LAW SOCIETY
OF SOUTH AFRICA

COMMENTS TO THE SOUTH AFRICAN LAW REFORM COMMISSION IN RELATION TO ISSUES RAISED IN DISCUSSION PAPER 131: REVIEW OF THE LAW OF EVIDENCE

The Law Society of South Africa (LSSA) has considered Discussion Paper 131: Review of the Law of Evidence, issued by the South African Law Reform Commission (SALRC) and wish to comment as follows:

SALRC ISSUE 1: Should the ECT Act be reviewed on a regular basis to take account of advances in technology?

- **If so, what should such a review entail?**
- **When / how often should such a review take place?**
- **Who should undertake the review?**

There seems to be, by and large, consensus on the need for regular review of the provisions of the ECT Act. The SALRC invites further suggestions on the appropriate technical forum (which must be in a position to facilitate the engagement of multiple stakeholders) for such review.

LSSA COMMENT:

As the issues of existing and emerging information and communications technologies and their applications in our society permeate every nook and cranny of our daily lives, it is suggested that this standing committee (in whatever its form) has broadly the following representation:

- **The South African Law Reform Commission** – to enable an early warning system relating to particular aspects of law which may be identified as requiring revision and review. The standing committee must also be entitled to rely on the existing framework of the South African Law Reform Commission for the purposes of researching and drafting new law or revisions to existing law.
- **Representatives of the Department of Communications** as the custodian of the Electronic Communications and Transactions (ECT) Act and other communications-related legislation.
- **Representatives of the Justice, Police and Security cluster**.
- **Cybercrime representation**. The as yet unpublished (save for a limited number of persons) consultation document on proposed Cybercrimes and Related Matters Bill contemplates the establishment of structures to deal with cybersecurity in South Africa. In this Bill it is contemplated

that a cyber-response committee is established. Its functions will be to coordinate government policy relating to cybersecurity (at this stage an amorphous mass of uncertainty), prioritise areas of intervention and generally coordinate cybersecurity at a central point of contact for cybersecurity matters pertinent to national security. As cyberspace is not confined to national security it is submitted that it will, of necessity, have to deal with the coordination of many of the other issues which will be necessary to establish in order to combat cybercrime.

- **The Law Society of South Africa**. The Law Society of South Africa has already initiated interaction with the deans of law faculties to deal with various issues of legal education. The Attorneys Fidelity Fund (AFF) provided a grant for the incorporation of E- / IT Law into the LLB and Legal Education and Development (L.E.A.D) curricula.

- **The Regulator**, established in terms of the Privacy Act. The issue of privacy is the most burning jurisprudential issue globally as technologies which allow for the processing of vast tracts of information, the development of the Internet of Things and the development of Big Data processing capacity pose new threats to the right of privacy. As this is a constitutional right upon which our democracy is dependent, this should be jealously guarded in South Africa. Among the powers of the Regulator are those of education and consultation. It is submitted that there are enormous synergies between the duties of the Regulator and the requirements of review of law (legislation and secondary law) which relate to information and will be required to be addressed in the 21st century. Further, with regard to consultation, the Regulator is required to receive representations from members of the public relating to the protection of personal information, facilitate cooperation on a national and international basis and act as a mediator between opposing parties relating to the protection of personal information. It is believed that should the review function as contemplated in this recommendation be established, consultation with the Regulator would not only be enormously fruitful, but essential to the proper working of both bodies.

- **ICT and Information Specialists** capable of providing guidance as to developments in ICT and Information Security[1]. Information security is a discipline which is evolving rapidly but that has already established a mature framework within which to approach information security issues. Information security is the foundation upon which the principles in Chapter III of the ECT Act are based. It is also the basis of future cybersecurity initiatives. Therefore it is essential that information security specialists be included in considering how best to address the risks that we face in these revolutionary times.

One of the standing committee's tasks must be to ensure harmonisation of our law with developments in other countries. Information knows no boundaries and this harmonisation will assist in avoiding some of the jurisdictional issues that have inevitably occurred. In this regard, there are areas of the ECT Act, particularly those based on the UNCITRAL Model Law and international developments in this regard, which should only be changed with the greatest of care. That being said, there are vast tracts of the ECT Act, not based on the Model Law, which were ill-conceived at the time of inception, have never been

[1] While it is believed that it is essential that the standing committee has permanent representatives in this regard, it should be expressly enabled to consult with experts in specific areas of technologies as and where this may be necessary.

implemented and should be dealt with by other entities within government rather than the Department of Communications.

Finally, part of the function of the standing committee could be to at least annually (and possibly more often) report to Parliament as an independent arbiter monitoring the ICT landscape. In reporting it should identify areas of potential risk, the measures that may be taken to address the risk and progress and/or failures of government departments and institutions to fulfil their mandates.

SALRC ISSUE 2: Are the provisions in the ECT Act adequate to regulate the admissibility of electronic evidence in criminal and civil proceedings?
Although the ECT Act is largely adequate in facilitating the admissibility of electronic evidence, there is apparent inconsistency between the approach in criminal and civil proceedings arising from the provisions of the CPA and the CPEA. There is support for a less fragmented approach to the admissibility of documentary evidence. The SALRC proposes reform: either through amending and supplementing existing provisions or, as the SALRC recommends, through a proposed repeal of these provisions and the introduction of a single statute to regulate documentary evidence or hearsay and documentary evidence, as set out in Annexure A.

LSSA COMMENT:

For the reasons discussed at length below, the LSSA supports the amendment of existing provisions rather than the repeal of these provisions and the introduction of a new statute to regulate documentary evidence or hearsay and documentary evidence.

In the context of the production of electronic communications and records into evidence, the initial objection by our courts was that all computer evidence constituted hearsay evidence. Notwithstanding the fact that increasingly, and almost exclusively, our society and our commercial world process communications and records electronically, the courts previously interpreted that electronic evidence processed by computers constituted hearsay and therefore had to be excluded. This lead to the untenable situation where a vast majority of important and relevant evidence was not automatically admissible. This is what the ECT Act - our law for already 12 years and under which huge tracts of electronic evidence have been introduced into our courts as evidence without material difficulty - had sought to address.

The interpretation that normal rules of hearsay, governing the exclusion of evidence based on the credibility of another who is not "in court" and capable of being cross-examined, appears from reported cases to have been more than adequately dealt with by our courts to date.

The issue of whether poor programming of computers or failures in operation by administrators of computers or information systems may pervert evidence, is more than adequately dealt with in Section 15(3) of the ECT Act[2], which deals with the reliability of the computer itself and the integrity of evidence produced using computers. It is in this sphere that - due to the general lack of understanding by attorneys, advocates and presiding officers of the principles of information security that inform the reliability and

[2] Particularly if the wording of Section 15(4) is revised as proposed below in the comments on Issue 6.

integrity of data messages (electronic communications and records) and the assessment of the weight of electronic evidence - the difficulties occur.

SALRC ISSUE 3: Should the current definition of "data message" in the Act be revised?

For consistency and clarity, should the ECT Act or other legislation relevant to admissibility of electronic evidence in criminal proceedings include a definition of "electronic', "copy" and "original"? There are two aspects: (a) concern has been expressed about the inclusion of "voice, where the voice is used in an automated transaction" which does not appear in the UNCITRAL Model Law definition of a data message; the SALRC proposes either deleting this from the definition or amending the expression to "voice, where the voice was recorded in electronic form". The second aspect (b) is the question of further clarity on the "original" and "copy" of a document. The SALRC proposes a wide definition of copy; however, given the existing provisions of the ECT Act regarding an "original" and the "best evidence rule', no further reform is proposed at this stage. The SALRC invites feedback on the desirability of abolishing or further clarifying the "best evidence" rule; section 15(1)(b) may still result in the rejection of evidence if it is not in its original form.

LSSA COMMENT:

The term "*data message*" is, itself, confusing. The term is defined in Section 1 of the ECT Act to mean:

"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."

The word "*message*" has an obvious long standing meaning in the English language related to a communication between two or more persons. This ordinary meaning is significantly departed from by the definition of a "data message" in the ECT Act, which includes data records which are never communicated. The LSSA is of the view that, while the substantive meaning of the defined term should remain unchanged (save for the comments below pertaining to "*voice*" records), the term "*data message*" should be replaced by a more sensible phrase. The term "*data record*" is preferred by the LSSA to "*data message*", notwithstanding the use of the phrase "*data message*" in the UNCITRAL Model Law. Records of data communications will fit naturally within the meaning of a data record, as will data records which are not communicated. The departure from the term used in the UNCITRAL Model Law will not serve as a problem to international legal harmonisation in any substantive way, particularly so given the broader reach of the ECT Act compared to the narrower commercial scope of the UNCITRAL Model Law.

It is therefore proposed that the term "*data message*" be substituted by the term "*data record*" wherever it is used in the ECT Act.

The distinction between voice recordings made in the course of an ordinary transaction and voice recordings made in the course of an automated transaction has resulted in a number of anomalies.

It is clear that a voice recording made in an automated process constitutes a data record and it is arguable that a "*voice print*" (where a person speaks their name into a telephonic recording to identify themselves

and to indicate their acceptance of terms and their intention to be bound by those terms) could constitute an "*electronic signature*" of that record given that Section 1 of the ECT Act defines an electronic signature to consist of "*data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature*" (own emphasis).

By contrast, where voice is recorded during a non-automated transaction which nonetheless results in a binding contract, the voice recording does not constitute a data record of the transaction. The basis for this distinction in law is hard to fathom.[3]

The LSSA accordingly endorses the Commission's proposal to amend the definition by either deleting subsection (a) from the definition or amending subsection (a) to include "*voice, where the voice was recorded in electronic form*" although it is noted that, if the revised wording of subsection (a) was introduced, it would mostly be beneficial for the avoidance of doubt, as anything recorded in electronic form would automatically constitute a data record.

