

THE LEGAL AND REGULATORY FRAMEWORK FOR ICT IN DEVELOPING COUNTRIES: CASE STUDY OF ICT AND THE LAW OF EVIDENCE IN TANZANIA

By Andrew Mollel¹

Introduction.

ICT Policies that are agreed upon in international, regional, and national institutions can only be implemented if there is a clear and comprehensive legal and regulatory framework at the national level. ICT policy-making happens at the international level through processes like the ITU discussions on telecommunications policy, UNCITRAL development of model laws,² and WTO negotiations on trade. And at the regional level it is seen in efforts to address cross-border issues like Internet exchange point negotiations, technology trade and investment cooperation, or consortium bids to roll out Internet backbone infrastructure. At the national level ICT policies cover a range of issues, from radio and television broadcasting to the provision of telecommunications services and business transactions.³

A range of projects are underway in developing countries that integrate ICT in a number of critical areas, including notably education, healthcare, government, trade, and small business support. However, these projects frequently encounter obstacles that directly or indirectly relate to the country's legal and regulatory framework. One example is projects that rely on technology or infrastructure use that may be limited by current laws or regulations, such as satellite, wireless, or Voice over Internet Protocol (VoIP) technologies. Another example is ICT projects that are hindered by a general law or regulation, such as fiscal or other regulations that limit cross-border trade and communications. A final example is projects working in a particular area (such as healthcare) where current laws or regulations do not cover ICT use (such as privacy and data protection laws governing the handling of electronic health data).

¹ LLB Hons (Dar), LL.M (Lund), PhD Candidate (University of Joensuu -Finland), Assistant Lecturer & former Dean, Faculty of Law, Tumaini University, Iringa University College-Tanzania.

² See for example the UNCITRAL Model Law on Electronic Commerce (1996), UN and Draft Resolution No. II: UN Convention on the Use of Electronic Communications in International Contracts, 2005

³ Model Law on Electronic Commerce with Guide to Enactment, Adopted by UNCITRAL on 12 June 1996.

ICT for Development initiatives need to consider how the legal and regulatory framework will affect their activities, and plan accordingly. There are many examples where a nation's leadership has embraced ICT and is ready to promote a legal and regulatory environment that will enable its widespread use. But often at the working level, government officials do not understand the implications of existing laws and regulations that may hinder ICT use, nor the changes they need to formulate and implement to create a more favourable framework.

However, there is no "one size fits all" solution and transplanting legal models to developing countries' environments does not work. An effective ICT legal and regulatory framework is unique for each country, and must be shaped by the existing web of legislation, local culture, economics and politics, or rather, it must be contextualized.⁴

When the legal and regulatory framework limits ICT use, it can be helpful for development projects to engage in advocacy activities to inform ICT decision-making and promote appropriate changes to laws and regulations. Various questions may be posed for applying this criterion: Do the country's laws and regulations affect the use of technology? How do the laws and regulations affect technology use in the country? Does the legal and regulatory framework promote or inhibit technology use? How do legal and regulatory issues affect the use of technology envisioned in the ICT project/policy? What can the ICT project/policy do to help ensure that laws and regulations promote, and do not inhibit, technology use?

A case Study of the Legal environment, particularly the Law of Evidence,⁵ with relation to ICT development in Tanzania addresses some of these questions.

⁴ See Mikko Vesisenaho, *Developing University-Level Introductory ICT Education in Tanzania: A Contextualized Approach*, PhD Dissertation, University of Joensuu, 2007.

⁵ Almost all rules of Evidence applicable in Tanzania are provided for under the Tanzania Evidence Act, (hereafter referred to as "the TEA"), originally Act No.6 of 1967 (Cap.6 R.E 2002).

