AN APPRAISAL OF THE ANALYSIS OF THE ELECTRONIC SIGNATURES' ACT NO 7 OF 2011 AND ITS IMPACT ON EVIDENCE LAW IN UGANDA

BY

NAMBUSI MARIAM

LLB/37843/123/DU.

A RESEARCH REPORT SUBMITTED IN FACULTY OF LAW IN PARTIAL FULFILLMENT OF REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS (LLB) OF KAMPALA INTERNATIONAL UNIVERSITY

JUNE 2016

DECLARATION

I, NAMBUSI MARIAM, DO HEREBY declare that this dissertation is my own original work. And that it has not been presented and will not be presented in any institution for the same purpose or for award of any degree.

Signature: .....

Date: 8th/05/2016

Reg. No: LLB/37843/123/DU.

APPROVAL

The undersigned hereunder certifies that she has read and recommends for acceptance by Kampala international university a dissertation titled:

An Appraisal of the analysis of the electronic signatures' act no 7 of 2011 and its impact on evidence law in Uganda in partial fulfillment of requirements for the award of the degree of Bachelor of Laws (LLB).

Supervisor: Miss. KARUNGI ANNET MUTABINGWA:

Signature..Karungi..... Date: 7/6/2016.....

COPYRIGHT

DEDICTATION

I solely and whole heartedly dedicate this work to my dear DAD Mr. MATAYO KAZIBWE NYOMBI and my lovely MUM MISS EVELYN KAZIBWE.

ACKNOWLEDGEMENTS

May the blesses above be unto categories of persons here below, under whose assistance this study work is completed well; I sincerely thank my supervisor,. Miss. KARUNGI ANNET MUTABINGWA .under whose efficient supervisions and academic guidance this study work is completed. She has given me not just material supports, directions, and courage but the support and directions which encouraged and motivated me in trying whatever possible means and material is in doing the same, I thank you very much Counsel. A word of appreciation is to be noted for the Dean of Faculty of Law Miss. SARAH BANENYA, and the (Lecturers at the Faculty of Law)

for their direct and indirect supports for the best of this study. I thank my family, my father Mr. MATAYO KAZIBWE NYOMBI, my mother Miss EVELYN KAZIBWE my sisters, and my brothers for their love, financial support and courage while in my studies.

May God grant in you PEACE and LOVE always.

A special note to Counsel EVANS OCHIENG OMWANDA and Counsel JORDAN ASORDIO for supporting me. And to me myself NAMBUSI MARIAM.

I know I owe a debt for my dearest colleagues, referred to as

AMICUS

All my classmates, which words cannot merely repay for you but the love I have for you is far reached guys. To all the above, named and unnamed, may I say to the best I can, THANK YOU ALL.

... as it was in the beginning, is now, and ever shall be world without end.

AMEN

LIST OF CASES

Howley v. Whipple, (1869) 48 N.H. 48 New Hampshire Supreme Court

Mehta v. J Pereira Fenandes SA, [2006] EWHC 813 (Ch.) (07 April 2006)

R v. Prof. Costa Ricky Mahalu and Another, Economic Case No. 1 of 2007, the Resident Magistrate's Court of Dar es Salaam, Kisutu (*Unreported case*)

Trust Bank Ltd v. Le-Marsh Enterprises Ltd., Joseph Mbui Magari, LawrenceMacharia, Case No. 4 of 2000. High Court of Tanzania Commercial (*unreportedcase*)

LIST OF STATUTES

Electronic Signatures in Global and National Commerce Act, 2000

Electronic Signature Law of the People's Republic of China, 2004

Directives 1999/93/EC of the European Parliament and of the Council of 13 December1999 on a Community framework for electronic signatures (OJ No. L 13 p. 1219/1/2000.

Mauritius Electronic Transactions Act No. 23 of 2000

Mauritius Electronic Transactions (Certification Authorities) Regulations, 1s tof December 2010.

Government Notice No. 213 of 2010

Mauritius Data Protection Act No. 13 of 2004

Mauritius Information and Communication Technologies Act No. 44 of 2001

Mauritius National ICT Policy, 2007

Personal Information Protection Electronic Documents Act, 2000

Uniform Customs and Practice for Documentary Credits for Electronic Presentation("eUCP"), 2007Uniform Electronic Transactions Act, 1999

UNICTRAL Model Law on Electronic Commerce with Guide to Enactment 1996 withadditional article 5 *bis* as adopted in 1998,

UNICTRAL Model Law on Electronic signatures of 2001

ABBREVIATIONS

ATMs	Automatic Teller Machines
BOU	Bank of Uganda
CAP	Chapter
CAs	Certification Authorities
CCAs	Controller Certification Authorities
CPS	Certification Practice Statement
CRDB	Community Rural Development Bank
UCP	Uniform Customs and Practice for Documentary Credits forElectronic Presentation
Ed.	Edition
E-Signature	Electronic Signatures
E-Commerce	Electronic Commerce
E-Transactions	Electronic Transactions
E-Government	Electronic Government
EPIC	Electronic Privacy Information Centre
GBDe	Global Business Dialogue on E-commerce
Ibid	ibidem (*in the same place*)
ICC	International Chamber of Commerce
ICT	Information and Communications Technology
ILPF	Internet Law and Policy Forum
LL.B	Bachelor of Laws*(Legum Baccalaureus)*
Ltd	Limited
NBC	National Bank of Commerce Limited
NMB	National Microfinance Bank

Op. cit	Opera citato (*as cited earlier)*
PIN	Personal Identification Number
PKI	Public Key Infrastructure
Pp.	Pages
R	Republic
SADC	South African Development Community
SAUT	Saint Augustine University of Tanzania
SWIFT	Society for World Interbank Financial Telecommunications
TLR	Tanzania Law Reports
TRA	Tanzania Revenue Authority
TTPs	Trusted Third Parties
UNCITRAL	United Nations Commission on International Trade
UN	United Nations
USA	United States of America
WIPO	World Intellectual Property Organisation.
WTO	World Trade Organisation

TABLE OF CONTENTS

ABSTRACT

Digital signature provides information regarding the sender of an electronic document. It provides data integrity, thereby allowing data to remain in the same state in which it was transmitted. Here the most widely used type of cryptography is the public key, where the sender is assigned with two keys, one public and another private key. The original message is encrypted using public key while the recipient of the message requires private key to decrypt the message. Then the recipient will be in position to determine whether the message is altered or not.
The following were objectives, To examine the legal basis for Electronic Signatures in Uganda, to find out whether Uganda reaches the international standard in recognition of electronic signatures, to determine the role of electronic signatures as a tool for authentication of electronic record, to give suggestions and provide ways for Uganda to follow in reaching the international standards of E-Commerce by formulating the matching legal basis for E-Signatures.
The method to be employed here in carrying out the research for the purpose of this paper would be by means of secondary sources which is mainly documentary. Information would be sourced from textbooks, internet, journals written by jurist and public lectures delivered by various professors if there is any related to my thesis, studying them and drawing a conclusion and preferring recommendations. Also, in illustrating the admissibility of electronically generated evidence, great reliance would be placed on case law and the constitution will serve as the primary source of all the provisions to be analyzed.

Normally, the real meaning of development is that changes occurs either automatically or brought by forces of something not easily controllable, but which demands for its adherence for better ending. With the ICT development in the world, changes have been noted from individual to government perspectives, as billions of people are using internet or electronic in transacting. The development which is brought by technological changes, which in any society are inevitable. With this technological evolution, different sectors of society's mode of social, economic, political and technological life are in need to be changed incompliance with this global changes
Act to be amended to Add Reciprocal Recognition of Foreign CA's and Certificates Issued by Foreign CA's Most international E-commerce laws now provide for various forms of legal recognition of foreign CA's and certificates issued in foreign countries, the ESB fails to do this.
Assign More Potential Liability to CA's It is unusual in international E-signature law to find as much limitation of a CA's liability as in Uganda. This needs to be changed·
Information Technology Courts Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology ("I.T.") Courts should be established as a court-of- first-instance for them. The I.T. Courts would be tribunals consisting of three experts.

CHAPTER ONE

GENERAL INTRODUCTION

1.0 INTRODUCTION.

This chapter presents the general introduction of the topic of study. It discusses the background, the problem statement, the general objective and specific objectives of the study.

The researcher also gives the scope, justification, significances' and the conceptual framework of the study.

The study assesses the impact of the electronic signatures Act No.7 of 2011 on evidence law in Uganda.

Handwritten signatures have always been generally accepted as giving sufficient certainty as to the signor's identity for a great many transactions. . Hand written signatures are used for two main purposes that of authentication and that of integrity, by various technological means electronic signatures have sought to achieve the same level of authentication and integrity. This is achieved successfully in most instances and digital signatures appear to be becoming an alternative to the more traditional handwritten signatures, if not a suitable replacement.

