The Legality of E-commerce and E- signature Under Ethiopian Law

Tigist Ashenafi

A Thesis Submitted to School of Law and Governance Studies

School of Graduate Studies

Presented in Partial Fulfillment of the Requirements for the LL.M Degree (Public International Law Stream)

Advisor:- Professor TilahunTeshome

Addis Ababa, Ethiopia

February 2017

Addis Ababa University

School of Graduate Studies

This is to certify that the thesis prepared by Tigist Ashenafi Assefa, entitled: "*The Legality of E-commerce and E-signature under Ethiopian Law "*and submitted in partial fulfillment of the requirements for the degree of Masters (LLM Public International Law) complies with the regulations of the university and meets the accepted standards with respect to originality and quality.

Tigist Ashenafi

_____

Members of the Examining Committee

Advisor: TilahunTeshome (Professor) Signature ———————— Date ————————

Examiner: Zekareas Kenea (Asso. Professor) Signature ———————— Date ————

Examiner: Tewodros Mihrete (Asst. Professor) Signature ———————— Date ————

ACKNOWLEDGMENT

This research has been accomplished with the help of many people to whom I am indebted. Next to our omnipotent God, I am heartily thankful to my adviser PROF. TILAHUN TESHOME, for his unreserved and timely support in checking, commenting and giving constructive advice all along my activities.

I wish to extend my sincere gratitude to Ato Samuel Fasil and Ato Wubishet Demisse who helped me materially and morally during my study.

My utmost gratitude also goes to my friends Tigist G/Egziabher, Meaza Fikre, Misrak Kifle, Elzabeth Getachew, Sosina Alemayehu,Tseada Fantahun and Rekik Mesfin for their relentless support, love and cooperation in every respect.

I owe special thanks to my parents, whose sincerity and encouragement I will never forget.

Last but not least, the lion share of my thanks goes to my beloved husband EYOB YOSEPH, for his unfailing support, strength, care and love. I offer my regards and blessings to all of those who supported me in any respect during the completion of the research.

Thanks GOD for making it happen!

Acronyms and Abbreviations

ADLI: Agricultural Development Led Industrialization

ATM: Automatic Teller Machine

B2B: Business to Business

B2C: Business to Consumer

B2G: Business to Government

C2B: Consumer to Business

C2C: Consumer to Consumer

CITA: Communications and Information Technology Agency

DECLPD: Draft Electronic Commerce Law Proclamation

E-Business: Electronic Business

EC: European Commission

E-Commerce: Electronic Commerce

ECA: Economic Commission for Africa\

EDI: Electronic Data Interchange

E- Signature: Electronic signatures

EU: European Union

GDP: Gross Domestic Product

ICT: Information Communication Technology

IDRC: International Development Research Centre

INSA: Information Network Security Agency

ISSs: Information Society Services

IT: Information Technology

MCIT: Ministry of Communications and Information Technology

MLEC: Model Law on Electronic Commerce

MLES: Model Law of Electronic Signature

MoST: Ministry of Science and Technology

NGO: Non-governmental Organization

NOC: National Oil Company

OECD: Organization for Economic Co-operation and Development

PADIS Net: Pan African Documentation and Information Service Network

PAEI: Pan African E-commerce Initiative

PK: Public Key

PKI: Public Key Infrastructure

Root CA: Root Certificate Authority

SADC: Southern African Development Community

S&T: Science and Technology

STI: Science, Technology and Innovation

UN: United Nations

UNCITRAL: United Nations Commission on International Trade Law

UNECA: United Nations Economic Commission for Africa

WTO: World Trade Organization

WWW: World Wide Web

Table of Contents

Abstract

The purpose of this study is to assess the existing legislation governing e-communication and storage of information in Ethiopia, which is inadequate or outdated because it does not give recognition to electronic commerce. Ethiopia has not yet set a comprehensive legal framework for e-commerce in general and electronic signature in particular. Ethiopia's e-signature and e-commerce laws are still at draft stage. The research design for this study is a descriptive survey with a critical and analytic approach. The research will describe existing situations in the selected study area. The study revealed that the absence of laws dealing with electronic commerce and e-signature , cause uncertainty as to the legal nature and validity of the information presented in a form other than a traditional paper document. This undermines the prospects for the successful development of e-commerce. Finally, recommendations were made on the current e-commerce and e-signature laws.

CHAPTER ONE

Introduction

1.1 Background of the Study

Today it is believed that the world has turned into a global village. The main reason is that the internet has become a very powerful tool for dissemination of information from one part of the world to another. The internet can be used very cost effectively, very efficiently and very speedily for the transmission of data from one point to another.

The effect of using the internet has changed the way or means of conducting business in different sectors. One may say that trading system all over the world has broadened its dimension. For instance, the internet has paved the way for entrepreneurs to generate ideas and start businesses by identifying the needs of customers through internet's worldwide network. The internet has also created an opportunity for any other kind of trade that involves online education, online information services, computer software, and entertainment products such as games, professional consulting and advertising as well as provision of financial, medical, and technical services.[1]

The internet has dramatically lowered unnecessary expenses and enabled new ways of doing business transactions for various professionals such as engineers, product developers, and managers. [2]These professionals can show their consent to manufacture and design new products more efficiently from thousands of miles away. Consumers also tend to have greater choice and may shop from home from a wide variety of products either from manufacturers or retailers at all corners of the world. In addition to this, they could view these products on their computers, get information about products and services; and order and pay for their choices, all from their living rooms.[3]This somehow initiated people to enter into e-commerce thereby contributing to the

[1] Z A Zainol, "Electronic Data Interchange (EDI) and Formation of Contract: A Malaysian Perspective",1999, *International Journal of Law and Information Technology* , P. 181.
[2] Ibid.
[3] Dr. Nnaemeka Ewelukwa, (2013) "Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for E-commerce in Africa", available at, <http://www.acicol.com/__temp/Dr_N.pdf>. Accessed on: June 8, 2015.

transformation of trade. However, there are many kinds of restrictions on how e-commerce is to be conducted across national boundaries. Import, export procedures, restrictions and barriers, exchange control regulations, transport and insurance related issues as well as availability of efficient telecom infrastructure and even political considerations at times hinder e-commerce. E-commerce actually began with the intention of sharing information with business partners and suppliers by larger corporations through creating private networks in the 1970s.[4] This process is known as Electronic Data Interchange (EDI). It is used to transmit any standardized data that smoothed the procurement process between businesses so as to avoid paperwork and human intervention.

The use of the internet in Ethiopia began in 1993 when the UN Economic Commission for Africa (UNECA) established a store and forward e-mail service called PADIS Net (Pan African Documentation and Information Service Network) which connected daily via direct dial calls to Green Net's internet get way in London. [5]At that time as there was no alternative, the facility was heavily used by international organizations and NGOs, some academics, individuals, and private companies. At its peak, the service had about 1,200 users.[6]

Currently, though e-commerce lies at an infant stage in the country, it is growing rapidly. The 2014 World Internet Status declares that Ethiopia has had only 1.9% internet penetration.[7]However, the world status of 2015 shows that the 1.9% internet penetration reached 3.7%.This report also indicates that the number of internet users increased from mere 10,000 in the year 2000 to 3,700,000 in 2015.

As the number of internet users in Ethiopia grew, companies have shown their interest to transact online despite the absence of online payment system and efficient delivery system for items

---

[4] <http://www.uky.edu/classes/MKT/390/slides/whatec.ppt>. Accessed on: July 15, 2015.

[5] International Telecommunication Union, "Internet from the Horn of Africa: Ethiopia Case Study", 2002, available at, <http://www.itu.int/osg/spu/casestudies/ETH-cs1> . Accessed on: July 15, 2015.

[6] Ibid.

[7]< http://www.statista.com/markets/413/e-commerce >. Accessed on: June 10, 2015.

brought online. Local players like mekina.net and delala.com have recently been joined by et.kayimu.com.[8]

From a legal perspective, businesses may be reluctant to get involved in an electronic transaction if the present legal framework fails to offer necessary guarantees for a trustworthy and secure online commerce. This could be achieved through the use of electronic signatures because technology makes it easier to obtain user signatures on key documents. Electronic signatures play significant roles in national and international commerce. Worldwide, many companies rely on e-signature technology in their day- to- day business transactions. If a government is unable to give guarantee to the legality and validity of electronic contracts and online transactions, then e-commerce would most likely come to a standstill. That is why lawmakers in many countries have made it a priority to enact national e-signature legislation.