THE POLICY, LEGAL AND REGULATORY FRAMEWORK FOR ICT DEVELOPMENT IN TANZANIA

The current status of ICT in Tanzania has been influenced by various Policies, Statutes, Laws, Acts and Regulations, passed and enacted in the last 10 years. Although they were never intended to cater specifically for ICT issues, these have, among other things, brought about liberalization in the various social/economic sectors that have led to impressive economic performance. The more relevant ones are briefly described below:

Tanzania ICT National Policy: An Overview

Despite good intentions, Tanzania has been plagued by an unclear and inconsistent policy environment. This is acknowledged in the National ICT Policy, which states:

“The lack of an overall policy and poor harmonization of initiatives, has led to random adoption of different systems and standards, unnecessary duplication of effort, and waste of scarce resources, especially through the loss of potential Synergies. Therefore, this National ICT Policy deploys a broad-based strategy to address Tanzania’s developmental agenda. The need for an appropriate institutional arrangement to ensure that all stakeholders can rise to the challenge of implementing this ICT policy, cannot be overemphasized”⁶

In acknowledging that ICT is vital in supporting its efforts to achieve national objectives for the promotion and consolidation of democracy, transparency and openness, and good governance; for extending the provision of social and economic services for poverty alleviation; and for narrowing the existing digital divide,⁷ the Tanzanian government prepared the National ICT Policy of 2003 to coordinate all matters related to ICT in the country.⁸

The policy is divided into several key areas, which include (but are not limited to) the development of ICT infrastructure and Universal Access. One may however ask, today,

⁶National ICT Policy: Ministry of Communication and Transport, 2003

⁷ Ibid

⁸ The policy can be viewed at www.ethinktanz.org/secretariat/DocArchive/zerothorder.pdf visited on 30 June 2007

how successful has the National policy been? Has it achieved any of its stated aims or objectives? The success-so far-of the policy can be evaluated through two representative examples: the creation of the Tanzanian Internet Exchange and the Rural Telecommunications Development Fund.⁹

The National ICT Policy has as its first objective the need to:-

“Foster efficient, inter-operable, reliable and sustainable national ICT Infrastructure commensurate with grass-roots needs and compliant with regional and international standards, with increasing access while reducing cost”¹⁰

Background, Vision and Mission

The Policy acknowledges the wide range of converging activities, the dangers of the digital divide and the risk of being excluded further from the knowledge economy, all these being issues that pressed the Government to formulate a policy framework through which coordinating mechanisms and harmonised strategies for ICT might be nurtured.¹¹

The Policy states its vision in the following words: “By exploiting its unique geographical position, Tanzania becomes a regional hub of ICT infrastructure providing ICT-based solutions that enhance sustainable socio-economic development, which addresses national and regional poverty reduction concerns.”¹² The Policy states that its mission is “to coordinate ICT activities in the public and private sectors and to provide a conducive legal and regulatory framework and private infrastructure investments in e-commerce capacity building (infrastructure and human capital), software and hardware development and production, and promoting regional and international cooperation.”¹³

⁹Mutagahywa, B. Kajiba, J “Connectivity and E-commerce in Tanzania”
Economic and Social Research Foundation (ESRF), Tanzania, 2000 accessed at
<http://www.eldis.org/static/DOC9183.htm> on September 20, 2007

¹⁰ Article 3.2 of Tanzania National ICT Policy

¹¹ Article 1.1 of the Tanzania National ICT Policy

¹² Ibid, article 1.2

¹³ Ibid, article 1.3

Objectives of the Policy

The objectives of the Policy are grouped into nine main areas. These are: strategic ICT leadership, legal and regulatory framework, capacity building, ICT infrastructure, ICT industry, ICT productive sectors, service sectors, universal access, and local content. The main focus of this study is legal and regulatory framework. It is the Policy's objective to establish and maintain an enabling legal and regulatory framework aligned with Tanzania's constitutional provisions, legislative and regulatory environment and consistent with regional and global best practices. It further aims at ensuring that legislation is put in place to address intellectual property rights issues unique to the use of ICT networks. Finally, it is the objective of the Policy that Tanzania does not become a haven for perpetrators of cyber-crimes.

ICT Legal and Regulatory Framework in Tanzania

Despite the above-discussed objectives, there is currently no single law, which specifically regulates ICT in Tanzania. The Tanzanian Communications Regulatory Authority Act of 2003 comes closest to this function. The Act establishes the Tanzania Communications Regulatory Authority for the purpose of regulation of telecommunications, broadcasting, and postal services. The Act also aims at providing for allocation and management of the radio spectrum, covering electronic technologies and other Information and Communication Technologies (ICT) applications.