Under the Ugandan Legislation an electronic signature means data in electronic form affixed to or logically associated with a data message, which may be and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature[1]. This might include, for example, using your name on an email and sending it from an identifiable email address.

This considered it is also evident that digital signatures bring with them a whole host of new difficulties in relation to data protection, security and advancement of technology. Reliance on digital signatures alone causes concern because a key pair may be created by an individual who then fraudulently represents the key pair as belonging to another person or entity. This is partly

[1] Electronic signatures' Act no7 of 2011

addressed through verification by a certificate authority. A certificate authority is a trusted third party (e.g. the post office or a bank) that will satisfy itself as to the identity of an individual or company. This is done by for example checking an individual's passport or driver's licence details, or a company's corporate documents and returns. The certificate authority will then issue a digital certificate signed with its own digital signature, which the user will attach to its own digital signature as proof of identity.

As technology and globalization grow digital signatures have become an essential requirement in relation to business transacted electronically. With the growing use of the internet as an acceptable and indeed standard medium, one does not have to look further than their own residence to confirm the growing need for electronic signatures and therefore the research into this area continues and suggested that it should be concentrated on the need to improve security measures.

1.1 BACKGROUND TO THE STUDY

The latter part of the twentieth century was marked by the electronic transistor and machines and ideas made possible by it. As a result; the world changed from analogue to digital. Although the computer reigns supreme in the digital / electronic domain, it is not the only electronic device. An entire constellation of audio, video, communication and photographic devices are becoming so closely associated with the computer as to have converged with it.

An early validation of electronic signatures' came from the new Hampshire supreme court in the case of Howley v Whipple[2] Where it was held that;

"... it makes no difference whether the telegraph operator writes the offer or the acceptance in the presence of his principle and by express direction with a steel pen an inch long attached to an ordinary penholder or whether his pen be copper wire a thousand miles long.in either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case a more suitable fluid known as electricity performs the same office..."

[2] 48 N.H. 487 (1869)

In the 1980s companies and even some progressive individuals began using fax machines for high priority or time sensitive delivery of paper based documents.

On June 30, 2000 President Bill Clinton signed the electronic signatures' in global and national commerce act (ESIGN) using his electronic signature id and thereby established the validity of electronic signatures' for interstate and international commerce. Ironically, he did so using the exciting new technology himself instead of using pen and paper; he used a smart card encrypted with his unique digital signature.[3]

When the first contract was signed and faxed it created the basis for the discussion of electronic signature validity. After all it was the first time someone could sign something, place it in a machine, send it from one phone line to another and deliver a digitally reproduced signature. The path this signature took was not controllable or traceable, but nonetheless the issue as to whether it constituted a valid signature could be determined on an analysis of basic principles. Thus, the intentions of the signature were clear. Following a succession of decisions in which courts on different countries ruled that this method of signature capture carried the same validity as if the parties were standing in the room together, the fax became a standard procedure for concluding contracts world-wide. [4] Today the fax machine is a staple of the business world. Most people do not even consider the original hurdles this new medium created nor do they consider /its impact on the spread of communication and the advantages of its use. However in its infancy many of the same issues surrounding electronic communications and electronic signatures' had to be resolved when utilizing the facsimile.

By the time the act officially became law, a number of states had already passed laws involving electronic signatures and recordkeeping. However, the E-Sign Act made electronic contracts legal for both interstate and global commerce, providing the entire nation with new ways to conduct business online. The bill addressed concerns many had about U.S. companies keeping pace with their international counterparts, who already possessed secure and legal means to sign contracts online. The law also allayed concerns about the legal validity of non-paper signatures

[3] The History of Electronic Signatures' Laws Monday (03/16/2009) Article by Isaac Bowman.
[4] Law reform commission consultation paper on documentary and electronic evidence (LRC CP 57 - 2009)

in court. By directly addressing these concerns, the new law created marketplace legitimacy for electronic signatures.

1.2 STATEMENT OF THE PROBLEM.

In Uganda, like any other country, recently companies, individuals and the country is in use of internet as a means of transacting. Still this study believes that there is mismatching of the law regulating such transactions, and most specific in aspect of authentication of electronic transactions. To this point, the study having reveals this lacunae, it further suggests and give ways for better formulation of the matching legal basis for electronic signatures as a tool for authenticating any electronic records.

1.3 SIGNIFICANCE OF THE STUDY

This study realized many goals;

- As a researcher acquired new knowledge on the effectiveness and validity of electronic signatures in verification of business transactions
- The study creates awareness to the society, as private individual and companies' are engaging daily into international transactions by using online ways.
- The Government benefits as with regards to recommendations given out by the researcher, if are to be implemented, also the government is put aware in enacting supportive regulations.
- To Kampala International University, the copy acts as source of literature review after being put at library. It further enriches learning resources to other students.

1.4 OBJECTIVES OF THE STUDY

1.4.1 MAIN OBJECTIVES

- To examine the legal basis for Electronic Signatures in Uganda

1.4.2 SPECIFIC OBJECTIVES

- To find out whether Uganda reaches the international standard in recognition of electronic signatures.
- To determine the role of electronic signatures as a tool for authentication of electronic record.

- To give suggestions and provide ways for Uganda to follow in reaching the international standards of E-Commerce by formulating the matching legal basis for E-Signatures.

1.5 HYPOTHESIS

- This study is being guided with the following assumptions;
- That lack of effective legal mechanisms in recognition of electronic signatures has weakened the protection and realization of rights of persons who are transacting through internet.
- That lack of, and ineffective legal institutions, especially in providing security has marked the failure to meet the demands of the modern commercial transactions and the adopted global changes.
- That weak and poor policy in electronic commerce of the state in Uganda exposed business man, consumers and the government into huge financial loses and dormant economy

1.6 RESEARCH QUESTIONS

- What are Electronic Signatures?'
- What is the legal status of Electronic Signatures' in Uganda?
- How use full are Electronic Signatures' in Uganda?
- What is the Electronic Signatures Directive?
- How have electronic signatures' influenced evidence laws in Uganda?

1.7 SCOPE OF THE STUDY

The scope of the study is seen in the way it clarifies the confusion that has surrounded the admissibility of electronically generated evidence. This thesis will evaluate the practically application of electronically generated evidence and how it has been able to fare in the present day court system. Hence, this thesis is able to lay bare given some rules the situation that must exist for electronically generated evidence to become admissible or otherwise.

1.8 METHODOLOGY.

The method to be employed here in carrying out the research for the purpose of this paper would be by means of secondary sources which is mainly documentary. Information would be sourced from textbooks, internet, journals written by jurist and public lectures delivered by various

professors if there is any related to my thesis, studying them and drawing a conclusion and preferring recommendations. Also, in illustrating the admissibility of electronically generated evidence, great reliance would be placed on case law and the constitution will serve as the primary source of all the provisions to be analyzed.

1.9. LITERATURE REVIEW

Much have been written recently with regards to electronic commerce of which at large extent the concept of electronic signatures has been advocated as the means of authenticating such transactions made online or on open networks, as reviewed here below;

Mollel. Ain his article[5], he noted among other things that the evolution of ICT has come with it a new way of authenticating electronic documents. The tool he refers to as electronic signatures, the author poses questions such that whether electronic signatures can meet the degree which is met by manuscript or paper based signatures. He contends further that electronic signatures must meet legal standards for it to be reliable in evidence. Andrew has failed in his work by not providing the frameworks for Tanzania legal basis to that effect, the framework which this study is intending to propose.

Mambi A[6]he asserts that the increase use of electronic authentication techniques as substitutes for manuscript or handwritten signatures and other paper based authentications procedures suggest the need for creating a legal framework that will regulate e-signatures. He admitted that laws in Tanzania neither cover online transactions nor recognize cyberspace or digital signature. Adam further adds that the laws governing business transactions provides that the contract must be in writing and dully signed or authenticated before witnesses, and that this requirement is no longer applicable in online trades, then off-lines laws have to be changed and reformed to accommodate e-commerce principles.