In Ethiopia, E-commerce related laws and regulations pertaining to matters such as privacy protection and electronic signature have yet to be adopted. However, owing to increase in the number of internet and e-commerce users in Ethiopia, economic changes associated with globalization will inevitably put pressure on the government to take care of this kind of transaction by promulgating laws related to e-commerce and e-signatures.

1.2 Statement of the Problem

In a very short period of time, the internet has dramatically changed the way business is done and will continue to do so. As a result, e-commerce has become one of the essential components of current international trade and has greatly changed the ordinary way of trading.[9]

E-Commerce in its simplest sense may be defined as trading electronically. It offers potential benefits through lowering the cost of business transactions, especially in the service sector, reducing communication costs, lowering printing and publishing costs as well as improving the flow of information and providing rapid access to a wide variety of information sources.[10]

---

[8] Lusy Kassa, "NOC Launches 15m Br Electronic Card Fuelling System": Addis Fortune Magazine, 2015, *available* at, <http//www.Addis fortune.net/articles/ethiopias-tech-industry emerges/>. Accessed on: June 11, 2015.

[9] UNCTAD, E-commerce and Development Report, New York and Geneva, 2015.

[10] Schneider and Gary P., Electronic Commerce, 7th ed., Thomson Learning , 2007, P. 219.

Nowadays, e-commerce is an integral part of modern way of living. Hence, it has come to be pressing economic, political and social agenda. Even though so many day-to-day activities are carried out through cyberspace, the current regulatory laws and administrative frameworks cannot regulate the newly emerging global way of doing business. As stated above, e-commerce involves the process of buying and selling goods and services electronically. Accordingly, records are processed, stored and maintained in digital media. Traditional commerce involves paperwork and meets requirement of writing and signature. As opposed to traditional commerce, the conditions, and nature of e-commerce does not have to fulfill the requirements of writing and signature as is enshrined in current laws of Ethiopia. In addition, the significance of these electronic records from legal point of view is not addressed, especially their contractual effects.

The problem which this research intends to address is related to the existing laws governing communication and storage of information in Ethiopia, which are inadequate or outdated because they do not give recognition to electronic commerce. Ethiopia has not yet put in place a comprehensive legal framework for e-commerce in general and electronic signatures in particular. Ethiopia's e-signature and e-commerce laws are still at draft stage.

Unlike the conventional transactions, e-commerce depends on well-equipped infrastructure in the area of ICT, more reliable legal and regulatory framework, and widespread awareness among the public and business persons; and this naturally leads to smooth transactions. The law in Ethiopia, however, is not in tune with the modern information technologies, and hence, cannot protect the interests of those who rely on them. For instance, the provisions of the law of contracts in the Cvil Code were designed in a way that support oral and paper-based transactions.

For this reason, the absence of laws dealing with electronic commerce on its own, causes uncertainty as to the legality and validity of the information presented in a form other than the conventional paper documents. This undermines the prospects for the successful development of e-commerce.

Different country's national laws including Ethiopia's stipulates formal validity requirements like for the deal to be in written form or register the contract with a court or notary or having it attested by witnesses. When the transaction is commercial, the provisions clearly stipulates the responsibilities of the parties and the effects of the contract. For instance, Article 1723 of the Civil Code of Ethiopia requires any contract related to immovable property to be in a written

form and be registered before a court of law or a notary. In the same way, Article 1724 of the Civil Code stipulates the same requirement for contracts made with a public administration.

According to Articles 1727 a contract which requires a written formality, needs to be supported by a special document containing content of a contract signed by parties to the contract and at least two witnesses. In addition, Article 1728 of the Civil Code, obliges parties in the contract to affix their hand written signature or a thumb mark, if they are unable to write. However thumb mark of an illiterate or a blind person thumb mark never binds unless it is made in the presence of notary, registrar or a judge acting in discharge of his duty.

Therefore, no provision is given as to the acceptability of electronic signatures. This is mainly due to the fact that e-commerce and e-signature were non-existent at the time of its promulgation in 1960. The inadequacy of the current law, therefore, naturally creates problems in doing business at the international level.

Another instance which disregards e-signature is stipulated under Article 734 of the Commercial Code of Ethiopia. According to this article, any declaration or promise made on negotiable instruments must be accompanied by the signature of the person bound by such declaration or promise.

1.3 Objective of the Study

1.3.1 General Objectives

The general objective of the research paper is to examine the adequacy of the existing e-commerce and e-signature legal framework in Ethiopia and the problems associated with it. It also asks whether the traditional rules of contract and signature apply effectively to modern e-commerce transactions or whether consumers are adequately protected when they engage in online transactions.

The research is also conducted in view of enhancing awareness, cognizance of the subject, and to initiate the regulatory body to take further action.

1.3.2 Specific Objectives

A) To trace the existence of any electronic signature and e-commerce law in Ethiopia;
B) To identify constraints, challenges and problems of inadequate electronic signature and e-commerce laws for online transactions;
C) To examine whether the already existing laws fulfill the standards of international and regional e-commerce and e-signature legal instruments;
D) To suggest the best electronic transaction method for Ethiopia;
E) To identify and seek solutions to solve legal issues related to the use of electronic signatures and electronic commerce until market practices in that new area are better established.

1.4 Research Questions

The paper gives answers to the following major research questions:

A) Are there e-commerce transactions in Ethiopia? If yes, is there any law governing the transactions?
B) Does Ethiopia have e-commerce and e-signature law?
C) Is it necessary that Ethiopia introduces an e-commerce and e-signature regulatory system today? If yes, how should it be designed?
D) Are there problems in connection with e-commerce transactions in Ethiopia? If there are, what should the regulatory solutions look like?
E) If a law is necessary, what legal matters or issues and interests in relation to e-commerce and e-signature need to be identified, recognized and addressed by such law?
F) What is the experience of other countries in this regard?
G) What will be the role of the regulating agency?

1.5 Scope of the Study

The focus of this paper is electronic commerce and electronic signature. The paper covers global and sub-regional initiatives to govern e-commerce transaction. Particularly, it defines and delimits the scope of e-commerce and e-signature. Besides, the paper investigates and presents if there exists sufficient condition to issue laws with respect to e-commerce and e-signature in Ethiopia. Accordingly, the experience of other countries will be used to demonstrate the issue.

Moreover, the researcher tries to explore and present the practice in Ethiopia in relation to e-commerce as stated in the above paragraph of this section. Consequent to the finding of facts, conclusions will be drawn and recommendations will be made.

1.6 Limitation of the Study

Clearly, e-commerce is not being fully utilized and much needs to be done. Hence, there are hardly enough books to explore to have a clue on the status of e-commerce in Ethiopia. This is best witnessed in relation to laws or regulations of e-commerce and e-signature of Ethiopia. Therefore, World Wide Web (Internet), interviews and books written on general e-commerce and e-signature issues are used as sources of information.

1.7 Significance of the Study

The paper is meant to contribute to the development of e-commerce and the regulation of affairs to this kind of transaction. Thus, it is intended to serve as an initial stepping ground to promote safe and sound e-commerce practice in Ethiopia. Besides, it can also be used as an input for the promulgation of a law in relation to e-commerce and e-signature; which in turn warrants efficient and secure e-commerce, which Ethiopia will undoubtedly step into. In addition, it is believed to serve as a source for further research in the area.

1.8 Methodology

The type of research that will be used in this study is qualitative research. The research design for this study will be a descriptive survey with a critical and analytic approach. The research will describe existing situations in the selected study area, analyzes major issues and makes sound recommendations.

The research will employ qualitative methods to clarify concepts, characteristics and descriptions to demonstrate implications of the issue under question. Data which will be presented in the study was obtained through interview with concerned government organs as well as experts in the area and from secondary sources. Secondary data will be collected through review of relevant literature at international and regional level. International and national laws on electronic commerce and signature and other important legislative documents for the issue will be assessed thoroughly. Research reports and publications on the issue have also been considered.

1.9 Organization of the Study

The research is organized into five chapters. The first chapter deals with the introductory part of the research in which background of the research, statement of the problem, objectives of the study, significance, scope and limitation of the study as well as organization of the paper discussed. Chapter two defines e-commerce and e-signature, explains the different types of e-commerce and identifies the challenges and importance of e-commerce. It also introduces the methods, authentication and criteria for e-signature. Chapter three incorporates the legislative part of e-commerce and e-signature from the experience of UN, EU and SADC. Chapter four discusses Ethiopia's experience and nature of Ethiopian e-commerce and the e-signature legislative environment. Finally, conclusion and recommendation are presented in chapter five.