There is also an Electronic and Postal Communications Bill of 2005 which is aimed at providing for and regulating activities in the Electronic and Postal Communications sectors and related matters.¹⁴ This Bill is not intended to replace the Tanzanian Communications Regulatory Authority Act of 2003, although, if enacted, it will make extensive amendments, including repealing and replacing some of the sections of the previous Act.¹⁵

It remains clear, however, that regulation of ICT in Tanzania is still at very initial stage, and much needs to be done in the ICT legal framework.

¹⁴ According to available records, this Bill has not yet been tabled to Parliament for enactment

¹⁵ See Section 129 of the Electronic and Postal Communications Bill Act, 2005

The Policy underscores the new needs, rights and vulnerability brought by globalisation and by the pervasiveness of the Internet. The policy underlines that for secure electronic transactions to occur, an environment of trust must be created and sustained through the legal and regulatory apparatus, taking cognizance of constitutional rights and provisions of criminal, civil and commercial laws.¹⁶

The Policy acknowledges that Tanzania's legal framework, regulatory capacity and related institutional infrastructure are inadequate in quantity, quality, diversity; and that Tanzania currently lacks technological capacity conducive for ICT development and application. It then identifies the need for specific and effective legislative instruments on privacy, security, cyber crime, ethical and moral conduct, encryption, digital signatures, copyrights, intellectual property rights, fair trade practices and anti-trust practices as some legal issues that should be addressed. The Policy proceeds to declare the government's desire of providing a consolidated, effective legal and regulatory framework that offers an environment conducive to the development of ICT which can take into account issues associated with the convergence of telecommunication, broadcasting and information systems, so that new opportunities are created for the citizens of Tanzania, in line with their Constitution. It proposes, furthermore, to promote business in electronic form in a secure environment and to put in place a legal framework to provide the guiding principles, rules and regulations.

On placing the legal framework for ICT, the Policy promises that "the Government will review existing laws and regulations in order to repeal or adjust those that are not conducive to the healthy growth of the ICT industry and enact new ones that take account issues associated with e-Governance and the convergence of telecommunication, broadcasting and information systems."¹⁷

THE IMPACT OF INFORMATION AND COMMUNICATION TECHNOLOGY ON NATIONAL LAWS: THE LAW OF EVIDENCE IN TANZANIA

¹⁶ Tanzania National ICT Policy, part 3.5

¹⁷ Ibid.

In Tanzania, the role of ICT in day-to-day life is increasingly becoming more relevant and appropriate to socio-economic requirements, cultural priorities, and value systems.¹⁸ A considerable fraction of the Tanzanian public is educated in the use of Information and Communications Technologies (ICTs) and is aware of the benefits available by accessing, sharing, and processing knowledge via modern technologies.¹⁹ Tanzania has made remarkable progress in deploying ICT. This progress has been well received by many service providers who are striving to address unmet demands and competition in newly liberalized markets.²⁰

Commercial, financial and service transactions (stock markets, negotiable instruments, stock exchanges, banking business or rather SWFT networks, securities, fund transfers, purchase of goods, including motor vehicles, sales transactions, etc) are all, mostly, done electronically today in Tanzania as elsewhere. Evidence generated through this new form of business and transactions is also electronic in nature.

The current principles under the law of evidence in Tanzania assume the existence of paper -based records and documents and assume that these documents and records should bear signatures for legal recognition.

The Impact on Documentary Evidence

On documentary evidence,²¹ the Law of Evidence demands production of the *best evidence*, which is the original document or record. Electronic transactions, particularly through computer technologies, enable businesses and consumers to use computers to create, transmit, and store information in electronic form. This scenario raises a number

¹⁸ The source of this information is a document on ICT Policy in Tanzania accessed at www.ethinktanktz.org/ICTPolicy-Workshop.htm visited on 20/12/2004

¹⁹ Ibid

²⁰ Ibid

²¹ According to Section 3 of the Tanzania Evidence Act, 1967, the expression “documentary evidence”, is defined as all documents produced as evidence before the court, and may include any writing, handwriting, typewriting, printing, photostat, photograph and every recording upon any tangible thing, any form of communication or representation by letters, figures, marks or symbols or by more than one of these means, which may be used for the purpose of recording any matter provided that such recording is reasonably permanent and readable by sight.

of challenges for principles of evidence, particularly those governing admissibility of documentary evidence and authentication. The Act defines primary evidence as the document itself, produced for the inspection of the court.²² According to this rule, the document itself is the original.