---

[5] Mollel A:*The Legal and Regulatory Framework for ICT in Developing Countries:* Case Study of ICT and the Law of Evidence in Tanzania, at p. 9

[6] Mambi A (2010)*"ICT Law Book: A Sourcebook for Information & Communications Technologies and Cyber Law"* Mkuki na Nyota Publishers Ltd, Dar es salaam, , at pp. 102-103

Adam Mambi though gives this good position but he neither did propose nor provide the relevant legal basis, as he suggested, the basis which this study is intending to show. According to

Davidson A[7]he pointed out that the signature has been the prime method used as the proof of identity, and as a material intent and execution of documents. A signature on a document indicates the provenance of a document and the intention of the signatory with regards to the contract. With the advent of electronic era, a form of signature is adopted for electronic documents. The author[8] asserts further that electronic signature has different risks. While the simple electronic signature merely typed at the end of an electronic record may be less secure than traditional signature

"... anyone could type a person's name at the end of a typed electronic communication. Such signature, while valid in the right circumstances, is most insecure".

Alan does not suggest for mechanisms for securing and validating such electronic transactions, as he does not give much credits on electronic signatures as a tool for security, a tool which this study believes as the only one for authenticating any electronic record. According to

Lewis M[9], on his article he advocated for the Canadian legislative approach designed to ensure that electronic signatures have the validity and trustworthiness required by businesses to compete in the global marketplace. The author has tried to cover the traditional objective of signatures and on how those objectives can be met by applying digital signature. However the author has failed to show the framework that develops a systematic methods for promoting secure electronic commerce transactions between parties over open networks.

According to Stephen E. B[10],he define electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. He added that an electronic signature may take a number of forms, as a digital signature, biometric identifiers such as a voice pattern, facial recognition, a retinal scan, a

[7] The Law of Electronic Commerce"First Published, Cambridge University Press, pp. 74
[8] Op. cit.
[9] Lewis M (2002) "Digital Signatures: Meeting the Traditional Requirements Electronically - A Canadian Perspective" 2 as per Rev. International Businesses & Trade Law. Pp. 63
[10] Stephen E. B (2010) "Rangoon Enters the Digital Age: Burma's Electronic Transactions Law As A Sign of Hope for A Troubled Nation" Vol. 3, No. 1 January 2010, p. 5

digitized fingerprint or a digitized handwritten signature, a pin number or merely a name typed at the end of an e-mail message. Professor Stephen Blythe has failed therefore to give the legal verifications on whether if the above mentioned mechanisms or systems are capable of ensuring security in aspect of business transactions as he asserts being the authenticating mechanisms of an electronic signature.

Also Prins C[11], while addressing to the Canadian authority he asserts that the government transition to electronic services has been seen as if its services were analogous to those of enterprises that sell or offer services online. Moreover, he suggested that the Canadian government should become a model user of information and communication technologies (ICTs) given that a government's commitment to electronic commerce would be a key means of unleashing the enabling effect of ICT in government and in the economy as a whole, putting in mind the fact that governments around the world have recognized widely this potential but new technologies. However, the author was in the view that even states do transact other than private individuals, but he fails to show remarks on how does electronic signatures verify business transactions in legal sense.

Turban E[12]his work is of significance. He among other things asserts that in E-Commerce we have what is so called the distance selling contracts using distance communication through internet. In real sense he was in the view that a distance selling contract is any contract concerning goods and services concluded between supplier and a consumer under an organized distance sales or services provision scheme run by the supplier, who for the purpose of the contract, makes exclusive use of one or more means of distance communication up to the moment which the contract is furnished. He similarly failed to point out means which can verify such distance trading, since they employs internet as means of communicating.

Edward L[13]in his work, he tries to give solutions on questions raised out of transactions done over the internet, as when communications is deemed to be an offer and bind the offeror and when the acceptance is effective. These all come into being since the problem which might be

[11] Prins C (2007) E-government: A Comparative Study of the Multiple Dimensions of Required Regulatory Change" Electronic Journal of Comparative Law, vol. 11.3 (December 2007), pp. 10

[12] Turban E (2002)*"Electronic Commerce"* Sweet & Maxwell Publishers, London at page 30-31

[13] Edward L (1977) *"Law and the Internet, Regulation Cyberspace"*

observed in online contracts is on how to determine the rule with regards to instantaneous communication which should apply or whether the postal rule is the more appropriate analogy, out of which the author suggested that dispatch of the accepting email or response form is more effective. He is silent then failed by not addressing the issues on whether the dispatch of the accepting email is comparable to seal or electronic signature, also the author similarly failed by not pointing the authenticity of an email in verifying online contracts.

Jianying Z et all[14]in their work they noted that the important feature of digital signatures is to serve as non-repudiation evidence. To be eligible as non-repudiation evidence, a digital signature on an electronic document should remain valid until its expiry date which is specified by some non-repudiation policy. As signature keys may be compromised and the validity of signatures may become questionable, additional security mechanisms is needed to be added on digital signatures. Meaning while, the authors have failed to point out on what is to be added on digital signatures as a tool and evidence that electronic data or record have not tempered with in course of its transmission to the other part, as they were not exhaustive in suggesting other modes as comparable to digital signatures and as electronic signatures in electronic commerce.

Zaremba J[15]his work is of significance as he tries to respond to hypothetical issues on how electronic contracts are made and the applicable law. He added that internet allows the instantaneous communications of digitized information which is an ideal of negotiation and closing of contracts between distant parties, he went further giving advantages of online contracts as time efficiency and storage savings, for businesses and all the world, and that due to these incentives more and more parties will be transacting over internet for distant parties. He also failed to give solution and position on parties transacting from different jurisdictions, as the other part for instance might be trading from Tanzania the country which do not have good electronic regulatory instrument and the developed one like United State of America, he fails also by not showing the authenticity of such transaction in case of default by one part.

[14] Jianying & Robert Deng:*On the validity of Digital Signatures*, Kent Ridge Digital Labs, 21 Heng MuiKeng Terrace Singapore 119613

[15]Zaremba J (2003) *"Article: International Electronic Transaction Contracts Between U.S and EU Companies and Consumers"* Connecticut Journal of International Law, Spring 2003 18.Conn. J. Int'l L. 479

In his work *Dr. M. Patterson*[16] he pointed out that even though legal issues in electronic transactions like the applicable law, jurisdiction and enforcement of legal rights, commercial protection and unsolicited email have been appropriately resolved, internet users will be unlikely to use the internet on a routine basis for commerce, unless they have confidence that their communications and data are safe from unauthorized access or modification. Here the author was in view that electronic data especially in electronic transactions need appropriate security and authentication however the writer is silent by not suggesting on what can authenticate such communications.

[16] Dr. M. Patterson (2001) *"E-Commerce Law, Session 4b: Info economy issues"* Hyatt Hotel, Canberra (Law school of Monash University)

CHAPTER TWO

CONCEPTUAL AND THEORETICAL FRAMEWORK

2.1. INTRODUCTION

This chapter focuses on legal basis for E-Signatures based from the overview of computer system revolution, historical background of ICT in Uganda, concepts relating to E-Signatures, including what is E-Signatures, its forms, the concept of authenticity and the law and trust in E-Commerce, looking at legislative frameworks from other jurisdiction's laws.

2.2. OVERVIEW OF COMPUTER SYSTEM REVOLUTION.

It is true that with the development of computer system in the world, life has become easier with the use of internet, as trade and other stuffs, like contracts to which individuals, banks, accounts, lawyers, businessman and even governments in the world use electronic as a means of communicating or disseminating information. As once noted by Alfonso Lenhardt that;

> "We need strong laws to protect the builders and users of the internet in order to foster innovation and creativity, safeguard consumers, drive economic growth and protect our borders"[17]

Here the US ambassador was in the view that states in the world are in need of enacting laws to coup with such global changes. It is well founded that the only tool to be used in authenticating any electronic record, as being advocated in different E-Commerce laws from different perspectives is E-Signatures, which in real sense is the only tool, however being in different forms. It is therefore the requirements of electronic transactions that there must be clear legal basis for E-Signatures at least in each country.

2.3. HISTORICAL BACKGROUND OF ICT IN UGANDA.

The first computer ever in Uganda was an unwieldy mainframe, which arrived in 1967[18]. According to Dr Ham-Mukasa Mulira, an IT expert, Independence resulted in a rise in

[17] US ambassador Alfonso Lenhardt and Tanzanian Attorney General Frederick Werema officially opened the cybercrime legislation and capacity building workshop for Eastern and Southern Africa on Wednesday 23rd February 2011.

[18] "Uganda's journey to a computer era" Daily Monitor Kampala 13th March 2010 BY Isaac Imaka.

government workers so the computer was brought in to help with management of public servant's payroll[19].

The mainframe was a huge, heavy metallic box-like object with neither a keyboard, mouse, nor a central processing unit. Instead, it functioned through punch cards, usually operated by women, and it required special skills to operate. It could only be used for adding and subtracting numbers[20].

It was stationed at the Uganda Computer Services in the Ministry of Finance under the supervision of Mr I.K Kabanda, the then government chief statistician who also spearheaded the training of Uganda's first computer specialists[21].