CHAPTER TWO

Literature Review

2.1 E-commerce

In its simplest sense, commerce is a business transaction which involves two or more persons who meet with the intention of buying and selling goods and services one with the obligation of delivering the product or rendering the service and the other with the duty of paying the price. Compared to e-commerce we may name this kind of transaction as a conventional commerce. This kind of commerce demands contracting parties or physical agents or legal representatives to appear physically. In other words, all its dimensions are physical. All business transactions are performed offline.

On the contrary, if someone does some kind of business online using a computer network that would come under e-commerce it may be not only about goods but also about services. Most people, however, use the word e-commerce and e-business interchangeably. E-business is a broader form of e-commerce or one may say that e-commerce is part of e-business. E-business includes servicing customers, collaborating with business partners and carrying out transactions electronically with an organization. [11]It mostly focuses on internal matters of a company. With this, the definition part of e-commerce will continue.[12]

2.1.1 Definition of E-commerce

E-commerce is believed to have equal underpinning in different areas of study- technology, business, law and policy study. That is why various definitions were given by different scholars, organizations and national laws. A generally accepted definition of the term e-commerce is an emerging concept that describes the process of buying and selling or exchanging of goods, services and information via computer network including the internet. Black's Law Dictionary

[11] Efraim Turban, David King, Dennis Viehland & Gae Lee, Electronic Commerce: A Managerial Perspective, 4th ed., Prentice Hall, 2006, P 16.
[12] Ibid, P 56

defines e-commerce as "*the practice of buying and selling goods and services through online consumer services on the Internet*."[13]

This definition seems to restrict e-commerce to buying and selling through the internet. Kalakota and Winiston suggested that e- commerce has the following perspectives:

- Communication- the delivery of information, products or payments by electronic means.[14]
- Business process- application of technologies towards automating transaction and workflows.[15]
- Service- contributing to reducing costs and at the same time as increasing speedy quality of delivery.[16]
- The buying and selling of information and products online. The information should have some commercial bearing or should be for the provision of the facility, some service to individual customers.[17]

In addition to the above perspectives other researchers added the following dimensions:

- Learning- is an enabler of online training and education in schools, universities and other organizations including businesses.
- Collaborative- the framework for inter- and intra-organizational collaboration.
- Community- provides a gathering place for community members to learn, transact and collaborate.[18]

In 2009 Organization for Economic Co-operation and Development (OECD) defined e-commerce as:

"The sale or purchase of goods or services conducted over computer networks by methods specifically designed for the purpose of receiving and placing of orders." [19]The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or

---

[13] Bryan A. Garner, *Black's Law Dictionary*, rev. 9th ed.,St. Paul, Minn, 2009.

[14] Kalakota R. & Whinston A.B, Electronic Commerce: a Manager's Guide, Addison Wesley, 1997, P.67.

[15] Ibid ,P.67.

[16]Ibid, P.67.

[17] Ibid ,P.68.

[18]Efraim Turban, David King, Dennis Viehland & Gae Lee, Supra note at 11, P.21.

[19] Paulos Biruk, The Legal Architecture for E-commerce in Ethiopia: Lesson from the EU Experiences**,** Anchor Academy, 2015, P 115.

services do not have to be conducted online."[20] E-commerce may broadly be defined as the exchange of information across electronic networks and any stage in the supply chain whether within organization, between business and consumer or between private and public sector rather paid or unpaid.[21]

An even broader description comes from the European Commission (EC), again in 1997, which argued:

"Electronic commerce is about doing business electronically. It is based on the processing and transmission of data, including text, sound and video. It involves both products and services; traditional activities and new activities". It encompasses many diverse activities including electronic trading of goods and services, online delivery of digital content, electronic fund transfers, electronic share trading, electronic bills of lading, commercial auctions, collaborative design and engineering, online sourcing, public procurement, direct consumer marketing, and after-sales service.

A Pan African E-commerce Initiative, sponsored by the Economic Commission for Africa (ECA) and the International Development Research Centre (IDRC), in 2001 adopted the definition of the European Commission.

In summary, e-commerce is not restricted to the buying and selling of goods it rather includes pre-sale and post-sale activities across the supply chain.

2.1.2 Types of E-commerce

E-commerce may take different forms based on the method of transaction or based on the parties involved in the transaction or by the degree of digitalization. Based on the method of transaction e-commerce can commonly be classified as follows:

- Business to Business (B2B): in this kind of electronic commerce, transactions take place between organizations. [22]Both the parties are full-fledged businesses, corporations, and organizations instead of individuals. [23]This is the most popular type of e-commerce.

[20] Ibid.

[21] Coppel Jonathan, "E-commerce Impact and Policy Challenge", OCED, Volume 36, 2000, P.43.

[22] Schneider and Gary P.,Supra note at 10, P 38.

[23] Ibid.

Companies using B2B e-commerce relationship observe cost saving by increasing the speed, reducing errors and eliminating manual activities.

- Business to Consumer (B2C): retailing transactions with individual shoppers. The sellers are business organizations and the buyers are individuals. [24]It involves customers gathering information, purchasing physical goods that are tangible such as books or consumer products or information goods or goods of electronic material such as an e-book.[25]
- Consumer to Consumer (C2C): consumers sell directly to consumers. [26]There is no organization involved. These are individuals who are sellers and buyers. Some organizations may play the role of intermediaries, but they are not actually involved in the transaction itself. Eg. Some auction sites.[27]
- Consumer to Business (C2B): individuals who sell products or services to organizations and those who seek sellers and conclude a transaction.[28]
- Business to Government (B2G): e-commerce between companies and the public sector. It refers to the use of the internet for public procurement, licensing procedure and other government related operations.[29]
- Intra-business (organizational) e-commerce: all internal organizational activities involving exchange of goods, services or information, selling corporate products to employees, online training and cost reduction activities.[30]
- Peer-to-peer e-commerce: this kind of e-commerce enables internet users to share files and computer resources directly without having to go through a central web server. On the other hand, no intermediary is required.[31]

Based on the degree of digitalization e-commerce may be classified as:

---

[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Kenneth C.Laudon, , E-commerce: Business, Technology, Society, 3rd ed., Prentice Hall, 3rd ed., 2007,P.92.

- Pure e-commerce- in this kind of e-commerce everything is online. All the dimensions are digital in nature. Pure online (virtual) organizations. [32]
- Partial (hybrid approach) e-commerce- it is the combination of traditional and pure e-commerce.[33] Either one of or both of the parties are physical.

2.1.3 Benefits and Limitations of E-commerce

The benefits of e-commerce are multi-dimensional. One can see it from the organization's angle or from the consumer's angle or from the society's angle. Organizations that use e-commerce would have a chance to have an international marketplace. They can find customers all over the world. Operational and telecommunication costs will be saved because e-commerce transactions do not need printing of paper-based documents and the price of internet is much cheaper than other means. It also saves time.[34]

From consumer's angle, e-commerce provides full access at any time. Consumers can easily order products and services online and also effect payment online. In addition to this, they would be given chance to choose and they can compare prices. Improved delivery process is also one of the benefits of e-commerce to consumers. From the society's angle, e-commerce enables more flexible working practices, which provides a quality of life for a whole host of people. It also enables the society especially those who live in rural areas and developing countries to enjoy and access products, services, information and other people which otherwise could not be so easily available to them. It also facilitates delivery of public service.[35]

Besides, e-commerce has technological and non-technological limitations. From the technological angle, there is no universal standard for quality, security, reliability and communication protocols. It is difficult to integrate electronic commerce software with some existing applications and databases. Internet accessibility is also still expensive and/or inconvenient. From the non-technical angle, consumers raise the issue of privacy and security because frauds are increasing at an alarming rate, consumers still get confused with the paperless transactions and they also want to touch and see the products.[36]

---

[32] Ibid.
[33] Ibid.
[34] Rana Tassabehji, Applying E-commerce in Business, Sage publication, 2003, P.29.
[35] Ibid, P. 33.
[36] Efraim Turban, David King, Dennis Viehland & Gae Lee, Supra note at 10, P.21.

2.2 E-signature

Using electronic signature instead of traditional paper and ink to seal important deals with customers has become a normal phenomenon. This is because it will save transacting parties from printing a copy of documents and avoids the hassles of trying to get multiple persons at the same place and at the same time.

Most people believe that a reasonably well-designed process supported by a solid technology can actually reduce risk relative to the traditional process. [37]It turns out; it is more about process and workflow & less about technology. But in meeting the admissibility and compliance challenges of the effective e-signature process the appropriate deployment of technology is essential. [38]This is why it is important to understand the process and how the technology is deployed.