SALRC ISSUE 4: In view of technological developments, should the ECT Act be amended to extend its sphere of application to the laws mentioned in Column A of Schedule 1 (ie Wills Act, Alienation of Land Act, Bills of Exchange Act and Stamp Duties Act)? Should the ECT Act include the excluded transactions mentioned in Schedule 2 (i.e. agreements for the alienation of immovable property; agreements for long-term leases; execution, retention and presentation of a will; and execution of a bill of exchange)? Concerns about extending the scope of the application of the ECT Act to the transactions in Schedule 2 revolve around issues of authentication and reliability. The SALRC proposes that an appropriate body (such as the standing committee proposed in terms of Issue 1) consider amendments to the ECT Act, taking into account the views expressed by the national departments that have control over the legislation listed in Schedule 1.

LSSA COMMENT:

Several legal practitioners have expressed concerns to the LSSA that evidence a mistrust of electronic documents generally and electronic signatures in particular. In relation to whether Schedule 1 to the ECT

[3] Note that Section 12 of the ECT Act provides that a requirement in law that a document or information must be *"in writing"* is met if the document or information is: (a) in the form of a data message; and (b) accessible in a manner usable for subsequent reference. It is noted that Section 12 of the ECT Act deals with "requirement[s] in law" and does not set a standard by which other documents are necessarily to be interpreted. Sometimes it is not clear what constitutes a requirement in law. For example, the Payments Association of South Africa (PASA) is the payment system management body recognised by the South African Reserve Bank in terms of the National Payment System Act of 1998. Where consumers provide other persons with authority to debit their bank accounts by means of a once-off or recurring debit order, the banks require the debiting party to be a member of PASA and PASA members are required to adhere to its guidelines and rules regarding the receipt of mandates to debit a bank account. PASA's rules draw a clear distinction between debit order mandates given "*in writing*" and mandates given by "*voice*". When it comes to electronic communications, this distinction is not necessarily mirrored in law. The consequence of the distinction, insofar as PASA is concerned, is that before a debit order can be processed, a "*copy of the signed mandate*" must be provided to the account holder in the case of a *"written"* mandate whereas, in the case of a *"voice"* mandate, the account holder must simply be informed in writing.

Act should be revised so as to accommodate the electronic signing of wills, the LSSA has noted the concerns of family law practitioners that wills are peculiar documents in that, unlike many commercial documents, when a will comes before a Court, the author and signatory (the testator/testatrix) will be deceased or incapacitated and it will be impossible for the author/signatory to give evidence as to the contents of the document or its integrity.

Wills also have a potentially very long 'shelf-life'. In this regard, the LSSA has also noted the reservations of some practitioners regarding the potential for even advanced security methods of signing documents to be exploited in the future. For example, where a document is signed with an advanced electronic signature today, practitioners have questioned whether that technology would still be relatively tamper proof in 30 to 40 years' time (or would a future grandchild with a degree in Computer Science be able to easily decrypt the technology of 2015 and alter the contents of his or her grandparent's electronic will)?

However, by and large, practitioners have also expressed a very strong desire to be able to interact with the Master's Office and Deeds Office electronically with a view to maximising efficiencies in the administration of estates and property transactions.

The LSSA accordingly maintains its previous stance that the currently excluded transactions should ideally be included in the sphere of application of the ECT Act and that greater efforts must be applied at educating members of the profession in the appropriate use of technology in legal practice generally.

Despite taking 10 years between the promulgation of the Act and advanced electronic signatures becoming a reality, they are now a reality. Against this background there appears to be no immediate reason that the current exclusions should not fall away, subject to the reservations indicated below. It is also agreed that, in the event of a standing committee being constituted, one of the issues that it should consider is the repeal of the exclusions in the ECT Act and consequential amendments that may be necessary to the ECT Act or other affected law.

With regard to Wills and the issues of signature, the requirement that the testator or testatrix and the witnesses sign every page and that they are all present at the time of signature, would have to be revised. An advanced electronic signature relates to the full record which will be signed only once and because of the nature of the identification elements of the provisions of advanced electronic signatures (which incorporates positive identification) the necessity for witnesses fall away.

It must be stated that levels of integrity which we seek to protect in a Will can be achieved and significantly exceeded in electronic form and using advanced electronic signatures.

It is also important to recognise that the application of an advanced electronic signature provides the benefit of the presumption contained in Section 13(4) of the Act that the signature has been applied correctly. To some degree this may exclude disputes relating to the signature of Wills which currently come before the courts. Quite possibly this should be welcomed. It also opens the way for the signature of a digital or video recording of a Will. An advanced electronic signature will be as effective in "locking" a digital video/audio recording and ensuring the integrity of the record as it is with a text record. In the case of video or audio digital Wills, while the integrity may be assured, the question of administration of these Wills may also beg some questions that would require amendment at least of the Administration of Estates Act.

Although antenuptial contracts are generally reviewed at a time when persons are still alive and in a position to testify, some reservations have been expressed in relation to electronically executing any documents affecting the legal status of a person.

Practitioners have also raised the question of whether affidavits should be capable of being signed in ink by a deponent (e.g. a client who might not have or need an advanced electronic signature) and then being scanned and signed electronically by a Commissioner of Oaths using an advanced electronic signature. The Committee discussed whether a Commissioner of Oaths could apply his or her electronic signature to a scanned copy of a deponent's affidavit and, at the same time, certify that the electronic copy is a true scanned copy of the signed paper copy. This would be particularly useful in relation to service and filing of court applications electronically.

With regard to Bills of Exchange, it is submitted that one of the reasons that this was excluded is that the legislation governing bills of exchange contemplates bills of exchange in a paper format. The importance of signature in the negotiation of these bills is integral to the use of paper bills of exchange. However, the use of paper bills of exchange is reducing dramatically (considerably fewer cheques are written today than in years gone by) but they still exist and care will need to be taken to ensure that traditional negotiation of these bills of exchange in paper form are not adversely affected.

While traditional bills of exchange may become a dead letter in the future, different electronic transactions are replacing these. It is not clear whether these new electronic instruments fall to be dealt with in terms of the Bills of Exchange Act or whether there is any necessity to govern the emerging electronic products. It does appear that this is definitely not something which needs to be dealt with in terms of the ECT Act save by reference in new legislation incorporating the legal principles relating to electronic communications, as may be deemed necessary.

The Alienation of Land Act does not at first blush appear to present the same constraints as either the Wills Act or the Bills of Exchange Act. There appears to be no practical reason why these agreements cannot be entered into by electronic means and as a matter of fact it appears that often faxed agreements of sale (notoriously insecure from a technology and information point of view) are accepted as valid evidence of sales of land by attorneys.

The warning that needs to be sounded is that in certain instances it may be necessary for these documents to be lodged in a Deeds Office to protect one or other of the parties. There is no logical argument why a printout of an agreement transferring land cannot be dealt with by way of a printout in terms of Section 15(4). Of course there may be arguments as to whether this is a record in the ordinary course of business if the current formulation of Section 15(4) is maintained. It is suggested that, if this exclusion is removed, issues of administration of electronic documents in the Deeds Office would require consideration and the Deeds Registries Act or its Regulations would have to be amended, alternatively Directives provided by way of Chief Registrars Circulars.

SALRC ISSUE 5: Should the distinction between "advanced electronic signature" and "electronic signature" be abolished in the ECT Act? Should physiological features of biometrics (including fingerprint, iris recognition, hand and palm geometry) be included in the ECT Act as a form of assent and electronic identity?

The SALRC recommends that a technical and expert standing committee or body (such as that established as recommended in issue 1) be tasked to consider (as a priority matter) the current regulatory regime that recognises a distinction between electronic signatures and advanced electronic signatures, and in particular to make recommendations in respect of the accreditation of foreign signatures. It is furthermore recommended that such body deliberate on the issue of biometric technology and provide guidance in this regard.

LSSA COMMENT:

Background information

It is respectfully submitted that, when dealing with electronic signatures and the concept of advanced electronic signatures, the drafters of the ECT Act misunderstood the issues, possibly due to misunderstandings related to the underlying technologies which these provisions seek to govern. With the greatest respect to both the author of and commentators on the Discussion Paper, to a large degree this section of the Discussion Paper reflects, perhaps unsurprisingly, the same misunderstanding of the nature of signature as it has developed in our law and the background to the drafting of Section 13. In particular, it is submitted, that there is a misunderstanding of the UNCITRAL Model Law on Electronic Signatures and the European Union Directive on which the ECT Act is based, as well as in relation to the concept of "functional equivalence", on which Chapter III of the ECT Act is based, in the context of signatures.

Regulation No. 910/2014 of the European Parliament and of the Council[4], which was published last year and will take effect on the 1st January 2016, could obviously not have been considered by the drafters of the ECT Act, nor by the drafters of the Discussion Paper. However, the importance of the EU Regulation is that it clearly indicates the misdirection of the drafters of the ECT Act relating to electronic signatures. It also provides a clear framework for the recommendations that are provided below as to a practical approach that is in harmony with global developments on electronic signatures, digital signatures (which incorporate the concepts of "reliable", "secure" or "advanced electronic signatures" as they are termed in other jurisdictions) and form a regime governing the use of what we have come to understand as advanced electronic signatures, but which should have been referred to as qualified electronic signatures by the drafters of the ECT Act.

For the sake of convenience, some important issues relating to electronic signatures and advanced electronic signatures have been highlighted in the comment provided below.

The function of signatures

Signatures are of critical importance to the commercial practices that we have developed over thousands of years. The primary functions of signatures are to identify the signatory and to indicate that the signatory intended the signature to be his or her signature in a particular context. (In some cases a signature may be intended merely as an autograph, in others the signature may be affixed but not intended to sign a particular writing. An example of this is where we witness the signature of a person signing a particular

[4] Regulation EU No. 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

document. The signature of the witnesses is not intended as a signature of the document but merely as a risk management mechanism to provide assurances that the signatory is the person that they purport to be. In other circumstances, we may affix a signature merely to acknowledge receipt of a document or other artefact without any intent to sign the document as such and acknowledge that any legal consequences may flow from our signature.) The third function is to confirm the adoption of writing or text to which the signature may be associated.

Aside from these primary functions there may be certain secondary functions that include the validation of forms of administrative action (sometimes ceremonial by nature) and the protection of consumers.