In 1968, the second mainframe arrived and was taken to Makerere University's department of mathematics and placed under Prof. Paul Mugambi, currently vice chancellor of Nkumba University. It was a preserve for those who were doing mathematics, today's computer scientists. Later, this was sold to Dr Patrick Mangheni of Uganda Data Services, making him the first Ugandan to offer computer services commercially[22].

It was not until the mid 80's that the first desktop Apple was brought to Uganda. It was purchased by Makerere University at the prompting of the then bursar, Mr Khan, to handle the university's payroll[23].

Hardly 50 years since the mainframe's arrival, there are now hundreds of thousands of computers in the country.

According to Mr Blasio Kigozi, Uganda's first systems analyst, now in private business; "if the current development is not politicised, IT development in Uganda is headed for good things"[24].

Now not only IT professionals use computers, but the everyday person, especially in the urbanised part of the country. The noisy type-writers have been replaced by soft touch and sensor

[19] Ibid 18
[20] Ibid 18
[21] Ibid 18
[22] Ibid 18
[23] Ibid 18
[24] Ibid 18

key boards, and work which used to take two days during the era of the mainframe, now takes less than an hour to complete[25].

Productivity levels have definitely moved up with this development. Almost all the nearly 30 universities across the country offer an ICT component on their programme prospectus which means the critical mass required to service the growth is being built in tandem with the increased access. The increase in computer usage and ownership has been boosted by the scrapping of tax on computers. A computer that used to cost about Shs1.6m now goes for as low as Shs500,000[26].

About one million Ugandans have access to computers, a number which is still lacking compared to the developed countries. For instance about 120 million people in the US, according to statistics from US Census Bureau have access to a computer[27].

2.4. CONCEPTS RELATING TO E-SIGNATURES.

These concepts to be discussed here below are essential part in this study. They are discussed not just as the cornerstone but as linkage of the coming discussion at hand.

2.4.1. WHAT IS E-SIGNATURES?

Electronic signature is referred to as data in electronic form in affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in a data message[28].

A. Davidson (2009)[29] in his writing asserts that; "The signature has been the prime method used as the proof of identity, and as a material intent and execution of documents. A signature on a document indicates the provenance of a document and the intention of the signatory with regards to the contract. With the advent of electronic era, a form of signature is adopted for electronic documents".

[25] Ibid 18
[26] Ibid 18
[27] Ibid 18
[28] Ibid 1
[29] A Davidson (2009) "The Law of Electronic Commerce" First Published, Cambridge University Press, pp.74

Stephen E. B (2010)[30] defines electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Example of E-Signatures includes;

a. A name typed at the end of an e-mail by the sender, as it was determined in ***Mehta Vs. J Pereira Fenandes SA***[31] to the effect that if a person sent an email typing his name or his principal's name then such an email amounts to a valid signature.

b. A digitized image of a hand-written message signature that is attached to an electronic document (sometimes created by biometrics-based technology called signature dynamics)

c. A secret code, password, or PIN to identify the sender to the recipient (such as used with ATM cards and credit cards)

d. A unique biometric-based identifier (such as fingerprints, voice print, or a retinal scan) sign the record". The definition which was initially provided under the U.S Uniform Electronic Transactions Act,1999

e. A mouse click (such as "I accept" button also called web-click in case a person orders goods by visiting website of the seller and initiates the transactions)

f. A sound (such as the sound created by pressing "9" on your phone to agree)

g. A "digital signature" (created through the use of public key cryptography)

Therefore, the term electronic signature implies a stylized script associated with a person.

[30] Stephen E. B (2010) "Rangoon Enters the Digital Age" Burma's Electronic Transactions Law As A Sign of Hope for A Troubled Nation, Vol. 3, No. 1 January 2010, p. 531 [2006] EWHC 813 (Ch.) (07 April 2006)
[31] [2006] EWHC 813 (Ch)

It is comparable to a seal in paper based documents. In commerce and the law, a signature on a document is an indication that a person adopted the intention recorded in the document in question.

2.4.2. DIGITAL SIGNATURES.

As there is no central authority controlling the Web, it is assumed that anyone can say anything about anything. This freedom of expression is a great idea, but it can lead to misuse of this freedom and result in mistrust. If the Web has to become the single source of all information, it has to provide a mechanism of proving trustworthiness. The digital signature is the mechanism that is going to be used to provide proof that a certain person wrote (or agrees with) a document or statement. This will create trust to users.

Digital signature provides information regarding the sender of an electronic document. It provides data integrity, thereby allowing data to remain in the same state in which it was transmitted. Here the most widely used type of cryptography is the public key, where the sender is assigned with two keys, one public and another private key. The original message is encrypted using public key while the recipient of the message requires private key to decrypt the message. Then the recipient will be in position to determine whether the message is altered or not.

However, although this system guarantees the integrity of the message, it does not guarantee the identity of the sender (the public key owner). Then in order to remedy this a "Certificate Authorities" (CAs) is required.

The Certificate Authorities are trusted third parties who provide a variety of cryptography service to their clients. CAs are trusted third parties who have been given license to produce digital certificates authenticating digital signatures. In order for this to work the Licensed CA must be reliable and have the confidence of the public and business community. And for those acquires license from the CAs are to be held liable upon any errors by themselves. Hence this provide assurance that electronic commerce are secured.

2.4.3 THE CONCEPT OF AUTHENTICITY

2.4.3.1 AUTHENTICITY

This is concerned with the source of information, or the sender of such information. Then as the legal requirement and in order to meet this requirement, the most common and popular way of accomplishing this identity check is to use an e-mail based identifier. This is a process most people have experienced at some point while using the Internet. If you sign up for a web based service you generally need to create a user name and password.

When you create this account many systems will send a verification e-mail to the e-mail address you entered for your record, thus proving that you own this e-mail address.

Another way to verify an identity is to use a known third party validation mechanism. That you may have experienced it with a web site requiring you enter in your home zip code, an account number or in some cases a credit card number. Many web sites will have you enter your credit card information into a form, allowing them to cross reference the information you provide them with a credit card merchant[32]. Presumably if you told the credit card company the truth about you, then it will match with the information you provided the website

2.4.3.2 INTEGRITY

Integrity simply means providing a reasonable belief that any file electronically signed on a system cannot and has not been tampered with by anyone or anything. Integrity is critical in e-commerce in negotiation and contracts formation online, licensing of digital content, payment through internet and proving the content of the same at later[33]

2.4.3.3 NON-REPUDIATION

Non-repudiation is the ability to hold the sender to his communication in the event of a dispute. A party's willingness to rely on a communication, contract or funds transfer request is typically contingent upon having same level of comfort that the party can prevent the sender from denying

---

[32] Isaac Bowman: Electronic Signatures Compliance, available at http://www.arx.com/resources/whitepapers/digital signature-compliance-whitepaper.htm, visited on 20th November, 2012

[33] Adam J. Mambi (2010); ICT Law Book; A Sourcebook for Information & Communication Technologies and Cyber law; Mkuki na Nyota Publishing Ltd. Dar es Salaam, Tanzania, at pp. 122

that he sent the communication or from claiming that the content of the communication as received are not the same as to what the sender sent[34]

2.4.3.4 SECURITY PROCEDURES

Establishing trust in electronic transactions involves the use of security procedures.

Security procedure in this context means a procedure employed for purpose of verifying that electronic signature, record or performance is that of a specific person or for detecting changes or error on an electronic record. There are number of procedures to be employed as security in this aspect, like the use of digital signatures, e-mail based identifiers, replies and acknowledgements, repeat-back acknowledgements, date or time stamping, encryption and or the use of Trusted Third Parties (TTPs), (TTPs) in this context referred to mean Certificate Authorities (CAs)[35]

2.5. THE LAW AND TRUST IN E-COMMERCE.

A trustworthy electronic signatures is a precondition to enforceability as a signature. This approach requires an electronic signatures possess four attributes, such that it must be unique to the person using it, it must be capable of verification, it must be under sole control of the person using it and lastly it must be linked to the data such a manner that if the data is changed, the signature is invalidated[36]

2.6. CONCLUSION.

It is well notable that with the advancement of computer systems in the world individuals are being in frequent use of that system, Uganda are not behind with this global changes since internet is in use. The Electronic Signature Law in Uganda is in fact in compliance with the UNCITRAL framework. Hence the intention of this study in this chapter is to show how the advancement of computer compels Uganda to come up with the best infrastructure in enhancing this revolution.

---

[34] Opt cit.