Currently, an e-signature could have the same legal standing as a traditional signature given that it could be proven the person is one who said who he is and what his intention was at the time of signing. Therefore, the contract principles can still be applied to contracts signed using electronic signatures and documents including some of the disclosures delivered through electronic means.

E-signature is broader than a digital signature. It can be as simple as clicking "I agree", typing a name or even by saying "I agree". [39]In the case of digital signature certificate service providers use a system that encrypts transactions when one of the contracting parties sends them and decrypts them when they arrive at the destination. [40]Since each encryption code is unique at that the decryption is as well.

This way, it will be difficult for hackers to intercept this transaction for their own good. The problem lies in the identification of the users. Using password is often most convenient both for business and users though it could easily be compromised. Since people use the same password for many applications, the hacking of the database of a minor forum may have a great impact on the overall security of the system.

---

[37] Stephen E. Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United Stats: Promotion of Growth in E-Commerce with Enhanced Security", 2005, Richmond Journal of Law and Technology, Volume 11 Issue 2 Articles 3, P.91.
[38] Ibid.
[39] Ibid.
[40] Ibid.

2.2.1 Definition of E-signature

In its literal meaning, signature can be defined as a symbol or a name or a thumb mark which represents a person who signs. Signature assures the source and it can be used to authenticate writing. In addition to this, it binds the individual who signs in the document as per the contents in it. E-signature is, therefore, signing a document using the aforementioned methods and others through an electronic means to authenticate writing.

Different laws define e-signature differently. For example, the UNCITRAL model law on electronic signature in its article 2(a) defines electronic signature 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 the data message."[41]

In our legal system, the National Payment System Proclamation No.718/2011 and a Proclamation to Provide for the Establishment of the Ethiopian Commodity Exchange number 550/2007 gave the exact same meaning the UNCITRAL model law provided on electronic signature. The draft electronic signature law of Ethiopia provides no different definition to it. Besides, the laws of other countries provide definition to e-signature. For example, the 1999 European Union Electronic Signature Directive defines two types of electronic signature as simple e-signature and advanced e-signature.

Article 2 of the Directive broadly defines e-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."*[42] The reason for this kind of definition is to encompass all kinds of technologies which will be created in the near future.

The other type of e-signature included in this directive is advanced e- signature. This kind of e-signature is defined as an *"Electronic signature which is uniquely linked to the signatory, capable of identifying the signatory, created using means that the signatory can maintain under*

[41] UNCITRAL Model Law on Electronic Signatures (2001), article 2(a).

[42] Directive 1999/93/EC, article 2 (1).

his sole control and which is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."[43]

Different authors also give a definition for e-signature from different perspectives. For example, Dr. Abdulhadi defines e-signature as:

"..... any technique based on an electronic media that is used or adopted by a single party with the intention of linking itself to or authenticating a document, thus fulfilling all the functions performed by a handwritten signature." [44] This shows that e-signature doesn't have any lower status but on equal footing with paper and ink.

To sum up, electronic signature encompasses wider issues and it can shortly be defined as signing one's data or document in an electronic means using a different kind of technology. Therefore, e-signature may take a number of forms like a digital signature, a digitalized fingerprint, a retinal scan, a pin number, a digitalized image of a handwritten signature that is attached to an electronic message or merely a name typed at the end of an e-mail message.[45]

2.2.2 Methods of E-signature and Authentication

In doing business, the critical issue would be trust and security whether on the paper-ink market or in the case of online transaction. By avoiding these risks electronic signature and authentication plays an important role in e-commerce. This definitely creates trust and confidence among the transacting parties. This will be done through different methods of e-signature. There are four major methods of e-signature and authentication.

Biometrics

It is one method of e-signature which involves a unique physical attribute of a transacting party. This method of e-signature is used to identify a person through photograph, iris scan, fingerprint, voice pattern or a digitalized image of a handwritten signature normally attached to an electronic data.[46]

---

[43] Ibid, Article 2 (2) (a-d).

[44] Abdulhadi M. Alghamid, The Law of E-commerce, E-contract, E-business, Aunhor house, 2011, P.18.

[45] Ibid.

[46] Stephen E. Blythe, at Supra note 35, P.111.

DNA, retina, hand or facial geometry, facial thermogram, ear shape, body odor, blood vessel patterns, gait and typing patterns are also some of the traits that may be used in biometrics.[47]In using a biometric device the first thing we will do is capturing a biometrical sample either in digital form or a biological feature of an individual. Secondly, the biometrical data will be extracted from the sample. The final step would be creating a reference template. To identify one's biometrical sample or to verify the authenticity of communications originated from that same person we need to compare his or her biometrical data with those stored in the reference template.[48]

Scanned e-mail signature

This kind of signature consists of text, picture or a hybrid. Most of the e-mail portals have a tool for users to create and use a signature. [49]Nevertheless, business entities prefer these forms of "authentication" in the interest of ease, expediency, and cost-effectiveness of communications. [50]Most individuals use this method of signature in using outlook.

Passwords, codes, and hybrid methods

Passwords are the most common way of signing an online communication. It can also be used as a method of controlling access to any private information by a third party. Codes have also the same usage as passwords. For instance, we use those authentications in our banking transaction, especially in money transfer . The problem lies on the users side. Mostly online transacting parties use the same and familiar codes and passwords like birthdays and names for different transactions which can easily be hacked.

An online customer may also use a hybrid method by choosing two or more methods listed above and below.

---

[47] United Nation Commission on International Trade Law, "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods", 2009, United Nations Publication, P.72.

[48] Ibid.

[49]Ibid.

[50] Ibid.

Digital signature

Digital signing is a special process that is applied to an electronic document. The result of this process is a code that is specified in the document which could be created only by one person so that the signature cannot be copied to other documents. [51]The draft e-signature law of Ethiopia defines digital signature as: "*A means of an electronic signature that uses asymmetric cryptosystem which is uniquely linked to the signatory; capable of identifying the signatory; which is created using a private key that the signatory can maintain under his sole control; and linked to the electronic message to which it relates in such a manner that any subsequent change of the electronic message or the signature is detectable.*"

In this kind of technology, the signatory generates a pair of asymmetrical digital keys namely a public and a private key. [52]The keys normally constitute a large number developed from a cryptographic algorithm. [53]One can give his/her public key to everyone to whom she /he wishes to interact with posting it on their website so that everyone can find it. It is basically used to verify digital signatures encrypt messages and to encrypt messages using one of several different encryption algorithms.[54] It is stored inside a digital certificate.

The second key, a private key, is protected by the key owner physically or cryptographic protection of the key owner. [55]It is basically used to digitally sign messages and to decrypt all messages to be sent to the key owner. A message encrypted using the public key can only be decrypted by the key corresponding a private key. [56] In order to make sure that the public key used to which you are encrypting data is actually the public key of the intended recipient, you could add a digital certificate. The digital certificate is a public key with one or two forms of ID attached. [57]A certification authority, a trusted third party, creates and signs a digital identification

---

[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] International Trade Forum, "Secrets of Electronic Commerce: A Guide for Small and Medium-Sized Exporters", ITC, 2nd ed., 2009, P.64.
[55] Ibid.
[56] Ibid.
[57] Ibid.

certificate, which establishes a link between the signatory and his or her pair of keys so that the signatory cannot later deny the signature.[58]

To sign a document, the key holder creates a message digest, which is a number that summarizes the original information. [59]The message digest is then encrypted with the private key. The encrypted message digest, which can be deciphered by anyone who has the public key, is called a digital signature. [60]Upon receipt of the signed message, the message digest is decrypted and compared with the digest created from the received document. If the two match, then the document has not been altered during transmission. [61]In addition, a match guarantees that the document has been sent by the key holder, and hence authenticates the sender because only the key holder's private key would yield an encrypted message that could be decrypted by the associated public key.[62] All the above encryption process is known as Public Key Infrastructure (PKI). PKI is a two key (Asymmetric) cryptosystem. It is a framework that allows different IT systems to have a high level of information confidentiality, strong data encryption and high level of confidence through authentication of digital signature and digital certificate. [63]PKI encompasses digital certificate and the certifying authority.[64]

To sum up, each e-signature system will need to use multiple methods of identification which makes the whole system an expensive enterprise. Furthermore, the system which will continue needs to be updated with the latest security measures and also requires a properly functioning IT department.

---

[58] Ibid.

[59] Stephen E. Blythe, at Supra note 35, P.119.