The issue in an electronic environment is whether an electronic document, which may never take a physical form, should be considered to be in a written form as required by the law as indicated above. The field survey revealed that 66% of lawyers, including judges and magistrates, have ideas on the impact of ICT on the rules of evidence. Forty-Four pointed out documentary evidence as the main area so affected. The impact is reflected in the following questions: Can the document in an electronic form be retained permanently for it to qualify within the definition of the term ‘writing’ in the Statute of Interpretation. Though an electronic document may be retained permanently, in its plain definition, it cannot qualify to be a “thing” in writing. This is because a document in an electronic form consists in series of numbers stored in the computer’s memory.²³ What is displayed on the screen is a translation of the numbers by the computer, after application of a coding convention, into a form of words for the reader.²⁴

Under the Evidence Act,²⁵ therefore, the definition of the term ‘document’ entails existence of elements of physicality, visibility by sight and permanence of the record. In all senses, this excludes electronic records and documents.²⁶

Until very recently, the position of the law of evidence in Tanzania in respect of admissibility of records in electronic form was that such records were not admissible as

²² See section 64 (1) of the Act. For other definitions see 32A C.S.J. s.776, *Lukas v. Williams & Sons* (1892) 2Q.B. 113 at p. 116 per Lord Esher MR

²³ Christensen, S. “ The Requirements of Writing for Electronic Land Contracts – The Queensland Experience Compared with Other Jurisdictions”. *Murdoch University Electronic Journal of Law*

Volume 11, Number 4 (December 2004) at p. 13

²⁴ *Ibid*

²⁵Section 2 of the Tanzania Evidence Act, 1967

²⁶ *Ibid*.

evidence in court proceedings. In the most recent developments in the area, the TEA has been amended to give partial recognition to evidence generated electronically.²⁷ To keep pace with developments in science and technology, the Evidence Act is among the various laws amended by a Bill tabled before Parliament in January 2007 intended to amend various laws. The Bill introduced new types of evidence, which would be admissible by courts of law, including information obtained from computer systems, networks or servers.²⁸

However, it is still doubtful whether either under case law or statutory law a party may produce a flash disk or other compact disks or a computer hard disk to prove the contents of records resident therein. The reason, as pointed above, is that records resident in the items above are not visible unless displayed on a computer screen or as a computer- printout.

Electronic Signatures

The evolution of electronic commerce has brought with it new methods of authentication of electronic documents. Electronic signature is the main method of authenticating an electronic document or record. The issue to be addressed now is whether electronic signatures can perform the same function, which a manuscript signature performs. The rationale is that, as pointed out earlier in this study, such manuscript signatures work well for paper-based transactions.

An analysis of the various definitions of the term signature²⁹ shows that, firstly, electronic signature can consist of any electronic data, a symbol, a code, a mark or a sound logically attached or associated with electronic data. The attachment or association is logical because, as is the case with digital technology, electronic signature may sometimes take a form, which is invisible to a human eye. Secondly, that an electronic signature similar to a traditional signature is capable of performing two

²⁷ The Written Laws (Miscellaneous Amendments) (No. 2) Act, 2007

²⁸ Ibid.

²⁹ Source: www.scc-assessor.org/dictionary_of_terms.html accessed on 23/02/2005.

functions; namely, it identifies and authenticates a particular person as the source of the electronic message and indicates such person's approval of the information contained in the electronic message. Indeed, the proposed new definition of signature in this study would encompass any electronic or digital signature.

In order for a digital signature to qualify as such, it must meet the following conditions. First, it should be unique to the subscriber affixing it. Second, it should be capable of identifying such subscriber. Third, it should be created in a particular manner using a means under the exclusive control of the subscriber. Fourth, it should be linked to the electronic record to which it relates in such a manner that if the record were altered, the digital signature would be invalidated.³⁰

This discussion of electronic signature technologies demonstrates that electronic signatures are actually harder to forge than manuscript signatures. Sulner³¹ contends that identification of a piece of handwriting is not as simple as it may seem to be. It requires professional skills of comparing the handwriting. The only function which electronic signatures cannot provide is that of making a visible mark on a document. Its mark is in digital form. However, it is correctly contended that a signature, whether electronic or on paper, is first and foremost a symbol that signifies intent. The primary focus is on the "intention to authenticate," which distinguishes a signature.³²

Electronic Signatures: Meeting the law's Functional Requirements

As explained above, to be valid and effective, a signature must provide evidence of three things: the identity of the signatory, his intention to sign and his intention to adopt the contents of the document as his own.