[35] A Green Paper on E-Commerce for South Africa; Co-ordinated and compiled by the Department of Communications Republic of South Africa November 2000, at pp. 64

[36] This position is notable under section 2 of Canadian Law (PIPEDA), section 5 of ESIGN Act (USA), section 8 of UETA and Article 9 (1,2 and 3) of the Electronic Signature Law of the People's Republic of China

CHAPTER THREE

A LEGAL ASPECT OF ELECTRONIC SIGNATURES.

3.1. INTRODUCTION.

The importance of signatures in any transaction can hardly be overstated. A signature constitutes an authenticity on any record through which any legal obligation is born. With the advent of E-Commerce, online transactions are at climax as billions of people in the world use internet as means of transacting[37]

Therefore, it is the legal requirements that with this technological revolution, there be a well framed system for authenticating the same, to which E-Signatures is referred to as the only tool. Hence this chapter intends to show the legal aspect which is the basis for a well legal framework for electronic signatures in Uganda.

3.2. INTERNATIONAL POSITION IN E-SIGNATURES

Under international level E-Commerce is well framed with a number of international organisations[38], national or regional entities[39] and Non-Government Organisations[40] heavily involved in E-Commerce. Also there are laws, such as the UNCITRAL Model Law on Electronic Commerce (1996), UNCITRAL Model Law on Electronic Signatures (2001),the Supplement to the Uniform Customs and Practice for Documentary Credits for Electronic Presentation ("eUCP") revision of 2007 and European Directives which are given time to time. Specifically speaking of E-Signatures in international level is framed by the UNCITRAL Model Law on Electronic Signatures[41]

---

[37]Statistics drawn from Internet World Stats athttp://www.internetworldstats.com/stats.htm, visited on 20August, 2012, *Also* Daudi Mwita Nyamaka: Electronic Contracts in Tanzania: An Appraisal of the Legal Framework, November 2011, at pp. 75

[38] UNCITRAL, OECD, WIPO, ICAN, The Hague Conference on Private International Law, WTO

[39] European Union (EU), Council of Europe, APEC, United States, Colombia, Tunisia, Australia and Argentina.

[40] Global Business Dialogue on E-commerce (GBDe), Internet Law & Policy Forum (ILPF),Consumers International, Electronic Privacy Information Centre (EPIC) and the International Chamber of Commerce(ICC)

[41] The Model Law was approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000. It took effect in 2001.

Article 1 of the Model Law gives the scope for its application and it is when electronic signature is used in commercial activities. Article 6 effect that if there is requirement of signature, such is met by data message. The Model Law provide further for an E-Signature to be reliable it must meet four requirements, such that first, the data creation must link with the signatory. Second, the data creation was insole control of the signatory. Third, any alteration of electronic signature, made after signing, must be detectable. And fourth, where the purpose of the signature is to provide for the integrity of the underlined information, then the alteration must be detectable, respectively.

Under the eUCP[42] it requires for electronic records to be capable of authentication both as to identity of the sender and that the message has not been intercepted, read or tempered with during transmission. The eUCP provides further that if electronic record cannot be authenticated, it is deemed not to have been presented. Under eUCP authentication can be achieved by the use of an electronic signature. The eUCP's definition of electronic signature is broader enough to cover any form of encryption technology, including the public and private keys provided by the Certificate Authorities (CAs), keys which are used to lock electronic records. As electronic signature is defined to mean;

"A data process attached to or logically associated with an electronic record and executed or adopted by a person in order to identify that person and indicate that person's authentication of the electronic record"[43]

3.3. UGANDA ICT POLICY

The main policy guiding developments in the ICT sector in the country is the National ICT Policy[44]. The policy objectives and strategies to achieve the mission and realize the vision for this policy, a number of policy objectives have been identified covering the sub sectors of Telecommunications, Broadcasting, Postal, Information Technology, Information Management Services as well as other crosscutting and emerging areas.

---

[42] The Uniform Customs and Practice for Documentary Credits for Electronic Presentation ("eUCP")supplements the Uniform Customs and Practice for Documentary Credits (2007 Revision ICC Publication No. 600,) ("UCP") in order to accommodate presentation of electronic records alone or in combination with paper documents

[43] The Uniform Customs and Practice for Documentary Credits for Electronic Presentation ("eUCP")supplements the Uniform Customs and Practice for Documentary Credits (2007 Revision ICC Publication No. 600,) ("UCP") in order to accommodate presentation of electronic records alone or in combination with paper documents

[44] 2003 Uganda National ICT Policy Framework.

Uganda's ICT policy was approved by parliament in 2003 to provide Government guidance on ICT issues. Lack of an overall ICT Policy and poor harmonization of initiatives had previously led to the random adoption of different systems and standards, unnecessary duplication of effort and waste of scarce national resources on the one hand, and lack of strategies for the utilization of ICT as a driving force for national development on the other. The policy articulates ten main focus areas in harnessing ICT in Uganda; Application of ICT in Uganda, investment in ICT Industry, strategic ICT leadership, ICT infrastructure, ICT industry, human capital, legal among others.

From the above scenario, we can conclude that the required environment for the development of ICTs in Uganda is in place. This includes policies, legal and regulatory frameworks, political will, and public participation. However, implementation has been hampered by several challenges. What is important is that these challenges are being acknowledged.

Given the prevailing political will, a number of important projects have been implemented since 2007. These include the development of the national fibre optic backbone and the expansion of rural access programmes. These are positive signs that suggest Uganda is keen to achieve the targets outlined in the WSIS Plan of Action[45] (WSIS, 2003).

It is important and indeed incumbent upon government that civil society, the private sector and other stakeholders are able to fully participate in the planning and rolling out of ICT for development projects. In this way, the most effective and sustainable steps can be taken to ensure that basic communications services of acceptable quality are accessible at affordable prices and at reasonable distances by all people in Uganda, one may come to the conclusion that ICT technology in is at its initial stage, and that the implementation of the National ICT Policy with regards to electronic commerce, specifically in providing legal basis for electronic signatures is not yet seriously taken into account despite the enactment of the electronic Signature legislation.

3.4. THE UGANDAN LEGAL BASIS FOR E-SIGNATURES.

It is well established out of findings and as per inquiries of this study that Uganda unlike other Sub-Saharan African countries, has got specific legislation dealing with matters relating to

[45] World Summit on the Information Society (WSIS) Plan of Action 2003

electronic commerce, and so as to say in case of electronic signatures. This development has come out after vigorous findings and Reports that the Law Reform Commission of Uganda put into consideration in regards to enactment of laws to regulate internet related transactions, the idea which got rooted from the ambit of the UNCITRAL Model Law on Electronic Signatures (2001), National ICT Policy, 2003 as well as the influence from her neighbors, like Tanzania, Namibia and Mauritius whose system with regard to electronic commerce is far reached as I submit. Thus this study has come up with the findings adout the Uganda's electronic signature legislation which regulates electronic commerce, including the legal basis for electronic signature.

3.4.1 THE RELATED LAWS TO E-SIGNATURES AND THE INFLUENCE OF ELECTRONIC COMMERCE IN UGANDA

It is the findings of this study, as contended above, that with the advent of ICT and the adoption of a new means of transacting, this development has left lacunae in the Uganda legal frameworks in aspect of legal basis for authenticating electronic record, and in this context the reference is made to the lack of a well legal framework for E-Signatures. This study has therefore discover to the effects that, regardless that Uganda has no specific legislation to that effect but it has some related laws, which are to be discussed hereunder;

POLICIES, STATUTES AND LAWS, ACTS, AND REGULATIONS

The current status of ICT in Uganda has been influenced by various Policies, Statutes, Laws, Acts and Regulations, passed and enacted in the last ten years. These have, among other things, brought about liberalisation in the various social/economic sectors that have led to impressive economic performance. The more relevant ones are briefly described here below:

The Communications Act,[46] The Telecommunications Policy was enacted in 1996. The main objective of the policy was to increase the penetration and level of telecommunication services in the country through private sector investment rather than government intervention.

Rural Communications Development Policy[47]**,** The main objective of the policy is to provide access to basic communication services within reasonable distance to all people in Uganda.

[46]The Communications Act, 1997

The Press and Journalist Statute[48], The Statute extended Article 29(1) *(Freedom of expression)* of the Constitution to the print media. It also created the Media Council, the National Institute of Journalists of Uganda and a Disciplinary Committee within the Media Council. The Council is responsible for regulating eligibility for media ownership and requires journalists to register with the National Institute of Journalists of Uganda.

The Electronic Media Statute[49],The Statute created a licensing system, under the Broadcasting Council, for radio and television stations, cinemas, and videotape rental businesses. The purchase, use, and sale of television sets was also to be subject to licensing by the Council.

Applicability of electronic signatures in Court Cases in East Africa.