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] Ibid.

CHAPTER THREE

Global and Sub-regional Initiatives on E-commerce and E-signature

Regulating the internet is not an easy task. In the past decade, many proposed laws of different nations have been ruled unconstitutional for being too broad and vague.[65] Regulating the internet also raises jurisdictional issues. The internet, unlike broadcasting stations, is worldwide and therefore beyond one's jurisdiction in many cases. In other words, it has no boundaries. No country can claim to own cyberspace.

Another dilemma relates to ways of punishing illegal activities occurring online. The internet hosts a lot of anonymous speeches. Often, authorities have difficulty tracing the source of controversial issues. Is there someone that controls websites and internet service providers? Would it be possible to hold them liable for the millions of things posted online every day?

Regulating the internet has also been hindered by technical difficulties of courts. Technology touches virtually every aspect of human lives and is often affected by laws. If courts cannot grasp how business inventions have changed, they might make decisions that misapply the law due to the misunderstanding of facts about technology.

On the other hand, perhaps ignorance is a blessing in disguise. [66]Some fear that more regulation on the internet by judges and lawmakers could cause more problems. They believe that the more the internet is regulated, the more it gives the government power to control it and limit one's freedom of expression. [67]

People need to trust what is transmmitted over the internet. The gap in trust emanates from the characteristics of e-commerce. There are three characteristics of e-commerce. The much-known characteristic of e-commerce is at a distance. The parties on e-commerce do not make deal around a table. That is why people lose confidence to trust one another. Another characteristic of

[65] Alan Davidson, The Law of Electronic Commerce, 1st ed., Cambridge University Press, 2009, P. 55.
[66] Ibid.
[67] Ibid.

e-commerce is that it is carried out through electronic equipment. Finally, it is conducted at the request of the recipient.

Therefore, inorder to fix problems of uncertainty and insecurity in the area of e-commerce and e-signature, special rules are very important. Such rules may be provided in a variety of legislative texts such as international legal instruments (treaties and conventions), transnational model laws, national legislation (often based on model laws), self-regulatory instruments as well as bilateral and multilateral contractual agreements.[68]Among the transnational model laws the United Nations model law of electronic commerce and electronic signature is well known.

3.1 U.N. Model Laws of E-commerce and E-signature

3.1.1 UNCITRAL Model Law on Electronic Commerce (1996)

One of the most active international organizations in the area of making uniform rules is the United Nations Commission on International Trade Law (UNCITRAL). UNCITRAL was established by the general assembly in 1966 (resolution 2205(XXI) as a vehicle which enables the United Nations to play an active role in reducing disparities in national laws governing international trade that create obstacles to the flow of trade. Its general mandate is to further the progressive harmonization and unification of the law of international trade, and it has come to be the core legal body of the United Nations system in the field of international trade law.[69]

The model law on electronic commerce was adopted by the United Nations in 1996 and the additional article 5 was adopted in 1998. The main purpose of the model law is to provide a uniform model framework for nations to use when they write their e-commerce statutes. It has a profound impact on the evolution of international e-commerce law.[70]

The Model Law on Electronic Commerce (MLEC) has 4 chapters and 17 articles. MLEC is thus a legislative text with the fundamental principles of non-discrimination, technological neutrality

[68] United Nation Commission on International Trade Law, Supra note at 22, P. 29.

[69] UN-General Assembly Resolution 2205(XXI) of December 1966.

[70] Stephen Errol Blythe, An E-commerce Law for the World: The Model Electronic Transactions Act, Xlibris, 2012, P. 12.

and functional equivalence that are widely regarded as the founding elements of modern electronic commerce law. The following are some of the most important principles on which MLEC is based.

The Functional Equivalence Principle

This principle lays out criteria under which electronic communications may be considered equivalent to paper-based communications. In particular, it sets out the specific requirements that electronic communications need to meet in order to fulfill the same purposes and functions that certain notions in the traditional paper-based system - for example, "writing," "original," "signed," and "record"- seek to achieve.[71]

The Principle of Non-discrimination

The principle ensures that a document would not be denied legal effect, validity or enforceability solely on the ground that it is in electronic form. Article 5 of the MLEC states that information shall not be denied legal effect, validity or enforceability solely on the ground that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message. In addition to this, Article 9 stipulates that information in the form of data message can be used as evidence in the same way as a handwritten document.

The Principle of Technological Neutrality

The principle of technological neutrality mandates the adoption of provisions that are neutral with respect to technology used. In light of the rapid technological advances, neutral rules aim at accommodating any future development without further legislative work. In short, it is all about equal treatment of different technologies. Besides formulating the legal notions of non-discrimination, technological neutrality, and functional equivalence, the MLEC establishes rules for the formation and validity of contracts concluded by electronic means, for the attribution of data messages, for the acknowledgment of receipt and for determining the time and place of dispatch and receipt of data messages.

[71] The UNCITRAL Model Law on Electronic Commerce, (1996), Article 6-8.

However, the model law is only a framework and nations must supplement it with detailed rules and regulations to achieve its implementation. One of the model's notable weaknesses is the omission of consumer protections: nations adopting the model statute should consider enactment of additional provision to achieve those protections.[72]

3.1.2 UNCITRAL Model Law on Electronic Signature (2001)

The Model Law of Electronic Signature (MLES) was adopted by the United Nations on July 5, 2001. The main purpose of the model law is to foster the understanding of electronic signatures and the confidence that certain electronic signature techniques can be relied upon in legally significant transactions. Moreover, by establishing with appropriate flexibility a set of basic rules of conduct for the various parties that may become involved in the use of electronic signatures (i.e. signatories, relying on parties and third-party certification service providers) the Model Law may assist in devising more harmonious commercial practices in cyberspace.[73]

The Model Law on Electronic Signature (MLES) has 12 articles. The MLES also incorporates the fundamental principles of non-discrimination, technological neutrality and functional equivalence like the model law on e-commerce. This Model Law recognizes both digital signatures based on cryptography (such as public key infrastructure - PKI) and electronic signatures using other technologies.

The MLES contains provisions favoring the recognition of foreign certificates and electronic signatures based on a principle of substantive equivalence that disregards the place of origin of the foreign signature.[74]

Still the model is a framework and nations must supplement it with detailed rules and regulations to achieve its implementation.

---

[72] UN-General Assembly Resolution 2205(XXI), Supra note at 29.

[73] UNCITRAL Model Law on Electronic Signatures, (2001), Preamble.

[74] Ibid, Article 12.

3.2 Regional and Sub- regional Laws of E-Signatures and E-commerce

3.2.1 The EU E-Commerce Directive

On May 4, 2000 the European Commission (EC) adopted a directive on central legal aspects of electronic commerce. The main objectives of the directive include removing obstacles to cross-border online services in the EU internal market (free movement of services), providing legal certainty to business and citizens, offering a flexible, technically neutral and balanced legal framework and enhancing competitiveness among European service providers.[75]

The e-commerce directive employed the so-called "country of origin" rule.[76]Pursuant to Article 3 of the directive, each member state must ensure that the Information Society Services (ISSs) provided by a service provider on its territory complies with its national law provisions applicable to e-commerce (the so-called "coordinated field").

The directive, as mentioned in Article 1(4), does not address international private law questions, except the issue of material law which is applied in judging whether a certain information service provider is lawful. The country of origin rule is applicable only within a certain field, as defined in article 21.[77]

The e-commerce directive outlines the framework of e-commerce in the international market, establishing harmonization law regarding a number of issues that are regarded as central to e-commerce. In addition to the general provisions, the directive deals with establishment and information requirements, commercial communication, contracts concluded by electronic means, the liability of the service provider, implementation and final provisions.[78]

3.2.2 The EU E-Signature Directive

Contracting on the internet raises questions with respect to the identification of the contractors. Identification is an issue both for the service recipient and the service provider. The contracting

[75]Directive 2000/31/EC, Preamble.

[76] Lucas Bergkamp, European Community Law for the New Economy, Antwerp, 2003, P. 31.

[77] Ibid, P. 42.

[78] Dennis Campbell and Susan Woodle , E-commerce: Law and Jurisdiction, 1st ed.,Springer, , 2002, P 68.

parties will often not be able to verify beyond doubt the person with whom they are contracting. In addition, problems arise with respect to the authentication of communications. Both issues are addressed through the use of e-signature.[79]

Directive 1999/93/EC of December 13, 1999, sets forth a general framework for e-signature to be implemented by the member states before July 19, 2001. The e-signature directive established a common framework for the development of e-signature law in the EU and thereby promotes the legal recognition of e-signature and their greater use. Only an advanced signature (supported with a qualified certificate and created by a secure private key) is considered to be fully and legally equivalent to a handwritten signature, but all e-signatures are potentially admissible into evidence in court.