Manuscript signatures meet these functional requirements in a number of ways. Identity is established by comparing the signature on the document with other signatures,

³⁰ Ibid

³¹ Sulner, H. F. (1959). "Mental Disorders: Their Effect Upon Handwriting." *American Bar Association Journal* 45: 931-4

³² Ibid

which can be proved, by extrinsic evidence, to have been written by the signatory. The assumption is that manuscript signatures are unique, and that therefore such a comparison is all that is necessary to provide evidence of identity. In practice, manuscript signatures are usually acknowledged by the signatory once they are shown to him, and extrinsic evidence is only required where it is alleged that the signature has been forged.

Intention to sign is normally presumed, because the act of affixing a manuscript signature to a document is universally recognized as signing.³³ Intention to adopt the contents of the document is similarly presumed because it is general knowledge that affixing a manuscript signature to a document has that effect. In both cases, the burden of displacing the presumption is on the signatory.³⁴

Electronic signatures can equally meet the law's functional requirements, but in rather different ways. To begin with, the signature itself does not provide sufficient evidence of the signatory's identity. To establish this, further evidence is required which links the signature key or other signature device used to the signatory himself or herself.³⁵

In practice, the recipient of an electronically signed document wishes to be able to rely on the signature without further checking, and so a number of organizations known as Certification Authorities have been set up. These bodies take traditional evidence of identity, (e.g., by examining passports), and, in the case of public key encryption signatures check that signatures effected with the signatory's secret key are verifiable using the public key.³⁶ Once the Certification Authority is satisfied as to the signatory's identity, it issues an electronic certificate, which includes, *inter alia*, a certification of the

³³ See also the case of *L'Estrange v. Graucob* [1934] 2 KB 394, 403 per Scrutton LJ

³⁴ See *Saunders v. Anglia Building Society* [1971] AC 1004.

³⁵ Reed C, 'What is a Signature?' *The Journal of Information, Law and Technology (JILT)*. 2000 (3): found at <<http://elj.warwick.ac.uk/jilt/00-3/reed.html>>. Accessed on 2/6/2006

³⁶ Thomas J. Smedinghoff, (ed.). *Online Law: The Special Legal Guide to*

Doing Business on the Internet. 1996, p. 46

signatory's identity and of his public key.³⁷ This certificate may be used by the recipient to prove the signatory's identity.³⁸

It is argued that, once identity has been proved, the very fact that an electronic signature has been affixed to a document should raise the same presumptions as for manuscript signatures.³⁹ There is one difference, however. In the case of a manuscript signature, the signatory has to be present in person and must have the document to be signed in front of him or her. Electronic signature technology is a little different. There are essentially two options. Firstly, the signature is effected by selecting from an on-screen menu or button, with the signature key stored on the signatory's computer. Secondly, the signature key is stored on a physical token, such as a smart card, which needs to be present before the signature software can affix the signature.⁴⁰

In either case, a third party who had access to the computer or to the storage device would be able to make the signature. For this reason, an electronic signature should be treated as more closely analogous to a rubber stamp signature.⁴¹ The party who is seeking to rely on the validity of the signature may need to adduce extrinsic evidence that the signature was applied with the authority of the signatory. In many cases, where an electronic signature which has previously been acknowledged by the signatory is effected by an unauthorised third party, the apparent signatory will be estopped from denying that it was his signature⁴² because courts presume that a third party who is given access to the signature technology has been authorised by the signatory to sign on his behalf.⁴³ Does this lead to a conclusion that an electronic signature fails to meet the evidential

³⁷ Ibid

³⁸ Ibid

³⁹ Reed C. *supra*

⁴⁰ Ibid

⁴¹ Ibid

⁴² See *Brown v. Westminster Bank Ltd.* [1964] 2 Lloyd's Rep. 187

⁴³ Smedinghoff, *supra*

requirements because a successful forgery cannot be detected easily? The answer is, no. The reason is that no such requirement is imposed for paper-based signatures.