The tension for admitting electronic records in East Africa has started since 2000 when the wisdom of the High Court of Tanzania was called upon to rule whether electronic evidence is admissible as best evidence in the case of ***Trust Bank Ltd v. Le-Marsh Enterprises Ltd., Joseph Mbui Magari, Lawrence Macharia***[50]

In this case, the court ruled that the electronic evidence is admissible in Tanzania courts and this was a departure from the strict rule of best evidence rule. Again in ***R v. Prof. Costa Ricky Mahalu and Another*** [51] when the court allowed for electronic means be employed in hearing evidence from Italy. These all has further, furnishes for the legislature to amend the Evidence Act which in effect provides for a room for verifying any electronic records, including an electronic signatures.

Banking laws, in this context the reference is to be made with regards to electronic payments system as adopted by mobile companies, like Airtel Money and MTN Mobile Money which are presupposes to be regulated under the Mobile Money Guidelines[52]. Also the Bank of Uganda under its report has proved that banks have adopted the electronic payments system. Mechanisms like the Society for World Interbank Financial Telecommunications (SWIFT) code till December, 2010 about 10 banks operating in ugnada have adopted this system

---

[47] Rural Communications Development Policy, 2001
[48] The Press and Journalist Statute, 1995
[49] The Electronic Media Statute, 1996
[50] High Court of Tanzania Commercial Case No. 4 of 2000
[51] 2006 (Unreported case) who were charged for loss of 2 million Euros during the purchase of an embassy building
[52] Uganda Mobile Money Guidelines of 2013

3.5 CONCLUSION.

The findings of this study on the legal basis for electronic signature in Uganda has the proof that Uganda has the legal framework for e-commerce and e-signature totally, and thus the other related laws, such as the Electronic Media Statute[53],law which also have specific provisions to regulated e-signatures and e-transactions specifically. It is also been noted from the finding of this study that banking laws are in have been reinforced since under today's technological evolution with the adoption of ICT in the world, banks has also resorted to a new system of trading, for instance in uganda's strong legal framework for e-transaction has exposed not only business man but also investor and tourist into hardships. The Bills of Exchange Act[54] for example, provides for Cheque to be in writing and signed by the maker, the effect of which if not so complied with, the person therein cannot be held liable, this position currently in uganda do favors paper- based banking, hence with the advent of ICT revolution a new legal regime need be employed to coup with such global changes.

[53] The Electronic Media Statute, 1996
[54] Bills of Exchange Act 1933

CHAPTER FOUR

ADMISSIBILITY OF ELECTRONIC EVIDENCE IN UGANDA,

4.0 INTRODUCTION.

Presently, most people around the globe use internet to send and receive instant messages, play on line games, download music and movies, share experiences and stories. Thus the internet undoubtedly provides a new vehicle for social connections and networking, linking people together without heed to geographic limitations. Yet despite all these benefits the internet has become a vehicle for criminals to meet their victims.

With increased reliance on technology in everyday life including transacting business, recreation and culture, individuals leave traces of criminal activity, concluded contracts and breaches and other correspondences, on their computer and on line. This raises questions as to the admissibility of such evidence given our present rules of evidence in Uganda under common law and statute.

During discovery, you assemble e-mails with all sorts of seemingly irrebuttable facts, computer records from which you can easily compute damages, and copies of Web pages from various sites that support your theory of the case. Your work is done; you are ready for trial. But are you? Will you be able to get all of that great electronic material admitted at trial? After all, in many cases, even if evidence is accumulated, it may be inconsequential if it becomes inadmissible at the trial.

This Research will therefore discuss whether electronic evidence (particularly e-mails) from internet-based sources, social networks can be admitted under the Uganda's evidence rules. There is little or no local material and case law on this subject. The author will traverse through the well known rules admitting evidence and discuss whether the same can be used in admissibility of electronic evidence. Specific emphasis to relevance, authenticity, and the best evidence rule.

4.1 ADMISSIBILITY AND RELEVANCE.

In order to successfully admit any piece of evidence, electronic or otherwise, a party must overcome three obstacles (1) authentication, (2) hearsay, and (3) the best evidence rule. The starting point was highlighted by Tsekooko, Ag.J (as he then was) in **Uganda vs David Kamugisha & Anor**[55] that the question of admissibility of evidence be it oral or documentary basically depends on whether it was relevant to the issue before court. Otherwise the court record would be filled with all types of evidence which was not sufficiently relevant and they might tend to prolong the trial unnecessarily because of immaterial matter. Among the exceptions was that affecting the credibility of a witness or impeaching his credit. Sec. 4 of the Evidence Act[56]states that only relevant evidence in respect of the existence or non existence of a fact in issue may only be given in any suit or proceedings. Thus all relevant evidence[57]is admissible except as otherwise provided under the Constitution[58] and Acts of Parliament[59].

Would these rules apply directly to electronic evidence? In the neighborhood, Tanzania's High Court has already pronounced itself on the admissibility of electronic evidence which has been followed by an amendment to their Evidence Act[60]. In the case of **Trust Bank Ltd vs Le-Marsh Enterprises Ltd, Joseph Mbui Magari, Lawrence Macharia Commercial Court Case No.4/2000** (High court of Tanzania) court was called upon to rule upon as to whether electronic evidence was admissible as best evidence. Court ruled that the electronic evidence is admissible in Tanzania courts. This was a departure from the strict rule of best evidence rule. The judge stated that the court should not be ignorant of modern business methods and shut its eyes to mysteries of the computer. Subsequent to that decision, the parliament of Tanzania responded by enacting the Electronic Evidence Amendment Act, No. 15 of 2007 which made provision for the admissibility of electronic evidence in courts of law in Tanzania[61]. Ugandan Courts have not

---

[55] [1988-90] HCB 77

Evidence Act Cap 6 Laws of Uganda Revised edition, 2000[56]

[57] Generally, all relevant Evidence is admissible. The most notorious bar to admissibility, of course is hearsay. According to **Osborn's Concise Law dictionary**, 9th Edition, 2001,Hearsay is defined as a statement [either oral or written] other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.

[58] In respect to right to privacy and privileged documents.

[59] The Evidence Act, The evidence (Bankers Books) Act etc

[60] Tanzania evidence Act, 1967 section 40

[61] Electronic Evidence Amendment Act, 2007 can be found in Miscellenous Amendement Act, No. 15 of 2007 available at http://www.parliament.go.tz

come out expressly on the admissibility of electronic evidence. This calls for searching within the existing legal regime to ascertain whether it is admissible[62].

4.2 AUTHENTICITY.

Authenticity in evidence is what the party claims it to be, otherwise it is irrelevant. The test of authenticity is that the proponent must present "evidence sufficient to support a finding that the matter in question is what its proponent's claims. A document may be authenticated based on

> "*appearance, contents, substance, internal patterns, or distinctive characteristics taken in conjunction with circumstances can provide sufficient indicia of reliability to permit a finding that it is authentic*"[63].

Consequently, the standard of authenticating electronic evidence is substantially the same as authenticating other documents[64]. It will usually take the form of testimony by an individual with direct knowledge that the produced evidence is what it purports to be

Authentication or identification should be a condition precedent to admissibility, and is satisfied by evidence sufficient to support a finding that the matter in question is what the proponent claims.

E-mail print outs should be admitted just like ordinary paper evidence with the foundation that the print out is what the person saw on the web after typing in a particular address. Other jurisdictions have so far gone ahead to draft rules of court and statutory rules in respect of admitting electronic evidence. In the American case of **US vs Briscoe, 896 f.2d 1476 at page 1494-95 (7th Cir.1990)**, the federal court stated that a proper foundation for computer records is generally established if the party presenting the computer records,

---

[62] There could be situation where courts in Uganda have admitted such evidence without contest from the opposite party or court cautioning itself on its authenticity.

[63] *The admissibility of electronic Evidence in Cou t*" Cybex initiative. A comprehensive study by Cybex; The Digital forensic company, supported by European Union; http://www.cybex.es/AG2005/news.htm

[64] *"The admissibility of electronic Evidence in Court"* Cybex initiative. A comprehensive study by Cybex; The Digital forensic company, supported by European Union; http://www.cybex.es/AG2005/news.htm

"provides sufficient facts to warrant a finding that records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof and how the records were maintained and produced".

Although authentication is a relatively low standard, in order to prevail, the proponent must be able to successfully show that the content of these social postings, e-mails are attributable to, connected to, and even authored by the defendant through the existence of direct or circumstantial evidence. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form[65].

Of course while the standard for admissibility of electronic records may not be extremely high, care should be taken to ensure that the records will withstand a challenge as to credibility. The authenticity of an electronic document would be stronger if,(a) Nobody but the author would be likely to put this type of information there, (b) The length of time the evidence was on the website; (c) The fact, if applicable that it is still on and can be viewed by the judge.