In determining the nature of the signature that may be required to perform an intended function, practices have been developed to avoid the risk of failure of these functions. To safeguard against the failure to evidence identity, in some instances witnesses are required by law or simply by virtue of business expediency. An example is where witnesses are required by law, in the presence of both the testator and the other witness, to sign each page of a Will. The reason being that the testator or testatrix will not be available to provide evidence when the Will becomes effective upon their death. The purpose of doing so is on the one hand to provide confirmation of the identity of the testator or testatrix and that their signature on the Will was affixed by them, and secondly to make it more difficult for a forgery or amendments to provisions in the Will to occur.

In certain instances, to ensure that the identity of the signatory (this may not be evidenced by the signature itself) can be easily established, we require that the name of the signatory is printed in legible form in close proximity to the signature (for instance Rule 44 of the Deeds Registries Act). The signatures of Commissioners of Oaths and Notaries Public require similar endorsement and information relating to their office and place of practice. This arises from the importance of the functions of both ceremony and integrity that are associated with the signatures of these officers, their potential legal impact and how documents bearing their signatures may be treated in evidence.

In dealing with the integrity of information in a paper-based document, we often initial each page of a document to avoid the possibility of pages being removed and rule through pages that are not complete. (A required practice in terms of conveyancing and notarial documentation.) This risk management measure is strengthened in the case of Wills, where each page is required by law to be signed by the testator or testatrix and both of the witnesses.

Turning to electronic signatures, it must be recognised that the identical functions are sought to be achieved (or exceeded) by the use of electronic signatures, but because of the way in which the signature is created and associated to the writing to which the signatory intends the signature to be applied, the evidence supporting the functions is, by its nature, completely different.

Electronic signatures, in the vast majority of instances of electronic communications, indicate the identity of the person. Our signatures may not necessarily be identical where an electronic signature is used. This is no different to what we are used to in the case of handwritten signatures, where often relatively unimportant communication may simply be initialled and in others, where the importance and formality requires, we will use a full signature. Of course our law requires nothing more than that we use a “mark” intended to be used as a signature.

It should also be acknowledged that in some cases the identity of the originator of a message is generated (for instance through caller identification on mobile phones) and this may be regarded as an indication of signature. In these instances the signature is not associated to the signatory at all but rather to the device which may be used by the signatory. Thus, it would be necessary to determine whether the signatory intended to use the device to sign an electronic communication.

In all of these instances, unless additional measures are taken to link the signatory to the purported signature, in the absence of other circumstantial evidence (which may not be conclusive if challenged), it may be difficult to prove the link between the purported signatory and the signature. This is more fully dealt with in dealing with digital and advanced electronic signatures later. Of course electronic signatures and communications context may be important and provide circumstantial evidence of the identity of the signatory.

It is evident that the first fundamental difference in form (from an evidentiary perspective) between signatures in manuscript and electronic form, is that manuscript signatures are, without exception, physiologically linked to the signatory. One cannot sign another person's signature; and save for instances of authority or exception allowed in our law, an attempt to sign another's signature may be a forgery.

Our law recognises, in circumstances of persons being illiterate or incapacitated in some way, that a judicial officer may sign on their behalf. In these cases a written endorsement or explanation of the fact that the signature is not of the purported signatory but is being made on behalf of the purported signatory is associated with the signature in writing.

Save where the law permits persons to sign on behalf of another party, in which event typically this would be indicated in writing associated with the signature, the signature always has to come from the hand of the signatory.

Turning to electronic signatures, it must immediately be recognised that there is no physiological link between the electronic pulses which evidence the electronic signature and the person making the signature. Therefore, from an evidential perspective, the forensic tests that may be used to link a manuscript signature to a purported signatory are of no consequence and the tests linking the signatory to an electronic signature have to be established through circumstantial evidence. For the most part the evidence linking the signatory to a signature are records retained electronically on the electronic devices used within the information systems that facilitate electronic communications. These records may not necessarily be displayed with the electronic signature or represented in a printout of the information representing the electronic signature. The link between the signatory and the signature will be established through circumstantial evidence of the processes in place that are designed to provide this assurance.

It is the functions of signature (in the context of what we are discussing, the question of identity) and not the form of signature that is critical. This is highlighted in the recent decision of the Supreme Court of Appeal of South Africa in the matter of Spring Forest Trading 599 CC (appellant) and Wilberry (Pty) Ltd t/a Ecowash (first respondent) and Others which was delivered on 21 November 2014 by Cachalia JA, concurred with by Lewis, Bosielo and Swain JJA and Mocumie AJA.

In this case, questions arose as to the legal efficacy of emails evidencing an agreement between the parties and signed in the way that emails are typically signed. In the one instance, one of the signatures

concluded the email communication by typing “Kind regards, Greg” and the other concluded his response by typing his first name “Nigel”. Neither the content of the emails, nor the signatures associated with the content providing prima facie proof of the identity of the originators of the emails, was disputed. The dispute was whether the signatures used should have been advanced electronic signatures. The court found that in this instance signatures were not required “by law” and accepted the electronic signatures as being perfectly valid signatures.

This is in line with our law of signature (that permits a mark, even if it does not necessarily indicate the identity of the signatory, intended to be used as a signature, to be regarded as a valid signature).

An important statement in the judgment is:

> *“The approach of the courts to signatures has therefore been pragmatic not formalistic. They look to whether the method of signature used fulfils the **function of the signature** – to authenticate the identity of the signatory – rather than to insist on the form of the signature used.”*
>
> *Emphasis added

Electronic signatures

Electronic signatures” as defined in the ECT Act incorporate all signatures which are provided in electronic form. Incorporated within the concept of electronic signatures are digital signatures. Digital signatures include reliable signatures as defined in the UNCITRAL Model Law on Electronic Signatures and the EU Directive. It must be noted at this point that advanced electronic signatures as defined in the EU Directive and in the more recently published EU Regulation are different to advanced electronic signatures as defined in the ECT Act. This arose from an error in conceptualisation of what an advanced electronic signature is by the drafters of the ECT Act. Thus, advanced electronic signatures as described in this diagram are signatures which have received accreditation in terms of the ECT Act and to which the same principles as are now required to qualified electronic signatures, as defined in the EU Regulations, apply. Advanced electronic signatures as defined in the ECT Act and qualified electronic signatures as defined in the EU Regulations must, of necessity and by virtue of the standards that apply to these signatures, be digital signatures. Therefore, as the diagram illustrates, advanced electronic signatures or qualified electronic signatures are a subset of the broader concept of digital signatures.

Electronic signatures, digital signatures (reliable signatures) and advanced electronic signatures

From the perspective of the ECT Act, the first thing that needs to be addressed and understood are the definitions of “electronic signature” and “advanced electronic signature”.

> *“Electronic signature” means data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature.*

This definition reflects the functions that we seek from signatures and the legal recognition that has been given to signatures over centuries. However, the application of the signature (its form), as already indicated, is significantly different.

> *“Advanced electronic signature” means an electronic signature which results from a process which has been accredited by the authority.”*

The "authority" contemplated in this definition (read with Section 37 of the ECT Act) has been established in the Accreditation Regulations. It operates under the control of the Department of Communications.

In this context, an advanced electronic signature falls within the definition of electronic signature, but it is limited to a specific class of electronic signature. The status of an advanced electronic signature is not achieved by virtue of the relative stringency in determining the identity of the signatory or the strength of the integrity which the encryption technologies used achieves, but solely by the act of accreditation.

The criteria which must be met for services or products supporting an advanced electronic signature to be accredited are stipulated in Section 38 of the ECT Act as supplemented by the Accreditation Regulations. These criteria and the provisions of the Regulations provide high thresholds in accordance with international standards that have to be achieved or exceeded before accreditation of the products and services will occur.

It should be noted that the term "digital signatures" incorporates the same concepts as are provided for in 6.3 of the UNCITRAL Model on Electronic Signatures, dealing with when a signature may be regarded as reliable and the definition of advanced electronic signatures in the EU Directive and in the EU Regulation. It is impossible in terms of criteria established in Section 38 of the ECT Act and implemented by the Accreditation Regulations for an advanced electronic signature to be anything other than a digital signature. As is indicated in the diagram, the concept of digital signatures incorporates advanced electronic signatures as defined in the ECT Act.

Misunderstandings of the UNCITRAL Model Law in the drafting of Section 13 of the ECT Act

It is respectfully submitted that the drafters of the ECT Act misinterpreted the meaning of the words "by law" as contained in Section 13(1) of the ECT Act.

The Interpretation Act stipulates:

> *""law" means any law, proclamation, ordinance, act of Parliament or other enactment having the force of law; …"*

Thus "by law" means all statutory law, secondary law, including regulations (for instance municipal by-laws and, it is submitted, even rules of court). Therefore, by providing that an advanced electronic signature must be used where the signature is required by law, the Act makes no distinction between the functions that may need to be addressed or the relative importance of the signature. The result is that, whenever a signature is required in legislation, even if this is by way of indication for a signature to be affixed to a form that must be completed, however innocuous the form may be, an advanced electronic signature must be used.

As a result, the requirement to use "advanced electronic signatures" (incorrectly defined to include the requirements for "qualified certificates" as contemplated in the European Union Directive) apply far more extensively than what it appears the drafters intended. This more extensive interpretation, while not expressly addressed by the learned judges in the Spring Forest case quoted above, is confirmed by the discussion in the judgment, indicating a clear understanding that the learned judges brought to bear on the interpretation of when an advanced electronic signature needed to be used.

This leads to the question "What is an advanced electronic signature?" As it is defined, an advanced electronic signature is dependent, non-negotiably, on its status of accreditation by the Accreditation Authority. Without this accreditation, regardless of how stringent the measures may be to establish the fact of identity of the signatory, or the strength of the encryption used to ensure the integrity of the electronic signature itself and the data with which it is associated, it cannot be an advanced electronic signature.

As previously stated, the Accreditation Authority contemplated in the Act is established in terms of the Accreditation Regulations. The workings of the Accreditation Authority are dealt with in Chapter IV Part 1 of the ECT Act and are not important in this context.

Chapter IV Part 2 deals with accreditation itself. Section 37 empowers the Accreditation Authority to accredit products and services in support of advanced electronic signatures. It is important to note that it is the products and services provided by a certification authority supporting advanced electronic signatures that are accredited and not advanced electronic signatures themselves.