The directives make a distinction between "e-signatures" (which are regular electronic signatures) and "advanced e-signature" and attributes different legal value to each other. A regular e-signature is very broadly defined as "data in electronic form which are attached to or logically associated with other electronic data which serve as a method of authentication". [80]No specific requirements are laid down in the directive, as it merely seeks recognition by the member states of e-signatures that are already used in the IT sector and which standards have been adopted by this sector. An advanced e-signature, on the other hand, is defined as "an e-signature which meets the following requirements: (1) it is uniquely linked to the signatory. (2) it is capable of identifying the signatory,(3) it is created using means that the signatory can maintain under his sole control, and (4) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable." [81] Both types of e-signature have legal effectiveness and are admissible in court as evidence. However, advanced e-signatures which are based on "secure-signature-creation device" must be accorded exactly the same legal consequences as handwritten signatures. In other words, both types of e-signatures are admissible as evidence, but courts have broader discretionary authority in assessing the probative value of regular e-signatures.

---

[79] Ibid, P.72.

[80] Ibid.

[81] Directive 1999/93/EC, Article 2(2).

3.2.3 SADC Model Law on Electronic Transactions and E-commerce

The Southern African Development Community (SADC) is a regional inter-governmental organization that comprises 15 member states: Angola, Botswana, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Tanzania, South Africa, Seychelles, Swaziland, Zambia, and Zimbabwe. It was established in 1992 with the objective of advancing regional integration and poverty eradication within Southern Africa through economic development and ensuring peace and security.[82]

SADC drafted a model law on electronic transactions and e-commerce in 2012. The model law has seven parts and 37 sections. The Model Law provides a tool that the Member States can use to create a more secure legal environment for electronic transactions and e-commerce. It also seeks to enhance regional integration and has adopted the best practices and collective efforts of Member States to address the legal aspects of e-transactions and e-commerce.[83]

This Model Law addresses the scope of application of key concepts and proposes neutral definitions. The legal recognition and effects of electronic communications are addressed. Clear rules for electronic transactions are adopted. E-commerce issues such as the attribution of electronic communications and electronic signatures, and the admissibility and evidentiary weight of electronic evidence are addressed. The obligations of online suppliers are–outlined. These include the type of information made available to consumers on the information system where such goods or services are offered, and a consumer's right to a cooling-off period, review of a transaction, withdrawal from a transaction, and the performance, correction or cancellation of a transaction for goods and services. Lastly, service providers' liability is addressed.

Like the UNCITRAL model law on e-commerce and e-signature, the SADC model law adopted the principle of technological neutrality, functional equivalence, and non-discrimination.

However, the SADC model law is in a better position compared to the UNCITRAL model laws. One of the model's notable strong points is the attention it gave to consumer protection. Like other model laws the model law is only a framework and nations must supplement it with

[82] Treaty of the Southern African Development Community, Article 5.

[83] SADC Model Law on E-transactions and E-commerce, Preamble.

detailed rules and regulations to achieve its implementation. Nations adopting the model statute should consider the enactment of additional provision to achieve those protections.

Chapter Four

E-commerce and E-signature Legality in Ethiopia

4.1 Introductory Remark

As discussed under chapter one it has become evident that cyber space is the daily route for communication and business activities across the globe. Thus, information society and information economy have become the major issues of the day. It's obvious that the internet and related technologies play a decisive role in bringing progress to a country's economy. In this regard, Ethiopia could be no different. The government has been making effort allocating massive budget and setting information communication technology as one of the national economic and social goals.

Accelerating international information flow has, therefore, created an opportunity for the government and the people to have knowledge of current affairs and utilize the same for the attainment of democracy and good governance goals set by the country. [84]

Consequently, several business processes were automated, decisive institutions were interlinked with information communication technology and several citizens are playing a vital role by taking part in the cyber environment. [85]The fact that businesses like electronic education, electronic healthcare service, electronic trade and similar services are expanding in the country shows the extent and the importance of information and information technology. There are also an increased number of individuals and businesses whose activities and daily routines are dependent on the internet. Especially, electronic banking (mobile banking, internet banking, ATM services, etc), electronic governmental services, electronic trade and similar services are given more emphasis as these play significant role in terms of the socio-economic development of the country. [86]As stated in chapter one, delala.com, merkato.com, like National Oil Company

[84] Halefom Hailu and Kinfe Micheal,"The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media", 2015 ,*Mizan Law Review*, Vol. 9, pp. 144.

[85] Ibid.

[86] Ibid.

(NOC) have launched an electronic card fuelling system.[87] The system will enable customers to use all of NOC's services, including filling gas, purchasing lubricants and liquefied petroleum gas, car washing service, as well as shop at NOC marts.[88]

In addition to this, insurance companies are also on the verge of introducing online insurance underwriting. United Insurance Company S.C (UNIC) has launched an online insurance sale as of January 1, 2017. [89]Clients can purchase insurance policies online by transferring payments from their account to company. The company has made various policies available online including travel insurance, motor third party insurance, and funeral insurance. [90]

There is also a trend in transformation of banking activities by way of internet and mobile banking as well as the increase in the use of ATMs. It has been quite a while since the Ethiopian Airlines introduced online ticketing and booking services.

However, the current legal requirement of writing, signature and originality which is incompatible with the electronic system is a barrier for those online services. Regarding e-banking transactions, the current regulatory system of banks could not effectively address problems and regulate the business in such a way that promote the task of efficient oversight supervision for smooth and sound e-banking business.[91]

Compared to other countries, Ethiopia's utilization of information communication technology is said to be at a low level. [92]However, it is showing rapid growth. Utilizing this sector with due efficiency has many challenges. Amongst these challenges is the risk of communications and data accuracy due to interception as well as denial and falsification of relationships and data. Traditional practices can also become challenges for the proper use of the advantages generated by the cyber environment. For instance, several provisions of the country order certain

[87] Lusy Kassa, Spra note at 8.

[88] Ibid.

[89]Addis Fortune Magazine, "United Insurance Launches Online Insurance Sales", 2017, available at, <http//www.Addis fortune.net/articles/ethiopias-tech-industry emerges/>. Accessed on: February 11, 2017.

[90] Ibid.

[91] Paulos Biruk, at Supra note 19, P 66.

[92] Ibid.

documents to be attested by the signature of the concerned parties and duly attested in writing and some documents required to be in the original version.

Therefore, technological advancements that need to be of assistance could be applied in this regard. We shall look at the significance and the need for introducing e-commerce and e-signature legislation with a view to filling gaps in terms of technology.

4.2 The Need for Reconsideration of the Existing Laws

Currently, the cyber environment is becoming a chosen way of communication in the world of commerce. However, most of the working laws in the country are formulated by taking documented trade, civil and administrative relationships; thus it is unable to entertain the new business methods. Amongst the legislations most of them impose an obligation so that they could be in written form and duly signed. For instance, the nation's Civil Code states that certain contracts such as those on immovable property, administrative contracts, and long-term contracts shall be written and signed.[93] Article 2003 of the code states that a contract cannot be orally proved or presumed when it is expressly prescribed by law that it must be in written form. In addition, a written agreement has greater weight when it comes to dispute resolution in a court of law. For instance, Article 2005 states that a written document is conclusive evidence.

Moreover, certain agreements/engagements require due registration with the concerned authority in addition to the requirement of being duly written and signed. For instance, the Acts and Documents Registration Proclamation states that documents that shall be authenticated and registered in accordance with the appropriate law shall not have legal effect unless they are authenticated and registered.[94]

In this regard, the main issue that must be addressed is that, if these legislations require a special format for concluding an agreement, how could business relationships requiring electronic method meet this condition? Unless there is a method to provide a system for registering electronic documents, their legal effect shall be unpredictable; the parties engaged in the transactions remain uncertain about the method as to how to proceed with their engagements.

[93] The Civil Code of Ethiopia, Article 1723-1725.

[94] Authentication and Registration of Documents Proclamation, Proclamation No. 922/2015, Article 9.

Therefore, there are several conditions forcing the preparation of legal frameworks to revise the existing laws and formulating new ones. Creating a favorable legal system for the implementation of electronic trade and e-government service provision is, therefore, necessary.