The party seeking the admission of an e-mail is not required to prove beyond doubt the accuracy of the record, rather, enough evidence required to satisfy the inquiry and shift the burden to the opponents to prove that the computer system is unreliable.

That notwithstanding, there various Challenges to authenticity of electronic documents which include; (a) Where the records are altered, manipulated or damaged after they were created, courts are skeptical of unsupported claims or alterations; (b) Reliability of the computer program that generated the records; (c) Identity of the author of the records- corroborate with circumstantial evidence; (d) There is a possibility of fabricating emails to create evidence of misconduct.

The authenticity of the email as evidence may be challenged by questioning if the evidence was altered or manipulated after they were created and this raises issues relating to the chain of custody of the evidence. However, it is my opinion that at this stage what the party seeking the admission of the document has to do is to establish a prima facie case for admissibility. This could be done by laying the foundation for admissibility. For instance by showing that the

[65] US vs Vela, 673 F.2d 86,90 (5th Cir.1982); US vs De Georgia, 420 F2d 889,893 (11th Cir.1969

internet service providers may be able to retrieve information that its customers posted or emails that its customers sent. Also showing the reliability of the third party service provider in handling the records of the digital evidence. Mere authentication may not be enough. Compliance with the requirements of identification by no means assures admission of an item into evidence as other bars like hearsay, relevance may remain.

4.3 LAYING FOUNDATION FOR THE ADMISSIBILITY OF ELECTRONIC EVIDENCE;

For admissibility, there must be both proper authentication and a basis for admissibility as a non hearsay or under an exception to hearsay rule. If the author of the record (i) admits that he/she authored the document, (ii) admits that the document is true, (ii) is available for cross examination, and there is no hearsay, then the document is admissible. The proponent, however, must establish a foundation that the record was created and stored in such a way as to ensure reliability[66]. Indicia of reliability can include; **(a)** Validation of computer systems to ensure accuracy, reliability, consistent intended performance and the ability to conclusively discern invalid or altered documents; **(b)** Ability to generate accurate copies of records in both human readable and electronic form; **(c)** Protection of records to enable their accurate and ready retrieval throughout the records retention period; **(d)** Limiting systems access to authorized individuals, and use of authority checks to ensure that only individuals who have been authorized can use the system, electronically sign the record, access the operation or device, alter a record or perform the operation at hand.

The requirements of admissibility of e-mails in evidence were classically expounded on by United States of America Magistrate Judge, Judge Paul W. Grimm in the case of **Lorraine vs Markel America Insurance. Co. 2007 WL 1300739 (D.Md. May 4, 2007).** In that case involving contract interpretation issues, Magistrate Judge Grimm refused to allow either party to offer emails in evidence in support of their summary judgment motions. He found that they failed to meet any of the standards for admission under the Federal rules of evidence. The emails were not authenticated but simply attached to their pleadings as exhibits, as has been the common practice. Even though neither party directly challenged the admissibility of the other's

[66] http://www.indianalawblog.com/archives/2007/06/discovery_of_el.html Monday, June 18th, 2007

emails evidence, the court was not in position to consider emails, because no basis had been provided by the parties for admissibility or authentication. In Judge Grimm's words,

"*unauthenticated emails are a form of computer generated evidence that pose evidentiary issues that are highlighted by their electronic medium. Given the pervasiveness today of electronically prepared and stored records as opposed to the manually prepared records of the past, counsel must be prepared to recognize and appropriately deal with the evidentiary issues associated with the admissibility of electronically generated and stored evidence*" [emphasis mine]

He noted that courts have recognized that authentication of electronically stored information may require greater scrutiny than for the authentication of 'hard copy' documents. Judge Grimm further noted that there are many ways in which email evidence may be authenticated with the most frequent ways being, person with personal knowledge, expert testimony, distinctive characteristics including circumstantial evidence.He further laid down five evidence rules which must be considered, to wit;

(a) Is the evidence relevant (does it have any tendency to make some fact that is of consequence to the litigation more or less probable that it otherwise would be).

(b) If relevant, is it authentic (can the proponent show that the evidence is what it purports to be?)

(c) If the piece of evidence that is being offered as evidence an original or duplicate under the best evidence rule, or if not is there admissible secondary evidence to prove the content and,

(d) Is the probative value of the electronic evidence substantially outweighed by the danger of unfair prejudice such that it should be excluded despite its relevance?

He noted that the above rules may not apply to every exhibit offered into evidence. The opinion of US Magistrate Judge Grimm is not only a review of the requirement for admitting electronic evidence under the Federal rules of Evidence, but a practical discussion of some of the technology and documents management issues raised by those requirements such as the indicia of authenticity and data collection techniques. Once a communication (letters, emails, web

pages) is authenticated as having been created by the opposing party, it should be admissible for any purpose as non- hearsay[67]. This should be primarily in the context of admitting e-mails in evidence. This would make a logical sense to extend it to publicly available network websites that are in essence held out as public diary or accessible to those surfing on line.

4.4 EVIDENTIARY WEIGHT OF ELECTRONIC DOCUMENTS.

Even if a record is authenticated and admissible, the court still must decide how much weight it should be accorded. The general rule with respect to authenticity of electronic records is that inaccuracies or suspicions of alterations of the records are an issue for the trial judge of fact to consider when weighing the evidence, not in determining its admissibility.Given that most electronic documents will be admissible for the same reasons as their paper counterparts, it appears that the majority of disputes will not be about admissibility but rather about what weight to accord to such records. So, does the fact that an e-mail record may be altered more easily than a written engender any special concern? Who will have the burden of proof as to reliability? In the American jurisdiction, in the case of **US vs Young Bros, Inc 728 F, 2d 682, 693-94 (5th Cir, 1984)** court rejected an argument by the defendant that computer records are inherently less reliable because of potential software and data entry problems[68]. Thus importantly, it is clear that electronic evidence is not deemed to be inherently less reliable or trustworthy than paper records. Thus in the absence of the specific evidence of tampering, allegations that computer records have been altered should go to their weight, not their admissibility.

4.5 THE EXCLUSIONARY RULE/BEST EVIDENCE RULE.

An oldest dogma of the law of evidence is that a party seeking to rely upon the contents of a document must adduce primary evidence of it[69]. Sections 60[70]and 61[71]and 63[72] of the Uganda's

---

[67] Jon Neiditz; ***"From E- Discovery to E- Admissibility? Lorraine v Markel and What may follow"***, Lord Bissel & Brook LLP. Information Management Practice. Available at http://www.lordbissel/.com accessed on 21st November, 2007, 13:25hours

[68] Similarly in the case of **US vs Glasser, 773 F,2d 1553 (11th Cir.1985)**, computer print outs of transactions relating to mortgage bank accounts were admitted into evidence under the business records exceptions. However, there is no similar legislation in Uganda regulating electronic evidence to incorporate the business records exceptions. Perhaps the new bill in the offing by the Law Reform Commission should consider such provisions

[69] P.B Carter (1970); ***Cases and Statutes on Evidence***, 11th edition, sweet & Maxwell, London, page 629

[70] Sec.60 states that *"The contents of documents may be proved either by primary or secondary evidence"*.

[71] That primary evidence means the document itself produced for inspection of the court.

Evidence Act[73] emphasis this best evidence rule. The perfect and the most common item is the original of the document itself[74]. In the case of **Macdonell vs Evans**[75]Maule.J states that what the best evidence is must depend upon circumstances. Thus when the subject of inquiry is the content of a document, no evidence is admissible other than the document itself except in the cases enumerated under section 64(1) of the Evidence Act[76].The crucial question at this stage is whether printed out emails and other computer records qualify as original to satisfy the test of the best evidence rule. It is my submission that if data are stored in a computer or similar device, any print out or other output readable by sight, shown to reflect the data accurately should be regarded as primary evidence with in the meaning of section 61 of the Evidence Act.

4.6 CONCLUSION;

Creating and securely archiving and retrieving is a trial of the entire electronically stored information management process, from the steps of signing the record all the way through sealing electronically the document are examples of an effective electronic process which may enhance the overall persuasiveness of the hard copy of the electronic contracts and other electronic communications and emails. Emails and similar forms of electronic communications may not be properly authenticated with in the existing framework of rules of evidence in Uganda. Electronic evidence brings a unique baggage to the admissibility equation that we need to think through very carefully. Essentially the appropriate body will have to create a whole body of law to deal with electronic evidence.