Section 38 establishes the criteria for accreditation. It reads:

*"**Criteria for accreditation***

38. (1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—

(a) is uniquely linked to the user;

(b) is capable of identifying that user;

(c) is created using means that can be maintained under the sole control of that user; and

(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;

(e) is based on the face-to-face identification of the user."

Section 38 follows very closely the wording setting out the criteria for "reliable signatures" in Article 6.3 in the UNCITRAL Model Law on Electronic Signatures.

"Article 6. Compliance with a requirement for a signature …

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable."

The wording of Section 38(1) in the ECT Act also follows almost identically the definition of "advanced electronic signature" in the EU Directive, to be repealed by the EU Regulation effective the 1st January 2016.

"2. "advanced electronic signature" means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;"

What should be noted is that this definition (which is materially identical in concept as the provisions governing reliable signature in the UNCITRAL Model Law on Electronic Signatures) does not require face-to-face identification as required in the criteria which allow accreditation on advanced electronic signature in terms of the ECT Act.

In the initial draft of the ECT Act, tabled before Parliament after public comment had been called for and received, the criteria in Section 38 was in fact identical to the definition of advanced electronic signature in the EU Directive. This is evidenced by the fact that the word "and" as published in the promulgated act is retained after paragraph 38(1)(c) and before 38(1)(d), despite the inclusion of face-to-face identification required in 38(1)(e).

The "face-to-face" identification requirement was possibly adopted as a result of the South African Post Office persuading Parliament that citizens could be positively identified at any of its 3000 post offices. Regrettably, the consequences of this approach have been highly damaging for the advancement of electronic commerce in South Africa. The Accreditation Regulations required to establish the Authentication Authority and rules by which it was to work (the responsibility of the Department of Communications) were inordinately delayed and were eventually published only in 2007. Some 6 years later the Post Office achieved accreditation, after Law Trust Third Party (Pty) Ltd had become the first entity accredited to provide advanced electronic signatures in South Africa a year earlier.

The result of the above is that advanced electronic signatures have only been a practical possibility for 3 years.

By making advanced electronic signatures subject to the accreditation, Parliament effectively followed a process and definition laid out in the EU Directive for a "qualified certificate" where:

"10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II."

In doing so, the drafters adopted the requirements for certification service providers issuing advanced electronic signatures from the Annexes I and Annexes II referred to in the definition of "qualified certificates". These are followed to a large extent in Section 38(2) of the ECT Act in determining the framework criteria for providers of advanced electronic signatures. However, the drafters did not change the wording used in the ECT Act to correlate with what is understood in Europe. They continued to use the definition "advanced electronic signatures", despite taking a further step and dealing with "qualified certificates". This misdirection is clearly indicated in further development of Electronic Signature Law in Europe documented in the EU Regulation. This regulation makes the clear distinction between advanced electronic signatures and qualified electronic signatures. In the case of the former, the EU Regulation now requires that an advanced electronic signature meet the following criteria:

> *"**Article 26***
>
> ***Requirements for advanced electronic signatures***
>
> *An advanced electronic signature shall meet the following requirements:*
>
> *(a) it is uniquely linked to the signatory;*
>
> *(b) it is capable of identifying the signatory;*
>
> *(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and*
>
> *(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable."*

Qualified electronic signature on the other hand is defined as:

> *""qualified electronic signature" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;"*

The qualified certificate is similar in concept to the accreditation principles that are established in the ECT Act.

It is only against this background and with an understanding of the misdirection that the drafters made, that the provisions relating to electronic signatures in the ECT Act can be properly considered and commented on.

Technological neutrality

Another issue that needs to be properly understood is that while the ECT Act, in purpose and sometimes in function, attempts to achieve the goal of technological neutrality, in the case of digital signatures (which as previously stated incorporate advanced electronic signatures) there is only one technology currently known which properly accommodates the criteria which have been established for "reliable signatures" as defined in the UNCITRAL Model Law or "advanced electronic signatures" as defined in the EU Directive. This technology is based on asymmetric encryption, the processes of the application of which in regard to signatures, is defined by the X.509 Standard. These, for the purposes of accreditation in South Africa, are in turn incorporated in the ISO21188 Standard, which is required in terms of the

Accreditation Regulations, to measure technical and organisational standards that have to be met by the providers of products and services necessary for advanced electronic signatures.

It should also be noted that the proposed amendments contained in the Electronic Communications and Transactions Amendment Bill of 2012 are poorly conceived and evidence a lack of understanding of the law of signature as well as the nature of advanced electronic signatures and their legal status. The LSSA submits that these proposed amendments should be abandoned.

By not properly following the basis of law governing reliable electronic signatures in the UNCITRAL Model Law and advanced electronic signatures in the EU Directive, the ECT Act has essentially rendered impossible the recognition of foreign electronic signatures. This illustrates how important it is to ensure that our law is properly harmonised with laws in other jurisdictions.

The EU Regulations provide guidance as to how a structure for recognition of foreign electronic signatures may be achieved. This is based on the concept of qualified electronic signatures (similar in concept to our advanced electronic signatures) receiving recognition within the European Union. It is suggested that, if the law on electronic signatures is revised to be properly aligned with the European approach (which is mirrored in some of the approaches in other jurisdictions) and the powers of the accreditation authority properly extended within an acceptable framework to accept qualified electronic signatures from other jurisdictions, this problem could be resolved. Based on the current wording of the ECT Act, it is submitted that recognition given to any foreign electronic signatures would be misguided and would lead to inequitable use of electronic signatures in the South African context.

Against this background, it is submitted that the comments in paragraphs 4.48 to 4.52 of the Discussion Paper, while possibly of academic interest, are of no practical importance until a revision of the Act to bring it in line with international practices can be effected.

<u>SALRC ISSUE 6:</u> The question of hearsay and admissibility in terms of section 15 of the ECT Act and the interaction of section 15 with other statutory exceptions:

Should section 15 of the ECT Act prescribe that a data message is automatically admissible as evidence in terms of section 15(2) and a court's discretion merely relates to an assessment of evidential weight based on the factors enumerated in section 15(3)?

Should a "data message" constitute hearsay within the meaning of section 3 of the Law of Evidence Amendment Act?

What is the effect of section 15(1) on other statutory exceptions such as section 221 (admissibility of certain trade or business records) and section 222 (application to criminal proceedings of certain provisions of Civil Proceedings Evidence Act) of the Criminal Procedure Act; and Part VI (documentary evidence) of the Civil Proceedings Evidence Act?

In line with the principle of technological neutrality, the SALRC supports the view that hearsay evidence made by a person in an electronic document should be treated in the same way as hearsay evidence in a paper-based document.

On the interaction of the ECT Act with the CPEA, the CPA and the LEAA, the SALRC supports a less fragmented approach to the admissibility of documentary evidence and therefore proposes reform: either through amending and supplementing existing provisions or, preferably, through a proposed repeal of these provisions and the introduction of one statute to regulate hearsay evidence and certain types of documentary evidence.

The SALRC also invites comment on whether its assessment of the provisions for the admissibility of documentary evidence is sufficiently broad in scope, or whether (for example) the SALRC should also consider the provisions relating to official and public documents, foreign documents, affidavits and so on.

Furthermore, the SALRC supports the development of a handbook on obtaining and producing electronic evidence, which would provide clarity to practitioners and judicial officers regarding the legal position and would also offer advice on technical aspects of producing electronic evidence in court.

The SALRC proposes that the Department of Justice should take a leading role in developing such a handbook, and invites feedback in this regard.

LSSA COMMENT:

The LSSA recognises that there is some confusion amongst members of the profession in relation to:

- hearsay as it applies to electronic evidence;
- the authentication of electronic evidence;
- the admissibility of business records in terms of Section 15(4) of the ECT Act;
- the interaction between (and applicability of) the various laws that regulate exceptions to the hearsay rule; and
- obtaining and producing electronic evidence.

The LSSA would welcome the support of Department of Justice in developing a handbook dealing with all of the above. However, the production of a handbook alone will not automatically result in clarity in the minds of practitioners or judicial officers. The LSSA has already produced a number of guidelines over the years, including a Guideline on Information Security, a Guideline on Electronic Signatures for South African Law Firms and a Guideline on the use of Technology in Legal Practice and support for practical training workshops would also be welcomed and encouraged. It would be highly beneficial if immediate guidelines could be produced relating to the gathering of electronic evidence and the forensic imperatives in doing so. This in turn could flow into the further guidelines of how this evidence (against the background of Chapter III of the ECT Act) should be produced and led in criminal proceedings and thereafter the guidelines guiding the interpretation by judicial officers of this evidence, including the detail of the assessment of the weight of evidence. This could create the foundation for the educational imperative which is critical to preparing aspiring lawyers and assisting practising lawyers in dealing with the realities of the 21st century.

Insofar as Section 15 of the ECT Act and the automatic admissibility of evidence is concerned, it should be noted that Section 15(4) of the ECT Act currently provides that:

A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other 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.

[Emphasis added].

The LSSA is concerned that the section may be interpreted to automatically elevate certain data messages to constitute proof of facts in dispute and favours a revision to Section 15(4) that makes it clear that the section is not intended to undermine the ordinary distinction between evidence and proof. In addition, the section is ambiguous in that it is not clear whether all data messages made by a person in the ordinary course of business require certification, or only copies, printouts or extracts from such data messages.

The following alternative formulation of Section 15(4) is suggested:

A data record adduced by a person, or a copy or printout of or an extract from such data record, certified to be correct by that person or by another person duly authorised by the adducer to do so, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible as rebuttable evidence of the information contained in such record, copy, printout or extract.

As will be evident from the further comment provided, it is submitted that the remainder of the evidentiary provisions in Section 15 of the ECT Act are adequate and do not require any material amendment or replacement by other provisions. The granularity that may be desirable should rather be dealt with in secondary law, for instance regulations or rules of court. The UNCITRAL Model Law and Chapter III of the ECT Act provide a robust framework for dealing with electronic communications and records. Chapter III of the ECT Act also allows for the development of supplementary law or rules, thus providing the flexibility so necessary in light of the very rapid changes to the information and communications technologies landscape that determines our societal and commercial interaction.

