivalent approach, electronic evidence should be treated as the functional

equivalence of paper evidence to prevent so called 'format shopping'. Hofman (2006, p.4) defines 'format shopping' as '...converting hard copy evidence to electronic evidence and destroying the originals or presenting a hard copy version and destroying the electronic version in order to take advantage of differences in the law of evidence that applies to each.'

Hofman (2006, p.30) justifiably makes the following observation: 'What is missing in the South African law of evidence are detailed procedures that the courts have approved as complying with the general law and with the Constitution for collecting evidence, storing it and presenting it in court. Only when these procedures are in place will the South African law of electronic evidence be fully effective.'

References

Books

Schmidt and Rademeyer (2006), Law of Evidence (Durban: Butterworths).

Zeffert, Paizes and St Q Skeen (2003), The South African Law of Evidence (Durban: Butterworths).

Cases and Page Numbers Within Cases

Key v. Attorney-General, Cape Provincial Division 1996 (6) BCLR 788 CC.

Narlis v. South African Bank of Athens 1976 (2) SA 573 (A) at 587.

S v. Fuhri 1994 (2) SACR 829(A) at 835.

S v. De Villiers 1993 (1) SACR 574 (Nm).

Seccombe v. Attorney-General 2002 (2) All SA 185 (Ck).

S v. Ndiki [2007] 2 All SA 185 (Ck) at 31, 53.

Sv. Ramgobin and Others 1986 4 SA 117 (N).

S v. Motata Johannesburg District Court case number 63/968/07 (unreported) at 622.

Links to URLs

Hofman, J (2006), Electronic Evidence in South Africa available at hofman@law.uct.ac.za (last accessed on 8 September 2008)

Solovy, JS and Byman, RL (2007), 'Don't Let Your E-Evidence Get Trashed; Legaltechnology', available at http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1181293533711 (last accessed on 15 September 2008).

Galves, C and Galves, C (2004), 'Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial', American Bar Association Criminal Justice Magazine available at http://www.abanet.org.crimjust/cjmag/19-1/electronic.html (last accessed on 15 September 2008).

Statutes

Civil Proceedings Evidence Act 25 of 1965, ss. 33, 34.

Computer Evidence Act 57 of 1983.

Electronic Communications and Transactions Act 25 of 2002, ss. 1, 13, 14, 15, 17, 18, 19(3).

Criminal Procedure Act 51 of 1977, ss. 221(5), 222, 246, 247.

Stamp Duties Act 77 of 1968.

Law of Evidence Amendment Act 45 of 1988, s.3.