---

[72] Documents must be proved by primary evidence except in the cases mentioned under sec.64

[73] The Evidence Act, Cap 6 Laws of Uganda, Revised edition, 2000

[74] See; **Macdonell vs Evans**, (1852) common pleas 21 L.J C.P 141 Maule.J stated that, *"it is a general rule... a party tendering a private document should give the best evidence. Generally the best evidence is the original document, which is primary evidence of its contents".*

[75] ibid

[76] See also; **Prince J.D.C Mpuga Rukidi vs Prince J.D.c Mpuga Rukidi, Supreme Court Civil. App. No. 18/1994** in the judgments of Odoki J.S.C and Oder J.S.C in respect of admissibility of photocopies of documents under section 64 of the Evidence Act.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1. INTRODUCTION

The findings of this study are centered on appraisal of the legal basis for electronic signatures and it's impact on evidence law in Uganda. Therefore, this chapter in upholding the findings above comes with a conclusive remarks and recommendations to the government and stakeholders, who are beneficiaries of e-transactions, as hereunder.

5.2. CONCLUSION

Normally, the real meaning of development is that changes occurs either automatically or brought by forces of something not easily controllable, but which demands for its adherence for better ending. With the ICT development in the world, changes have been noted from individual to government perspectives, as billions of people are using internet or electronic in transacting. The development which is brought by technological changes, which in any society are inevitable. With this technological evolution, different sectors of society's mode of social, economic, political and technological life are in need to be changed incompliance with this global changes. In this aspect the society is in need of changes in legal framework as it regulates every aspect of changes which affect an individual's life, as this study tries to single it out;

> *"Law is the informing principle of society at every stage of development, from the maxim* ***ubi societas ibi ius, ibi ius ubi societas****, meaning where there is society there is law and where there is law there is society, and the law grows with this society, from flint stones to genetic clones, from oral contracts to paper based contracts to cyber contract, law is a governing aspect that must reflect the reality to a particular aspect existing at that particular time"*[77]

This study shows that analyses Uganda's legislation providing provisions for authentication of electronic signatures. Meaning while individual, companies and the

[77] Nyamaka Daudi Mwita: Electronic Contracts in Tanzania **An Appraisal of the Legal Framework,** ADissertation in Partial Fulfillment of the Requirements for the Award of Degree of Master of Laws in Economic Law of Saint Augustine University of Tanzania, November, 2011, at p. 1

governmental institutions in Uganda employ in the use of electronic or internet as means of transacting, the country and stakeholders while about and before testing the sweetness of using cyber system they faces bad fumes even before they open their mouth, to mean that the system in uganda is secured, since it has a well-established legal basis to regulate the same, as this study tries to show.

5.3 RECOMMENDATIONS FOR IMPROVEMENT OF UGANDA'S COMPUTER LAWS.

5.3.1 ELECTRONIC SIGNATURE[78]

Act to be amended to Add Reciprocal Recognition of Foreign CA's and Certificates Issued by Foreign CA's Most international E-commerce laws now provide for various forms of legal recognition of foreign CA's and certificates issued in foreign countries, the ESB fails to do this. This is essential because Ecommerce transactions often straddle international borders. Turkey's Electronic Signature Law is a typical example and can be used as a model (Turkey, 2004).

Assign More Potential Liability to CA's It is unusual in international E-signature law to find as much limitation of a CA's liability as in Uganda. This needs to be changed. Too much responsibility is placed upon the shoulders of the subscriber, and too little responsibility is assigned to the CA. Some of the burden of potential liability should be transferred from the subscriber to the CA. The computer law of the Republic of Vanuatu can be used as a model (Vanuatu, 2000).

5.3.2 ELECTRONIC TRANSACTIONS ACT[79].

Information Technology Courts Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology ("I.T.") Courts should be established as a court-of- first-instance for them. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be

[78] supra
[79] The Uganda Electronic Transactions Act Law No.8 2011

required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of Nepal can be used as a model (Nepal, 2005).

Mandatory E-Government In order to reduce cost and to make governmental functions more convenient for citizens, E government needs to be emphasized and mandated. By established deadlines, governmental departments Journal of Management Policy and Practice vol. 11(5) 27 should begin to convert to provision of online services if possible. In Hong Kong, for example, a substantial number of government services may now be accessed online, e.g., the scheduling of an interview for a visa or the scheduling of a wedding before a public official (Chung, 2003).

Eliminate the Exclusion for Wills The ETB excludes wills from its coverage. The result is that a will is required to be in paper form with a handwritten signature affixed to it in order to be enforceable. This exclusion should be eliminated. Electronically-signed wills should be recognized. There is evidence that the aversion to electronic wills is beginning to dissipate. In 2005, the U.S. State of Tennessee became the first American jurisdiction to recognize the legal validity of a will that is executed with an electronic signature (Ross, 2005).

5.3.3 COMPUTER MISUSE ACT[80].

The following crime should be added to the CCB: Intentional Injection of a Virus Into a Computer System. This crime is especially heinous because of its potential for infliction of extreme damage to the Ugandan economy as well as to the international economy. The punishment should be stringent, as follows: first offense, mandatory ten years' imprisonment, without parole; second offense, mandatory twenty years' imprisonment, without parole; and third offense, mandatory life imprisonment, without parole.

[80] THE COMPUTER MISUSE ACT, NO.2 2011

BIBLIOGRAPHY

Books

ADAM, Mambi (2010) **"ICT Law Book: A Sourcebook for Information &Communications Technologies and Cyber Law"** Mkuki na Nyota Publishers Ltd, Dar esSalaam.

ALAN, Davidson (2009) **"The Electronic Commerce"** First Published 2009, Cambridge University Press

STEPHEN, Mason (2007) **"Electronic Signatures in Law"** 2nd Edition, United States Haywards Health Totell Publication

SCHELLENKENS, M.H (2004) **"Electronic Signatures Authentication Technology from a Legal Perspective"** TMC Asser Press

TURBAN, E (2002) **"Electronic Commerce"** Sweet & Maxwell Publishers,

NDITI, N.N.N, (2009) **"General Principles of Contract Law in East Africa"** DUP, 1stEdn.

RODNEY, R, (2001) **"Guide to Cyber Laws"** Oxford, 1st Edn.

ROSEN, A, (2002) **"The E-commerce Question and Answer Book"** A Survival Guide for Business Mangers, Oxford Press, 5th Edn.

Roy G, (2004) **"Commercial Law"** Penguin, 3rd Ed

SEALY, L S,*et al*, (2009) **"Commercial Law: Text, Cases and Materials"** Oxford Press,4th Edn .London

Paper and Journals

ADAM Mambi (2012) *"Support for Harmonization of the ICT Policies in Sub-Sahara Africa"* Workshop on the SADC Harmonized Legal Framework for Cyber Security Gaborone Botswana 27th February-3rd March 2012

CASTELLANI, L. G (2009) *"Policy considerations on the electronic communications convention"* Sungkyunkwan journal of science & technology law (Seoul)

CORIEN, Prins (2007), E-government: " *A Comparative Study of the Multiple Dimensions of Required Regulatory Change*" Electronic Journal of Comparative Law, vol. 11.3

Dr. MOIRA, Patterson (2001) " *E-Commerce Law*, Session 4b: Info economy issues" Hyatt Hotel, Canberra (Law School of Monash University)

EDWARD, L (1977) "*Law and the Internet"* Regulation Cyberspace

JIANYING, R, *et all* "*The validity of Digital Signatures*" Kent Ridge Digital Labs, 21Heng Mui Keng Terrace Singapore 119613

JOBODWANA, N. Z. (2009) " *E commerce and mobile commerce in South Africa: regulatory challenges* " Journal of international commercial law and technology

JOCHEM, Zaremba (2003) "*International Electronic Transaction Contracts Between U.S and EU Companies and Consumers*" Connecticut Journal of International Law, Spring18.Conn. J. Int'l L. 479

KLODWIG Mgaya (2012) *"Development of Information Technology in Tanzania* "available athttp://www.unu.edu/unupress/unupbooks/ visited on 16/May-2016.

Websites

http://www.ehow.com/facts_6801968_new-hampshire-electronic-signature-law.html,visited 09/05/2016.

http://www.isaacbowman.com/the-history-of-electronic-signature-laws, visited 09/05/2016.

http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta.htm, visited 09/05/2016.

http://www.uncitral.org/english/workinggroups/wg_ec/index.htm, visited 09/05/2016.

http://www.uncitral.org/english/texts/electcom/mlecomm.htm, visited on 20/08/2012http://www. europa.eu.int/comm/internal_market/ , visited 09/05/2016.

http://www.icta.mu/laws/ict_laws.htm, visited 09/05/2016.

http://www.businessinmauritius.com/e_commerce.html, visited 09/05/2016.