SALRC ISSUE 7: Should the ECT Act (or other relevant legislation) make a clear distinction between mechanically produced evidence without the intervention of the human mind (akin to real evidence) and mechanically produced evidence with the intervention of the human mind (hearsay)?

The SALRC supports the maintenance of a distinction between automated data messages and data messages "made by a person" and proposes statutory reform (see Annexure A) to guide the production and proof of both types of evidence in court.

In addition, the SALRC supports the development of a handbook on obtaining and producing electronic evidence that will provide clarity, to practitioners and judicial officers, on the legal

position and advice on technical aspects of producing electronic evidence in court to avoid unnecessary confusion.

LSSA COMMENT:

The LSSA thanks the Commission for giving recognition to its previously expressed view that:

> *"[A]ll electronically produced evidence is to a certain extent the product of the intervention of the human mind. For example, the computer printout of a telephone recorded message is the result of the software in the computer system which was in turn created by the human mind … [I]t could be extremely difficult to distinguish in each case what is the result of the intervention of the human mind and what is not. Therefore it is preferable not to make such a distinction."* [5]

The LSSA maintains its position on the above point and notes the Commission's further quotation[6] from the judgment of Gautschi AJ in the Ndlovu case where the learned judge expressed the following view:

Where the probative value of the information in a data message depends upon the credibility of a (natural) person other than the person giving evidence, there is no reason to suppose that section 15 seeks to override the normal rules applying to hearsay evidence. On the other hand, where the probative value of the evidence depends upon the "credibility" of the computer (because information was processed by the computer), section 3 of the Law of Evidence Amendment Act 45 of 1988 will not apply, and there is every reason to suppose that section 15(1), read with sections 15(2) and (3), intend for such "hearsay" to be admitted, and due evidential weight to be given thereto according to an assessment having regard to certain factors.

The standpoint is reiterated that the correct interpretation of Section 15 allows for the distinction between hearsay and real evidence to be easily made.

As has already been stated, the purposes of Section 15(1) and (2) do not intend doing away with the hearsay rule but are rather aimed at ensuring that it is not used (incorrectly, it is submitted) to disqualify the admission of data messages in evidence.

Thus the observation of Gautschi AJ that Section 15 does not override the normal rules applying to hearsay evidence is respectfully agreed with.

Equally correct is the fact that sub-section 15(3) of the Act provides a more than adequate balance in dealing with so called "*real evidence*" in allowing for evidential weight of a data message to be dependent upon "*the reliability of the manner in which the data message is generated, stored or communicated*". Regardless of the categorisation of the evidence as hearsay or real, the integrity of the evidence is dependent upon the reliability of the computer processing the information.

---

[5] LSSA submission, p 15.

[6] At paragraph 4.91 of the Discussion Paper

SALRC ISSUE 8: Is a review of the principle of authentication necessary in view of the nature and characteristics of electronic evidence that raise legitimate concerns about its accuracy and authenticity?

The SALRC supports the clearer articulation of both statutory and non-statutory (in the form of a handbook/manual) guidelines for the authentication (and weight) of documentary evidence, in particular electronic evidence, and in addition proposes that the court be expressly vested with the discretion to exclude unfairly prejudicial evidence.

The SALRC proposes reform: either through amending and supplementing existing provisions or through a proposed repeal of existing provisions and the introduction of a unitary statute containing provisions such as those articulated in clauses 7 and 8 of Annexure A, and invites further comment in this regard.

LSSA COMMENT:

The LSSA reiterates its previously stated position that a review is not necessary at present, and that "*the Court should be allowed to test the aspect of authenticity further*."[7]

To attempt to stipulate specific best practice or international standards would be self-defeating. While information security practices, which are the discipline that will inform the issues of reliability and integrity referred to throughout Chapter III of the ECT Act, is already mature and is manifest in published standards and guidelines, the ever increasing acceleration in the development of technologies and their applications requires constant and ongoing assessment of threats to the reliability of processing of the information and the integrity of the information itself. This means that these best practices and international standards governing approaches to information security are rapidly evolving and cannot be defined in the static framework that the author of the Discussion Paper and commentators appear to seek.

It is accepted globally that international standards and generally accepted practice will play a key role in the interpretation of framework-type legislation. It should also be noted that the trend in legislation is to do just that by creating a framework which is sufficiently robust that it allows for clear interpretation and application within changing contexts and environments over time. In this regard, as an example, the ISO27001 and ISO27002 Standards which address information security have seen a regular evolution from the initial BS1779 to the ISO17799 to the initial ISO27001 and ISO27002 to the revised ISO27001 and ISO27002 Standards within the course of less than 20 years. The ISO27001 and ISO27002 Standards, first published in 2006, have been amended and replaced by the standards published in 2013. This demonstrates that the standards which shape good practice are considerably more agile than legislation and prove to be more effective in promoting the harmonisation of law and practice in different countries.

It should also be noted that the creation of standards is not confined necessarily to a "one size fits all". For instance, while the principles are very similar to general information security principles, information

7 LSSA submission, p. 17.

security standards governing the payment card industry deal with specific issues relating to the payment card industry and are documented in the Payment Card Industry Data Security Standard or PCI:DSS.

Against this background, it is submitted that the achievement of clarity in the understanding of the assessment of the weight of evidence does not lie in legislative reform, but rather in more flexible measures in the form of guidelines underpinned by international standards.

SALRC ISSUE 9: The admissibility of business records.

Should section 15(4) be reviewed to give a restrictive interpretation to the words "in the ordinary course of business"?

Should section 15(4) as applicable in criminal cases be reviewed in view of the current law on reverse onus provisions?

The SALRC is concerned about a possible preference to electronic evidence afforded by section 15(4) and suggests greater alignment with existing statutory provisions facilitating the admissibility of documentary evidence.

The SALRC proposes reform: either through amending and supplementing existing provisions or through a proposed repeal of existing provisions and the introduction of one statute to regulate documentary evidence or hearsay and documentary evidence (see in particular clause 4 of Annexure A).

Further, the SALRC invites submissions on the status of certificates confirming business records as hearsay or otherwise.

LSSA COMMENT:

See the detailed comments in relation to issue 6 above in regard to the amendment of Section 15(4). The proposed amendment would do away with a special statutory dispensation for business records only.

SALRC ISSUE 10: A presumption of regularity.

Should the law of evidence prescribe a presumption of regularity in relation to mechanical devices (involving automated operations such as speedometers and breath-testing devices)?

The SALRC provisionally recommends that the law of evidence should not prescribe a presumption of regularity in relation to mechanical devices but should include, in civil proceedings, a limited presumption (placing an evidential burden on the other party who did not object on notice).

The SALRC further recommends that the question of presumptions receive the attention of a standing committee / working group established in terms of the recommendations of this Discussion Paper.

LSSA COMMENT:

The LSSA draws attention to the judgment in the matter of the Trustees for the time being of the Delsheray Trust and Others (as appellants) and Absa Bank Limited (as respondent). This Judgment was delivered on 9 October 2014 by Blignault and Henney JJ, which Judgment was agreed with by Goliath J. As a Judgment of the full bench of the High Court of South Africa (Western Cape Division), it is submitted that it is persuasive.

Attention is drawn specifically to paragraphs 37 to 43 and paragraphs 49 to 51 of the Judgment which deal with presumption of reliability and the presumption of regularity, respectively. Attention is drawn to the fact that in this matter the judges deal with the common-law as opposed to the provisions of the ECT Act. Nonetheless, the comments of the learned judges are particularly pertinent to the assessment of the weight of evidence in terms of Section 15(3)(a) being the reliability of the manner in which the data message was generated, stored or communicated. In this regard, the judges indicate that generally the presumption of reliability has not been applied in South African law under that name but that the underlying principles of the presumption are established in our law.

The court quotes from the Law Commission of the United Kingdom, in a report entitled "Evidence in Criminal Proceedings: Hearsay and related topics" which formulated the presumption in the following terms:

> *"In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time."*

The court also quoted Steven Mason who, in writing on the issue of presumption of reliability, quoted an Australian case, Barker vs. Fauser (1962):

> *"It is rather a matter of the application of the ordinary principles of circumstantial evidence … circumstantial evidence is something which is largely based on ordinary life experience … it is merely an indication of this principle to our ordinary experience of life which tells us of the general probability of the substantial correctness of watches, weighbridges and other instruments. If they are instruments or machines of a type which we know to be in common use, our experience tells us that this is suggestive of the substantial correctness. Experience also tells us that they are rarely completely accurate, but usually so substantially accurate that people to on using them [sic], and that subject to a certain amount of allowances for some measure of incorrectness, they act upon them."*

What must be guarded against in considering this judgment, is that firstly it was handed down in 1962, before computers were in everyday use and relates to mechanical devices, which are significantly less complex than software that determines the operation of computers. The judgement also fails to take into cognizance the measures which allow an assessment of the reliability of the working of software and electronic evidence generally.

The learned judges in the Delsheray case go on to quote a 2010 article authored by DS de Villiers that in turn quotes an author by the name of Storm:

> *"The integrity of electronic evidence depends on the scientific reliability of the new generation of computers. The different controls, checks and tests in modern computers and software provide greater accuracy and reliability. Electronic evidence is not inadmissible simply because there is a possibility that it might be incorrect. Admissibility depends upon probabilities based on circumstantial evidence, which demonstrates that the evidence is to a certain extent reliable, not that it cannot be refuted. Although no system can ever be totally error free,* ***the use of security measures and certain controls can minimise these errors****, Storm promotes a presumption of reliability under certain circumstances –*
>
> > *'It should be recognised that computer-generated records carry a strong presumption of reliability which only an equally strong showing of a lack of trustworthiness should overcome. The application of the rules of evidence to computer records should incorporate such a presumption.'"*
>
> [Emphasis added].

With respect to De Villiers, his stating that admissibility depends on probabilities based on circumstantial evidence, misstates the law. Further, it is submitted that, in terms of the provisions relating to "original" in Section 14 of the ECT Act, electronic evidence constitutes original evidence if it meets the tests set out in Section 14.