With regards to e-commerce and e-signature, there are no laws in the country except for the Ethiopian Commodity Exchange proclamation No. 550/1999, the National Payment System Proclamation No. 718/2003 and the Proclamation to Provide for a Warehouse Receipts System No. 373/2003. These are pioneer legislation to have given legal recognition for electronic signature and electronic documents. But their scope of application is quite limited to the extent of failing to give cover other than just a legal recognition.

Apart from this, they are not designed in a manner that could avert the above-mentioned security threats and fill the legislative gaps.

Both the Ethiopian Commodity Exchange Proclamation Article 2(8) and the National Payment System Proclamation Article 2(11) define electronic signature as: "*data in electronic form, 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 the data message".*

Article 21 of the National Payment System Proclamation states that in the event when the law forces the conclusion of any instrument in writing, the presentation of such instrument in the digital copy is considered acceptable. The Proclamation further states that a digital presentation of such evidence shall be admissible in any court as evidence.[95]

Art. 2(8) of the Proclamation to Provide for a Warehouse Receipts System, defines an Electronic Document as *"a document generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange, electronic mail, telegram telex or telecopy."* Furthermore, Art. 2(17) defines a System Provider as *"a person wherever domiciled who provides services to a licensed warehouse operator in matters pertaining to management, to the provisions of electronic records, and to the setting up and maintenance of*

[95] National Payment System Proclamation, Proclamation No. 718/2011, Article 23.

*computer based systems to manage and record transactions in respect of electronic receipts"***.** According to Article 40 of the Proclamation, Electronic Warehouse Receipts is provided as *"a receipt may be created by means of electronic records and may be issued to a bailer or his transferee by a system provider appointed by the Ministry or its designate in line with procedures to be established for this purpose.*" The Proclamation further states that a duly drawn up warehouse receipt delivered to a bailor shall constitute a valid contract between a warehouse operator and a bailor.[96]

Meanwhile, people are using e-commerce in the absence of a legal framework. Devising a legal framework to protect consumers from fraud and to regulate cyber security on e-commerce security should be prioritized. There must be consumer protection law so that users could put trust in the market. Without prejudice to the same, very many companies and industries could leave the conventional business and join e-commerce operations to escape tax payment since the national law does not consider e-commerce taxation. Consequently, this could inhabit loss of nation's tax revenue.

In general, having no legal framework for e-commerce and e-signature may impede the development of creative works on technology, violation of intellectual property rights and trademarks as well as expansion of unfair competition. It also paves way for the spread of cyber crimes. Besides, it could prevent foreign investors taking advantage of opportunities in the country. The country loses revenue from electronics tax in the long run.

Therefore, the issuing of a full-fledged e-commerce and e-signature law that is geared towards avoiding the hurdles imposed by existing obligatory laws on the development and effectiveness of e-commerce, and other electronic communications with the institutional framework is mandatory.

In addition, there are several economic, political and international push factors which necessitate the enactment of the law at this time. For instance, the promulgation of the law plays a vital role in encouraging the country's electronic trade and enables the country to benefit from it. Amongst the requirements set by the World Trade Organization (WTO) is internationally accepted modern

[96] **Proclamation to Provide for a Warehouse Receipts System**, **Proclamation No. 372/2003, Article** 7(1)**.**

trade system and a reliable banking system. [97]Thus enacting this law will certainly help the country in its endeavor to fully engage in the global trading club. It also assists in the prevention of crimes and safeguarding national security since security issues will be resolved by e-signature laws.

4.3 The State of E-commerce and E-signature in Ethiopia

4.3.1 The Policy Framework

The National Science and Technology Policy was issued for the first time in December 1993. [98]The initiation, drafting, and ratification of the policy took 10 years from 1984-1993.[99]The policy had the following objectives:[100]

- *To build the national capability to generate, select, import, develop, disseminate and apply appropriate technologies for the realization of the country's socio-economic objectives and to rationally conserve and utilize its natural and manpower resources.*
- *To improve and develop the knowledge, culture and the scientific and technological awareness of the peoples of Ethiopia, and promote the development of traditional, new and emerging technologies.*
- *To make Science and Technology (S&T) activities more productive, efficient and development - oriented.*

However, there were some weaknesses that are observed during the implementation of the policy. One of its limitations was that it didn't treat social sciences as one branch of science and technology. In addition to this, the organizational structure of the national science and technology system didn't take into account decentralized government structure. The policy also

---

[97] Halefom Hailu and Kinfe Micheal, at Supra not 83, P 157.

[98]http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SC/pdf/sc_workshop_mombasa_lemecha_en.pdfAccessed on: April 2, 2016.

[99]Ibid.

[100] Ibid.

focuses too much on the public sector and there were no clear distinction between policy directives and strategies.[101]

In 2007 STI policy revision took place. The major reasons for revising the policy were the Ethiopian economy has gone through major transformations from centralized to an open market economy with concomitant political power decentralization whereby regions have legislative, executive and judicial powers over their regional matters designated by the Constitution as falling in their jurisdictions. Secondly, the policy has served for over a decade in which there has been a rapid change in the national socio- economy with the corresponding global advance in the understanding and application of science, technology, and innovation. Lastly, there is a strong need to create national STI capability to benefit from the opportunities for the global advancement of scientific knowledge and technology by strengthening the federal and regional government scientific and technological institutions, the universities and the private sector.

The 2nd revised policy has the following visions:[102]

• *To see Ethiopia become a country where a democratic rule, good governance and social justice reigns, upon the involvement and free-will of its peoples, and once extricating itself from poverty becomes a middle-income economy.*

• *To see the living standard of the people improved through the application of science and technology for sustainable social and economic development.*

Compared to the previous policy, the 2007 revised policy clearly demands the National STI council to be chaired by the prime minister. It also forced the government to upgrade the science and technology agency to ministerial level. The policy stresses that at least 1.5% of the country's Gross Domestic Product (GDP) shall be allocated annually to different STI activities in all sectors.

Ethiopia introduced new science, technology and innovation policy and strategy in 2012 which focuses mainly on implementing the Agricultural Development Led Industrialization (ADLI) strategy.[103] The STI policy states, among other things, devising a system of learning, adapting

[101] Ibid.

[102] The FDRE Science, Technology and Innovation Policy, January 2007, P.5

[103] The FDRE Science, Technology and Innovation Policy, February 2012, P.3

and utilizing as well as disposing of imported technologies in order to meet national demand. In this regard, import effective and appropriate foreign technologies and creation of capabilities of adaptation and utilization of these technologies in manufacturing and service providing enterprises have been identified as one strategic focus area of the policy with the following specific objectives:[104]

- *Establish and implement a coordinated and integrated general governance framework for building STI capacity.*
- *Establish and implement an appropriate national Technology Capability Accumulation and Transfer system.*
- *Promote research that is geared towards technology learning and adaptation.*
- *Develop, promote and commercialize useful indigenous knowledge and technologies.*
- *Define the national science and technology landscape and strengthen linkages among the different actors in the national innovation system.*
- *Ensure implementation of STI activities in coordination with other economic and social development programs and plans.*
- *Create a conducive environment to strengthen the role of the private sector in technology transfer activities sustainably.*

4.3.2 Administrative Framework

It is obvious that, on top of the STI policy, several institutional and regulatory frameworks are required in order to realize e-commerce and e-signature. The STI policy is implemented by the Ministry of Science and Technology (MoST) and other respective government bodies.

The current Ministry of Science and Technology (MoST) is a governmental institution that was established for the first time in December 1975 by Proclamation No.62/1975 as a commission. The commission had been entrusted with registering and maintaining readily accessible reference documents of research interest.[105]

---

[104] Ibid.

[105] www.most.gov.et, Accessed on: April 15, 2016.

Recently, the Ministry of Communications and Information Technology is the principal government organ in charge of ICTs in general. It has the powers and duties to facilitate the creation of institutional capacity for the effective implementation of information technology development policy.[106] It also initiates policies and laws in ICT areas. The MCIT also sets and implements standards to ensure the provision of quality, reliable and safe ICT services.[107] The Ministry is, therefore, the principal policy organ concerning ICT issues. Recently, the Ministry issued draft e-commerce law which is not yet put into effect. Each regional state has, however, its own Communications and Information Technology Agency (CITA) entrusted with implementing on the ground laws, policies and standards on ICTs adopted at the federal level.