Thus, while handwritten signatures in most cases serve merely to indicate the signer's intent, signatures in an electronic environment typically serve three critical purposes for the parties engaged in an e-commerce transaction: to identify the sender, to indicate the sender's intent and to ensure the integrity of the document signed.⁴⁴

Impact of ICT on Rules of Authentication

Admittedly, modern computer and communications technology is making it feasible, and in some cases essential, to use methods of signature which are very different from the 'traditional' manuscript signature for purpose of authenticating documents in electronic form.⁴⁵

In paper-based commercial transactions, the traditional signature has established itself as a cornerstone for effecting such transactions.⁴⁶ A set of well-defined rules governing the use of traditional signatures has developed over a substantial period. These rules are the foundation for the currently established commercial legal infrastructure, but the use of electronic signatures, it is suggested, will challenge many of these well-established rules.

The field survey revealed that 15 percent of practicing lawyers scan their signatures and embed them on electronic documents. One would be tempted to doubt whether judges are prepared to admit the documents so signed electronically. The study revealed that thirty percent of judges responded that they would allow a party in a case to tender a document signed in electronic form. Seventy percent of ⁴⁷ judges were, however, reluctant to admit documents signed electronically. Two main reasons can be attributed to

⁴⁴ Ibid

⁴⁵ Reed C, *supra*.

⁴⁶Reed, C., Op. Cit at. 1

⁴⁷ Ibid

this reluctance. First, the TEA does not provide for electronic signatures; and second, the meaning of signature does not include a signature in electronic form.

The analysis of the provisions related to signatures under TEA is that transactions must be documented in "writing" and be "signed." The immediate impression that this section demonstrates is that it requires ink on paper and, thus, the electronic communications do not meet appropriate legal requirements for writing and signature envisaged in a number of statutes, including TEA.

During the period of enactment of these statutes, the Legislature did not contemplate technological advancement, which makes it feasible to create documents in electronic form. For example, the Interpretation of Laws Act⁴⁸ defines writing as "any expression referring to writing include printing, lithography, typewriting, photography and other modes of representing or reproducing words in visible form."⁴⁹ From this definition, it is clear that digital information is not a representation or reproduction of words in a visible form. However, courts may adopt a purposive approach to the meaning of this definition and hold that an electronic document is a set of data from which words in visible form can be reproduced if required.

It is admitted that, given the ease with which the original of an electronic mail message can be forged, authentication may present a problem should the other party deny authorship of the message. Simply relying on the e-mail address in the 'From:' field of the message or on the person's typed name appearing at the bottom of the message for authentication may therefore not be enough. However, there are a number of common-sense measures that can be taken. These can include use of a private LAN, which provides independent record of message origin and reply to the stated e-mail address with an acknowledgement of receipt. An un-rejected acknowledgement may be accepted as evidence of authentication. If the order is from a known customer, the acknowledgement may be sent by fax or regular mail. The use of special customer codes or passwords

⁴⁸ Cap. 1 Revised Edition of 2002

⁴⁹ Ibid

known only to the customer may also be an alternative for meeting the rules of authentication.

Conclusion

Throughout this discussion, it becomes evident that ICT is increasingly gaining importance in almost all sectors of national development in developing countries. Electronic transactions are replacing the old and traditional methods of transacting in all walks of life. Yet, the full-fledged application of ICT for development in most of these countries is seriously hindered by lack of comprehensive legal and regulatory framework for the subject. Taking Tanzania as a Case Study, the discussion in this paper shows that although there have been some initiatives that may ultimately lead to having a legal framework that adequately regulate ICT application, much is yet to be done to eliminate the currently existing legal barriers.

The law of evidence was taken as just one such legal area where reforms are highly needed. It is observed that the Tanzania Evidence Act, 1967, that regulates admissibility of documentary evidence and signatures has been affected by the advancement of ICT. These technologies, as observed, have brought changes on the way of signing and authenticating electronic documents. It is now possible to sign an electronic document electronically.

On rules of authentication, it was observed that electronic signature technologies are capable of producing signatures that can meet legal requirements similar to those imposed on paper-based signatures. The underlying reason is that, there has been a shift from concentrating on the form a signature is supposed to take to the function the signature ought to perform. This function, as observed, is evidential.