Storm (quoted by De Villiers) in turn promotes the presumption of reliability too highly. The learned judges in the Delsheray Judgment go on to state that, while the presumption of reliability has not been established in our law under that name, it exists by virtue of the doctrine of judicial notice and that these principles are firmly established in our law. The judges quote Corbett JA in the matter of the State vs. Mthimkulu, Corbett refers to Wigmore on Evidence and quotes this authority as follows:

> *"It may be premised that though, on the principle above noted, any process or instrument must be preliminary found to be a trustworthy one, yet, if the appropriate science or art has advanced to a certain degree of general recognition, trustworthiness may be judicially noticed as too notorious to need evidence."*

Corbett goes on to say:

> "*The extent to which the court will insist upon, or relax, the standards of proof which theoretically apply when evidence involving the use of scientific instruments is presented to it will very much depend upon (a) the nature of the process and the instrument involved in the particular case, (b) the extent, if any, to which the evidence is challenged, and (c) the nature of the enquiry and the facta probanda in the case. No hard and fast rule can, or should, be laid down. Much will depend on the facts and circumstances of each individual matter."*

It is submitted that considering the complexity of computers and at this stage the relevant ignorance of most lawyers and jurists as to the workings of a computer, the wisdom of Corbett JA (even though the matter was decided in 1974) resonates today.

Judicial notice is to a large degree subjective and may vary from judge to judge. However, one of the overriding issues that needs to be considered in the interests of the administration of justice is that, when evidence is not challenged and there are no clear reasons to doubt the evidence which is put before the court, judicial officers should presume reliability.

The learned judges go on to examine further case law in South Africa and it is interesting to note that, in discussing the admission of photographs produced by a machine "the information contained in such photographs, which included the digital time report" in a decision made as long ago as 1994, this was admitted. It is not clear what the nature of the photographs are, whether analogue or digital, but what is clear is that the digital time report is electronic evidence. To the extent that reliance may have been placed on this by the court, it was admitting electronic evidence.

In its consideration of the facts, the learned judges referred to an extract from Ex Parte Rosch [1998] 1 or SA 319[W]:

> *"As was made clear that in all cases to which reference has been made the present case and all similar cases to which we deal with the admissibility of evidence obtained by automatic machines relates only to the admissibility of the evidence concerned, not to the weight of such evidence. At best for the party who relies on such evidence it is open to the other party, the appellant in the present case, to lead whatever evidence he wishes in order to rebut such evidence. In our view a court would be failing in its duty if it ignored the realities of modern science and technologies in the production of evidence.*
>
> *In 1997 courts are entitled to accept that computers are ubiquitous in the society in which we live. The process by which these instruments record and print information is no less commonplace than the operation of motor vehicles and cameras. It is not necessary that there should be evidence as to how each computer works as a prerequisite to the admissibility of evidence produced by such computer, if what has been produced has been done so automatically."*

The sentiments expressed in this judgment are trite and should be even more compelling in our world some 18 years after the judgment was delivered. However, sight must not be lost of the fact that there are continuous and rapid developments in technologies and their use. Sometimes these developments are not necessarily matched by the safeguards of the integrity of information which may be processed.

The learned judges in the Delsheray case then go on to base the presumption of reliability on four factors.

The first of these is credence given to a large commercial bank in the assumption that its computer systems are as sophisticated as other financial institutions. With respect, this is not necessarily the appropriate measure. This having been said, the assumption if couched slightly differently is more supportive of a presumption of reliability. If the presumption is based on the fact that large commercial banks have to comply with information security principles based in, for instance, the Basel conditions which govern financial institutions globally, the requirements relating to security as prescribed by the Reserve Bank and banks using the South African Payment System, general information security standards being incorporated in both of the abovementioned instances and security standards which may be specifically industry-based like the PCI-DSS Standard, this statement would, it is submitted, hold a lot more water.

The second factor is the employment of appropriate personnel filling the responsibility to ensure operation of the computer system is "proper". Again, these are issues which are based on information security principles and the same presumptions as apply to the first factor would be more appropriate.

The third factor relates to the nature of the evidence itself. In this regard, whether the evidence is challenged or not is a critical determinant. It is however submitted that in uncontested matters the presumption should be that the person providing a certificate in terms of Section 15(4) has not acted fraudulently.

The fourth factor is that in this matter the respondent's computer records with respect to the account in dispute are accessible to the client. This is an important determinant as in the majority of cases (certainly not all), by virtue of modern technologies, customers or clients generally have an insight into the processing of their information, whether it be personal or financial. In fact, legislation such as the Protection of Personal Information Act, the National Credit Act and the Consumer Protection Act are predicated on the principles of transparency. Thus obvious errors would in many cases be evident to clients or customers well in advance of any legal action being taken.

The learned judges go on to deal with the issue of human input as hearsay evidence. They state that the probative value of the operations performed by persons in question depends on their credibility as witnesses. However, they also point to the fact that this may be overcome by reference to Section 3(1)(c) read with Section 3(4) of the Law of Evidence Amendment Act. The judges believe that the exclusion of hearsay in this context is well based in our law and that there is sufficient precedent for the statutory exception of hearsay evidence to be applied. One of the issues which must be borne in mind is that, by the nature of computer evidence, in many cases the input to records is provided from difference sources. This may result in a plethora of witnesses having to be called if the hearsay rule was strictly applied.

The alternative to the application of the statutory exception of hearsay evidence as referred to above is the "presumption of regularity". The court has found that this has been applied in our law (R vs Minors; R vs Harper) before and that there is a significant degree of overlap between the "presumption of reliability" and the "presumption of regularity". On that basis the court found in the particular case that the arguments in favour of the application of the presumption of reliability applied equally to the "presumption of regularity".

In conclusion, the court found that computer-generated information, although it may contain evidence which was input by different parties, was sufficient for a person relying on the accuracy of the records to depose to an affidavit, verifying the information in the records relied upon and enforcing a claim (this matter related to an application for summary judgment and therefore reliance was placed on an affidavit).

With regard to Section 15(4) and comments previously made relating to the additional overhead of affidavits as opposed to certificates, it is submitted that the provision of a certificate where a matter is uncontested will achieve the same function as an affidavit. Indeed, in this particular instance an affidavit is required in terms of the rules of court as the application was for summary judgment. The same requirement is not necessary in applications for default judgment.

SALRC ISSUE 11: In general, are the provisions in the ECT Act sufficient to regulate the admissibility of computer generated evidence?

The SALRC recommends that the Rules Board for Courts of Law (the Rules Board), perhaps assisted by a standing committee/working group with technical expertise be requested to consider amendments to the rules of court to provide for the discovery and inspection of electronic documents.

The SALRC notes also that the Rules of Court may require amendment in the event of statutory reform that requires notice prior to trial to be given in respect of an intention to rely on hearsay or documentary evidence, as well as notice of any objections to the use thereof to enable parties to prepare for trial.

LSSA COMMENT:

The LSSA is of the view that the ECT Act is sufficient to regulate the admissibility of computer generated evidence. However, the LSSA also supports the recommendation that the Rules Board consider amendments to the rules of court to provide for the discovery and inspection of electronic documents and submits that such revisions would greatly promote the administration of justice.

It is clear that the admissibility and evidential weight of disputed data message (including ordinary emails, attached electronic files and electronically stored records) depend on an "integrity" assessment.

It is also clear that the "integrity" of a disputed electronic document cannot be properly assessed from a paper printout of that electronic document, but only from an electronic copy of the document containing file metadata, i.e. information contained in the electronic copy that typically evidences when, and by whom, an electronic document was originally created, whether it was revised or edited, to whom it may have been sent and when it was received.

Accordingly, should the admissibility or evidential weight of a paper printout of an electronic document be challenged in contentious litigation, it results in significant wasted costs and delays that could otherwise have been avoided had electronic copies of those documents been produced.

Internationally, civil procedure rules have been amended to address these issues by catering for the proper discovery and production of electronic documents before trial. For example, in the United Kingdom, the importance of electronic file metadata was recognized by an amendment to the civil procedure rules relating to discovery in October 2005 which revised the definition of a "document" in the UK's civil procedure rules to now specifically include "additional information stored and associated with electronic documents known as "metadata".

It is submitted that the issues and risks highlighted above could be easily be addressed by making two minor insertions to Rules 35(2) and (6) of the High Court Rules (depicted in underlined text below):

Rule 35: Discovery, Inspection and Production of Documents

(1) …

(2) The party required to make discovery shall within twenty days or within the time stated in any order of a judge make discovery of such documents on affidavit as near as may be in accordance with Form 11 of the First Schedule, specifying separately-

(a) *such documents and tape recordings in his possession or that of his agent other than the documents and tape recordings mentioned in paragraph (b)* ***and the electronic format, if any, in which any such documents and tape recordings exist****;*

(3) ….

(4) ….

(5) ….

(6) Any party may at any time by notice as near as may be in accordance with Form 13 of the First Schedule require any party who has made discovery to make available for inspection any documents or tape recordings disclosed in terms of subrules (2) and (3) ***and the electronic format, if any, in which such documents or tape recordings are to be made available****. Such notice shall require the party to whom notice is given to deliver to him within five days a notice as near as may be in accordance with Form 14 of the First Schedule, stating a time within five days from the delivery of such latter notice when documents or tape recordings may be inspected at the office of his attorney or, if he is not represented by an attorney, at some convenient place mentioned in the notice, or in the case of bankers' books or other books of account or books in constant use for the purposes of any trade, business or undertaking, at their usual place of custody. The party receiving such last-named notice shall be entitled at the time therein stated, and for a period of five days thereafter, during normal business hours and on any one or more of such days, to inspect such documents or tape recordings and to take copies or transcriptions thereof. A party's failure to produce any such document or tape recording for inspection shall preclude him from using it at the trial, save where the court on good cause shown allows otherwise.*

It is submitted that Rule 35(6) should retain its existing general discretion for Courts to permit the production and use of documents that were not produced for inspection in terms of the rule "on good cause shown".

If the rules were amended as proposed above (along with similar amendments to the relevant provisions of the Magistrate's Court Rules) then good cause for permitting paper copies of electronic documents to be used at trial may exist where a party making discovery notified his or her opponent of the electronic formats in which those documents existed and his or her opponent did not specifically request access to those documents in electronic form. By placing one's opponent on notice that certain of the evidence exists in electronic form and providing one's opponent with an opportunity to use the ordinary discovery rules to inspect the evidence should he or she deem it necessary, the discovery rules eliminate any need for all electronic evidence to be mislabelled as hearsay evidence in order to benefit from the potential for prior notice to be given.

If the rules are not amended as above, it will be difficult for a Court, in possession of only a paper copy of, for example, an email, and faced with admissibility challenge in respect of that email (irrespective of whether the challenge is bona fide or deliberately obstructive), to find good cause for allowing the disputed paper version to be used at trial because: (i) the "best evidence" of that email would not have been produced in terms of Section 15(1)(b) of the ECT Act if the original electronic copy could have been produced, (ii) the "integrity" of that email would not easily be capable of passing assessment in terms of Section 15(3) of the ECT Act and (iii) the "original" of that email would not have been made available for

inspection or produced at Court in terms of Rules 35(6) and (10) read in the light of Section 14 of the ECT Act.

If the rules were amended as outlined above, then not only would the rules regarding production of documents be more closely aligned with Sections 14 and 15 of the ECT Act but the process of obtaining copies of electronic documents would also become significantly more cost-efficient for litigants and their legal representatives. In addition, parties would also be in a proper pre-trial position to evaluate evidence and to consequently make informed, time-saving concessions during pre-trial conferences as to which documents may, without any further proof, serve as evidence of what they purport to be in terms of Rule 37(6)(k).

For the reasons outlined above, it is submitted that Rules 35(2) and (6) should be amended as suggested above and further submissions will be made directly to the Rules Board in this regard.

SALRC ADDITIONAL REQUEST FOR COMMENT:

In the absence of consensus on the issue, the SALRC provisionally recommends that the current approach to relevance remain unchanged; and invites submissions in this regard.

LSSA COMMENT:

The concern raised by the Commission in Discussion Paper 113 was that the application of the existing relevance rule enabled relevance to be "*determined by each presiding officer's common sense which is shaped by his or her own personal experience and therefore has the potential to be discriminatory*".

However, if Section 210 of the Criminal Procedure Act 1977 and Section 2 of the Civil Proceedings Evidence Act 1965 (which effectively preclude the admissibility of irrelevant or immaterial evidence which cannot conduce to prove or disprove any pint of fact in issue) were to be replaced by the contemplated definition of "relevant evidence" as being "evidence that, if it were accepted, could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding", then it is difficult to see how a presiding officer would not still be called upon to determine, based upon his or her own common sense and personal experience, whether a particular piece of evidence "could rationally affect the assessment of the probability" of a fact in issue.

Furthermore, if any new definition of "relevant evidence" was introduced using the contemplated phrase "could rationally affect" then, in order to avoid potential civil and criminal sanctions for non-disclosure of anything that "could" be directly or indirectly relevant, including to the assessment of the credibility of a witness, parties may tend to "over-disclose" documents and information. As we move further into the era of "big data", where a vast amount of information is being recorded in electronic form, the risks of "over-disclosure" become magnified. "Over-disclosure" can also be used, and frequently is used, to drive up costs in litigation (the so-called "drown them in data" tactic) and to deliberately conceal prejudicial information within huge troves of other discovered data which an opposing party would find very difficult to review in a cost effective manner. In this regard, it is preferable from an administration of justice perspective that parties conduct their own review of potentially relevant information and then discover that which is relevant, at peril of sanction for failing to discover all that is relevant.

The LSSA therefore supports the view of the Commission that, in light of the lack of consensus on this issue, the current approach to relevance should be left unchanged. It seems to be neither necessary nor reasonably beneficial to further codify the rules relating to relevance at this time. The existing provisions of the Criminal Procedure Act 1977 and Section 2 of the Civil Proceedings Evidence Act 1965, as well as the rules of court that require a party to civil litigation to disclose documents or tape recordings that tend to either prove or disprove any issue in dispute, are deemed to be adequate at present. As the technological landscape regarding access to huge quantities of information will likely evolve at a very steady pace, it is probably better to reserve the ability of our most senior judicial officers to utilise the flexibility of the common law to develop new approaches to determining relevancy as, when and where required, taking into account developments in other common law jurisdictions that are seized by the same shifting technological landscape.

SALRC ADDITIONAL REQUEST FOR COMMENT:

The SALRC provisionally proposes the introduction of a statutory requirement for notice to be given of an intention to produce hearsay evidence or automated electronic evidence (see clause 6 of the proposed Bill in Annexure A.)

The SALRC invites feedback on the need for clarification of the distinction between real and documentary evidence.

LSSA COMMENT:

Before commenting on the distinction between real and documentary evidence, the LSSA submits that it is critically important to maintain a clear distinction between disputed and undisputed proceedings.

In disputed matters it is assumed that any documentary evidence would be subject to discovery in almost all instances. It is assumed that this would include any hearsay or automated evidence in respect of which the SALRC is suggesting notice to be given. It is suggested that, if the recommendation of the SALRC to introduce notice of intention to produce hearsay and automated electronic evidence is adopted, in most contested matters issues of relevance, hearsay and any other factors which may be brought to bear on the evidence produced, are subject to debate and the protections lie with lawyers and judges to ensure that electronic evidence is dealt with in the interests of justice. This seems no different from issues of discovery and the relevance of discovered paper documents or their standing from a hearsay perspective.

However, a very high proportion of matters dealt with by the courts are undefended or undisputed matters (i.e. matters where no plea or answering affidavit placing any issues in dispute has been filed within the required time periods). These include a very high number of applications for default judgment which, in terms of the rules of court, require supporting evidence of the claim to be submitted. The LSSA submits that it would not be in the interests of justice, nor would it promote efficient administration of our courts, to require prior notice to be produced in such matters of any documents that might technically constitute hearsay or automated electronic evidence.

Section 3(1)(c) of the draft bill contained at Annexure A to Discussion Paper 131 permits the court a discretion to admit hearsay evidence without prior notice having been given with regard for “the nature of

the proceedings". This discretion should presumably be judicially exercised rather than administratively by default judgment clerks. The LSSA recommends that, if a prior notice regime is to be introduced into South African law relating to hearsay or automated electronic evidence, then a legislated exception should be created to provide for undisputed applications to be lodged and disposed of without any requirement to give prior notice to all parties of any hearsay or automated electronic evidence intended to be utilised in support of the application.

With regard to the need for clarification of the distinction between real and documentary evidence, the LSSA is concerned that the current wording of Section 15(4) of the ECT Act could permit even weak hearsay or documentary evidence to automatically serve as proof, simply by virtue of the fact that it is contained in a data message.

SALRC ADDITIONAL REQUEST FOR COMMENT:

The SALRC proposes to clarify the status of a printout as a form of electronic evidence, through statutory reform such as the amendment or introduction of definitions along the lines of "copy", "document" and "electronic document" (see clause 1 of the proposed Bill in Annexure A). The SALRC invites submissions in this regard.

LSSA COMMENT:

The LSSA does not agree that it is either necessary or desirable to introduce or amend definitions of "copy", "document" and "electronic document". However, as outlined above, Section 15(4) should be revised:

- to clarify its purpose and remove the confusion between printouts of documents provided in the ordinary course of business and printouts provided for the sake of convenience where these printouts have to be made by virtue of the fact that an electronic record cannot be viewed by the party to whom it is produced; and
- because of the already enormous and increasing reliance on information in electronic form, where printouts are used to be adduced in evidence (which is really the purpose that the drafters presumably had in mind when adding Section 15(4) to the provisions recommended in the UNCITRAL Model Law).

Further, it is submitted that an affidavit is not necessary in these circumstances. The reference to records in the ordinary course of business would fall away in Section 15(4), but of course would apply to the presumptions that our courts and our legislation already attribute to records of this nature. This would allow the functional equivalence principle to be applied consistently to electronic records.

The proposed revision to Section 15(4) above would remove the following perceived objections to its formulation as it currently stands:

- It does not apply only to records made in the ordinary course of business but of course this principle, already a part of our evidence, would continue to apply to electronic records in the same way as it would to paper documents.

- The objection of unconstitutionality raised by Professor Hofman in criminal matters falls away as there is no shift in onus. The onus to prove the integrity of the evidence adduced remains on the person relying on the evidence, if the integrity of the evidence is placed in question.
- Use of the phrase “rebuttable evidence” as opposed to “rebuttable proof” perhaps removes the concerns of Professor Hofman in this regard.
- It allows for the ever increasing number of electronic records that need to be adduced in evidence which are never manifest in a paper form to be placed before court, administrative body or any other proceedings where it may be received in evidence without the overhead of an affidavit.

If there are concerns that certificates in terms of Section 15(4) will be signed which are incorrect and would, if given under an affidavit, substantiate a prosecution of perjury, the form of the certificate could require that the person certifying acknowledges that, if the certificate is inaccurate and misleads the persons who may rely on it, the certifier will be subject to possible criminal prosecution.

Turning to the rules of court, much of this Discussion Paper relates to how evidence would be dealt with in contested matters, but what is not addressed is the far more prevalent uncontested litigation for other administrative purposes for which printouts of electronic records may be used.

By way of example, taking advantage of the enormous efficiencies and cost effectiveness of electronic records as opposed to paper, many organisations do not retain paper any more. If any of these electronic records are required to support an application for default judgment they could, subject to the limitations within the wording of the section and an appropriate certification, avail themselves of the provisions of Section 15(4) to provide the supporting documentation. Against this background, the rules of court should be amended to allow for printouts of electronic records to be used in this manner. From a practical perspective, the function intended by similar supporting documents which may be produced in their original form evidencing signatures in paper and ink, will be met.

It should be noted that the statutory recommendations made by the SALRC and provided in Annexure A to the Discussion Paper reflect how this has been dealt with in certain other jurisdictions. In that context these provisions include requirements relating to notice of intention to produce hearsay evidence and documentary evidence, which, it is submitted, are better dealt with in rules of court. The provisions themselves contemplate in 6.5 that rules of court specify the manner in which the duties imposed in that section are complied with, including the time allowed for such compliance.

The reason that it is preferable that these are dealt with in rules of court is that it provides more flexibility and avoids the necessity of embarking on the very cumbersome process of legislative change where new technologies or applications may demand this. Rules of court dealing with more procedural issues can provide the flexibility that is desirable in this regard.