In general, however, the legal framework for the flourishing of ICT for development is still seriously lacking in Tanzania. There is a general legal skepticism on the reliability and authenticity of documents obtained electronically.

There are a number of reasons attributed to the above scenario: The first one is based on concerns over reliability and authenticity of electronic records. For example an e-mail may just indicate the person's name as the sender of the same. The apparent issue would be whether the said e-mail message did actually originate from the purported sender. This issue centres on authenticity. The other issue would be whether the said e-mail message was not tampered with, bearing in mind the fact that the said message had been in transmission via a network composed of millions of computers. It is hard to believe that the message did actually originate from the person whose name is indicated at the foot of the message, without his/her signature.

Regarding computer print-outs, the question would be firstly, whether the purported records did actually originate from the purported computer system. Secondly, whether the records were entered in the computer system at the purported period. Thirdly, whether the records were kept or stored in a reliable system that does not allow tampering of the same, including unauthorized copying. These challenges revolve around integrity, authenticity and security of electronic records. Lack of clear answers to these challenges leads many people to be reluctant to engage in online transactions, which remain to be the main mode of transactions today.

References:

- Bacchetta, M, et al. Electronic commerce and the role of the WTO: World Trade Organization, Geneva, 1998
- Bwana, A. J., "Electronic Banking and Law in Tanzania: Approaches to its Regulation". Tanzania Lawyer, 2003.
- Chissick, M., Electronic Commerce: Law and Practice, 3rd Ed., London, Maxwell, 1999.
- Dalhuisen, Jan. Dalhuisen on International Commercial, Financial and Trade Law, 2nd Ed, Hart Publishing, Oxford and Portland Oregon, 2004.
- Field, D. Field's Law of Evidence, 10th Edition, Law Publishers, Allahbad – 1, 1971
- Hagberg, Karen L Hagberg, Karen L., and A. Max Olson. "Shadow Data, E-mail Play a Key Role in Discovery, Trial." New York Law Journal, vol.4 (1997), p.36
- Harris, V. "Law, Evidence and Electronic Records: A Strategic Perspective from the

- Global Periphery” National Archives of South Africa Journal of the Society of Archivists, Volume 25, Number 2 / October 2004 at pp 211 – 220
- Kamal, A & Gelbstain E., Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security, UNITAR, 2002
- Kerr S.Orin, “Computer Records and the Federal Rules of Evidence”, USA Bulletin (March 2001)
- Krishnamachari, V., Law of Evidence (as Amended by Act No. 4 of 2003).
- Mackaay, E et al (eds), Electronic Superhighway: The Shape of Technology and Law to come, Kluwer Law International, The Hague/Boston, 1995
- Malik, V., Malik, V., “Cyber Law: A Comparative Study for the Legal Framework for E-Commerce in India and the United States”, *The Southern Law Journal*, xii, Fall 2000
- Masara, Y. “Advancement in Technology: A Quest for the Law on Computer and other Electronic Transactions in Tanzania,” A paper presented at the Annual General Meeting for the State Attorneys, DSM, 2006
- Mercer, C. “Telecentres and Transformations: Modernizing Tanzania through the Internet,” *African Affairs: The Journal of the Royal African Society*, Vol.105 No. 419, 2006, pp.243-264
- Sarkar, M. C. Sarkar on Evidence, 15th Ed, Nagpur, Wadhwa & Company, 2001. Vol-I and Vol-II. Sweet & Maxwell, 2000
- Siegfried Eiselen. “Electronic commerce and the UN Convention on Contracts for the International Sale of Goods (CISG) 1980” *EDI Law Review* (1999) 21-46
- Singh, A. Principles of the Law of Evidence, 1st ed, Central Law Publishers, Allahabad, 1977
- Sulner, H. F. (1959). "Mental Disorders: Their Effect Upon Handwriting." *American Bar Association Journal* 45: 931-4
- United Nations, UNCTAD, “E-Commerce and Development Report 2002” New York/Geneva, 2002
- United Republic of Tanzania, Law Reform Commission of Tanzania, position paper on e-

commerce, accessed at <http://www.lrct-tz.org/Positionpaperone-COMMERCE.DOC>

Zekos G. I., "Technology and Electronic Signatures, Intellectual Property & Information Technology Law, Vol. 8, Issue 6, Dec. 2003.