Turning to the issue of “best evidence” and whether a printout can constitute best evidence, in the paper environment, where originals are available, they are always preferred because they can be subjected to forensic tests should the authenticity or integrity be questioned.

With electronic evidence, strictly the best evidence would be to take to court the computer or information system to display to the presiding officer the electronic evidence that is being led. This of course becomes absurd, particularly if the information system includes extensive parts of the Internet, as so many

information systems do today. Thus, printouts certified to accurately reflect the electronic information which has to be introduced in evidence are used and if they meet the criteria set out in Section 14 of the ECT Act dealing with originals, are regarded as originals and may, in many circumstances, be the "best evidence" that a party can reasonably be expected to produce at court.

With physical artefacts (paper documents) forensic tests are applied to the paper itself. For instance, where a signature has been applied the fibres in the paper may have been changed or torn. Where a forgery may be alleged, checks may be made relating to the ink used and its uniformity in being applied to the paper. Obviously this nature of forensic test cannot be conducted on electronic documents. However, forensic tests relating to the computers producing printouts of electronic records can be made and while changes to the printout of an electronic record may be more difficult to detect than changes to paper and ink records, certain technologies that have built into them forensic checks and balances will prove to be infinitely more secure and accurate in determining the authenticity or integrity of electronic records as opposed to paper and text documents.

SALRC ADDITIONAL REQUEST FOR COMMENT:

Promoting functional equivalence between paper-based and electronic business records (by aligning the various statutory provisions for the admissibility of documents) is a matter which the SALRC provisionally proposes to address through statutory reform and invites submissions in this regard.

LSSA COMMENT:

On the formulations of the statutory revisions proposed by the SALRC, it is far from clear whether these will promote functional equivalence to any greater degree than the ECT Act already does.

The focus of the Discussion Paper is on evidence. Further, the vast majority of the issues that are addressed relate to electronic evidence. While this is obviously an extremely important aspect of our regulating electronic communications and transactions, it is not the sole focus of the ECT Act or the UNCITRAL Model Law. The changes that are proposed by the SALRC, focused as they are solely on evidence, may have significant unintended consequences and create greater confusion than they seek to resolve, unless the whole of Chapter III of the ECT Act undergoes a similar revision.

It is submitted that this is unnecessary and that the most beneficial approach would be one of ensuring that lawyers (whatever their particular role may be relating to evidence) understand the law better and gain an understanding of how electronic evidence is safeguarded.

SALRC ADDITIONAL REQUEST FOR COMMENT:

Ensuring parity in the law relating to the admissibility of documents produced in civil and in criminal proceedings is a matter which the SALRC proposes should be addressed through statutory reform.

LSSA COMMENT:

Subject to the comments above, the LSSA agrees with the sentiment of ensuring consistency in treatment of evidence, whether in criminal or civil proceedings, without impacting on the different standards of proof required by the different systems.

SALRC ADDITIONAL REQUEST FOR COMMENT:

Providing clarity on the definition of "document" and parity between the definition in civil and in criminal proceedings, and parity between paper-based and other forms of documents, are matters which the SALRC proposes to address through statutory reform (see clause 1 of Annexure A).

LSSA COMMENT:

The proposed definitions contained in Annexure A in terms of which:

"Document" shall mean "*anything in which information of any description is recorded, and includes a copy*"; and in terms of which **"Electronic document"** shall mean *"data that are recorded or stored on any medium in or by a computer system or other similar device, and includes a display, printout or other output of that data*";

are not supported by the LSSA as a means of ensuring parity between paper based and other documents in civil and criminal proceedings. In particular, the stretched use of the word "document" will more than likely result in further confusion as the term will technically cover everything from cave writing to hard disk drives to photographs. Rather, the LSSA submits that proper understanding of the provisions of the ECT Act will be promoted by the substitution of the term "data message" with the term "data record" and that the proposed revision to Section 15(4) of the ECT will bring both certainty and substantial parity to the admission of electronic documents in civil, criminal and other proceedings instituted in terms of any law.

SALRC ADDITIONAL REQUEST FOR COMMENT:

Providing clarity on the admissibility of automated electronic documents and the rules for the admissibility of such documents is a matter which the SALRC provisionally proposes should be addressed through statutory reform (see in particular draft clauses 5 and 6, Annexure A).

LSSA COMMENT:

The LSSA submits that care must be taken not to damage or create greater confusion relating to the foundations upon which electronic communications and records should be dealt with in our law. The intended consequences of doing so and rendering our law in this regard out of line with international principles and development, must be avoided.

SALRC ADDITIONAL REQUEST FOR COMMENT:

Providing clarity on the "best evidence" rule in the context of documentary evidence is a matter which the SALRC proposes to address through statutory reform, and invites further comment on the preferred approach in this regard.

LSSA COMMENT:

The LSSA submits that, to the extent that any further clarity on the application of any particular common law rule in different contexts is required, that should ideally be provided by the Courts rather than by means of statutory reform, unless statutory reform is necessary or likely to be beneficial.

It should be remembered that, in dealing with best evidence, a distinction must be made between the admissibility and the weight of the evidence. This distinction is clear at common law in relation to traditional forms of evidence and it is submitted that the distinction is also already clear in relation to electronic documents in the ECT Act in terms of Sections 15(1) and 15(3).

In this regard, the Commission pertinently notes in paragraph 3.49 of the Discussion Paper that *"[e]lectronic evidence arguably requires a shift in emphasis away from the exclusion from admissibility based on hearsay and the best evidence rule, to the question of reliability. For reliability, the concepts of authentication and integrity (dealt with in the section below) become important. This is particularly so given the concern that electronic records may be more susceptible to undetected modification than are traditional paper-based records*."

These comments are wholeheartedly endorsed by the LSSA. It is also submitted that this is exactly what Section 15 of the ECT Act has achieved.

SALRC ADDITIONAL REQUEST FOR COMMENT:

Providing clarity on the method of authenticating documentary evidence, and ensuring reliability, specifically in the context of computer generated evidence is a matter which the SALRC proposes should be addressed through statutory reform (see clause 7 of Annexure A) and invites submissions in this regard.

LSSA COMMENT:

For the reasons stated above, any attempts to revise the law of evidence relating to electronic records needs to be addressed with an abundance of caution.

It is submitted that if there is any consolidation of the law relating to evidence, simply applying different wordings from jurisdictions that have not applied the ECT Act will create unnecessary confusion, particularly as some of the concepts derived from the UNCITRAL Model Law may be the same in intent but not in form as those applied in other jurisdictions.

It is again stressed that the solution to the difficulty of the misunderstanding of the ECT Act and its application to evidence lies in amendment of the definition of a data message and Section 15(4) or

improved education of the provisions of the ECT Act, rather than in statutory reform intended to address perceived deficiencies in the UNCITRAL Model Law or the ECT Act.

SALRC ADDITIONAL REQUEST FOR COMMENT:

Finally, and in light of the issues and questions raised above for consideration, the SALRC invites feedback on the choice of options for reform:

Option 1: Retention of the current regulatory landscape, with possible minor reform

This approach would result in the retention of the current regulatory framework, possibly with the introduction of some minor statutory reform (for example, the substitution of current definitions in the CPA and the CPEA). The advantage of such an approach is that fewer changes would be required – which would be minimally disruptive to the legal profession, and changes would likely be introduced more quickly than if more substantive regulatory reform is undertaken. However, this conservative approach would mean that multiple laws would still apply; the disadvantages of this scenario include the likelihood that confusion would continue to exist around certain laws and principles, including the following: hearsay as it applies to automated electronic evidence (and the seeming hesitance to treat electronic evidence as real evidence); the authentication of electronic evidence; the admissibility of business records in terms of section 15(4) of the ECT Act; and the interaction between, and applicability of, the various laws which regulate exceptions to the hearsay rule.

Option 2: Introduction of Electronic Evidence specific legislation or guidelines

This option would also largely retain the current regulatory framework, with possible minor statutory reform. However, it would introduce additional legislation[8] that would be more detailed than the current section 15 of the ECT Act, specifically to address the admissibility of electronic evidence (with a focus on issues such as authentication and reliability). The content of such legislation may be informed by the provisions of the Draft Model Law on Electronic Evidence,[9] commissioned and published in 2002 by the Commonwealth Secretariat to assist Commonwealth jurisdictions grappling with legislative reform in the context of electronic evidence, and endorsed by the Commonwealth Law Ministers as a Commonwealth model of good practice. The Model Law is attached as Annexure D.

Option 2 would provide greater clarity than Option 1 on the admissibility and production of electronic evidence. Option 2 would not, however, resolve the potential confusion and possible deviation from the functional equivalence approach that results from the multiple sources of law which would still apply to hearsay and documentary evidence.

Option 3: Reform of the current regulatory landscape

8 Or possibly Regulations in terms of the ECT Act.

9 Draft Model Law on Electronic Evidence (2002) available at *http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BE9B3DEBD-1E36-4551-BE75-B941D6931D0F%7D_E-evidence.pdf* (accessed 31 July 2012).

The third option involves a more extensive overhaul of the regulatory framework for hearsay and certain types of documentary evidence. This approach envisages the repeal of existing provisions on the admissibility of hearsay evidence and certain types of documentary evidence (primarily business records, including banking records) in terms of the CPA, CPEA, LEAA and the ECT Act. Option 3 would require the introduction of a single statute to regulate the admissibility of such evidence in terms of the hearsay rule, authentication, and the best evidence rule. Option 3 would require the enactment of legislation along the lines of that set out in Annexure A.

Option 3 would achieve the objectives of both Options 1 and 2, and would also reduce the opportunity for confusion that arises from the current multiple sources of law regulating the admissibility of such evidence. For this reason, the SALRC provisionally recommends Option 3. This option does, however, present a fairly extensive departure from the status quo and would therefore require further reflection and feedback from the various stakeholders.

In Annexure A the SALRC provides draft clauses that are largely reflective of practice in several Commonwealth countries (see in particular the Model Law in Annexure D). These clauses may be assessed and modified for use under any of the three options presented above. The SALRC invites submissions in this regard.

LSSA COMMENT:

For the several reasons raised and discussed above, the LSSA supports Option 1 outlined by the SALRC.