The Ethiopian Information Network Security Agency (INSA) is a parallel organ with statutory powers to formulate national policies, laws, and standards to ensure the security of information and computer based key infrastructure and oversee its enforcement.[108] In addition, the agency supervises the production and distribution of cryptographic products, necessary requirement and utilization system, develop public key (PK) infrastructure and serve as Root Certificate Authority for the implementation of these activities, thus these are good steps forward. However, the lack of detailed works and responsibilities makes it difficult for implementation. In addition, there is no legal framework detailing the responsibilities of certificate issuing authorities to launch crypto infrastructure works including digital signature and encryption and the relationship of such authorities with the users and other stakeholders.

Whilst the Ministry is bestowed with the broader mandate in connection with ICTs regulation in general, INSA is specifically mandated to deal with information security. In so far as the initiation of legislation is concerned, the MCIT has so far drafted e-commerce legislation (in cooperation with the United Nations Economic Commission for Africa (UNECA), and INSA has recently drafted e-signature law.

---

[106] Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, Proclamation No. 691/2010 (as amended in 2011), Article 24.

[107] Ibid.

[108] Information Network Security Agency Re-establishment Proclamation, Proclamation No. 808/2013, Article 6(2).

4.3.3 The Legal Framework

4.3.3.1 A Draft Proclamation on E-commerce

The draft e-commerce law is drafted by the Ministry of Communications and Information Technology and it is expected to be approved by the Parliament soon. The draft e-commerce law recognizes and facilitates, in its preamble, that the exchange of data messages and other communications in electronic form in Ethiopia; and provide legal ground for the appointment and certification of an authority. It also takes cognizance of the fact that the laws presently in force in the country are not in tune with the rapid technological changes and are not sufficient to accommodate the electronic form of transaction. To address the problems faced so far, it provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, which involve the use of alternatives to paper-based methods of communication and storage of information and primarily targets in facilitating electronic filing of documents with the government agencies in Ethiopia. Facilitating the use of electronic technology by reducing uncertainty regarding the legal effect of information that is in electronic form or that is communicated by electronic means is also the other objective of the Proclamation.[109]

The Draft Electronic Commerce Law Proclamation (DECLP) contains 27 detailed provisions with five parts. The first part defines different terminologies and shows the recognition of 'party autonomy' principle. According to the Proclamation, as between parties involved in generating, sending, receiving, storing or otherwise processing electronic records, any provision relating to electronic records, signatures and contracts may be varied by agreement.[110]

Similar to MLEC the draft Proclamation incorporates fundamental principles of non-discrimination, technological neutrality[111] and functional equivalence.[112] Article 5 ensures that a document would not be denied legal effect, validity or enforceability solely on grounds that it is in electronic form. In addition, Article 9 of the draft Proclamation states that electronic

[109] Draft E-commerce Law Proclamation, Preamble.

[110] Ibid ,Article 4.

[111] Ibid ,Article 6.

[112] Ibid ,Article 8.

documents can be used as evidence in much the same way as data messages. This implies the recognition of non-discrimination. The same applies to e-signature. Part 3 of DECLP talks about the liability of network service providers. Pursuant to articles 11 and 12 of the DECLP, a network service provider will not be liable for any civil or criminal acts under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on the making, publication, dissemination or distribution of such materials or any statement made in such material; or the infringement of any rights subsisting in or in relation to such material. A network service provider is defined as a person "who delivers processing, storing, hosting, presenting or communicating services."[113]

In part 4 of DECLP detail provisions in the area of e-contracts are incorporated. Article 13 of the draft Proclamation gives a choice for contracting parties to express their offer and acceptance through electronic means. In addition, a contract formed by electronic means will not be denied of validity and enforceability on the sole ground of an electronic record.

As regards e-contracts formation, the DECLP addresses two important issues. The first was the question of validity, i. e, whether a contract can be validly concluded between parties using the Internet or other modern electronic communications technologies. The draft law is drafted in a way of achieving this goal, and it resolved uncertainties regarding validity of electronic agreements by granting a legal recognition of 'electronic records'.[114]

The second addressed issue pertains to problems regarding time and place of dispatch. These issues are important in the law of contract generally and in e-contracts in particular, because they help to allocate risks between the parties and determine whether an offer can still be revoked. The place of dispatch is also significant because a contract may have to comply with certain requirements of that law.

Article 16 of the draft law provides that "Unless otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information system

[113] Ibid, Article 10,

[114] Ibid, Article 13(2).

outside the control of the originator or the person who sent the electronic record on behalf of the originator."

The DECLP further elaborates where and when data messages may be regarded as having been dispatched or received. The Article provides that:[115]

1. Unless otherwise agreed to between the originator and the addressee, the time of receipt of an electronic record is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving electronic records, receipt occurs: at the time when the electronic record enters the designated information system; or if the electronic record is sent to an information system of the addressee that is not the designated information system, at the time when the electronic record is retrieved by the addressee; or

(b) if the addressee has not designated an information system, receipt occurs when the electronic record enters an information system of the addressee.

2. Unless otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business

3. Sub.2 shall apply notwithstanding that the place where the information system is located may be different from the place where the electronic record is deemed to be received under subsection

4. For the purposes of this section:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) If the originator or the addressee does not have a place of business, reference is to be made to the usual place of residence; and

(c) "Usual place of residence", in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.

[115] Ibid, Article 16.

Part 5 of DECLP deals with online consumer protection. Article 18 of the DECLP stipulates several rights of online consumers and obligations of suppliers of goods or services through electronic communications. Suppliers are responsible for providng an extensive list of information to consumers and are liable for any damage suffered by a consumer due to supplier's failure to utilize a secure payment system. Article 21 of the DECLP also protects online consumers from unsolicited commercial communications. However, this alone will not protect consumers transacting online. The nation should work on an independent legislative document on consumer protection. The last part is miscellaneous provisions.

As stated previously in chapter three and in this chapter, in addition to other things the very demanding point of regulating e-commerce is solving the issue of jurisdiction and taxation. However, not a single provision is incorporated in the DECLP about these issues. This is a huge gap in the draft Proclamation.

4.3.3.2 A Draft Proclamation on E-signature

The draft law is aimed at creating a favorable, accelerated, safe and reliable condition in the electronic relation with users/clients, the business community, and the government. Thus, it must be devised in a manner enabling the attainment of the following detailed objectives:[116]

- *Creating reliability within relationships conduct with the internet and related technologies.*
- *Fill the gaps observed with the applicable laws related to the internet and similar technology utilization.*
- *Create a favorable legal environment for electronic trade and administration.*
- *Provide legal recognition for digital signature technologies to prevent security risks in the cyber environment.*

The proclamation comprises lots of detailed issues but it mainly focuses on the following:-

Regarding the provision of legislative acknowledgment to e-signature and digital signature especially as well as electronic documents and data:

[116] Draft Proclamation to Provide for Electronic Signature, Preamble.

As it is noted above, the primary purpose of the Proclamation is to fill the gap that resulted from the absence of full-fledged regulations in the existing laws related with electronic message exchange and e-signature and their legislative effect and acceptance. Hence, the draft Proclamation gives due attention to e-signature apart from the fulfillment of text and signature formalities required by different laws. In relation to this, although there are varieties of e-signature and other expected to be developed as the technology continues to grow, it is difficult to enact laws for each and every sort of e-signature. The law in principle allows users to use any type of e-signature depending upon their choice and interest by providing to all e-signature types.

However, due to the fact that e-signature that employs asymmetric cryptosystem requires a specialized technology, regulatory system, and institutional set-up a significant portion of the draft Proclamation deals with a digital signature. Thus, the draft proclamation pays more heed towards digital signature amongst other types of e-signatures. It also clearly states requirements to be met.

Regarding the structure of crypto structure

In order to make the digital signature functional four inter-related components are necessary. These are a technical solution, crypto infrastructure, a package of the legal regulatory system and institutional set-up. [117]In a situation where one of those is lacking, digital signature and its favorable grounds created by the cyber world cannot be utilized in a secured and trusted manner. Therefore, one of the core issues to be addressed by the daft Proclamation is what the package of legal regulation should look like. In this regard, there are three options from the international experience- hierarchical structure, horizontal structure and mixed structure. Although all those working systems have got their own merits and demerits, the most widely used one is the hierarchical structure which the draft Proclamation has taken into consideration. Accordingly, the structure of the crypto infrastructure would have a root certifying authority that could undertake policy and regulatory activities as well as, under the authority; there are certifying agencies that would avail the services to be provided by the infrastructure to users.

[117] Dennis Campbell and Susan Woodle , at Supra note 77,P 82.

Crypto Code Administration

Crypto helps in creating encrypted password service and digital signature (identification of participants, checking data authentication). These services have various purposes and are administered by various policies. Crypto requires several management controlling mechanisms. On the one side, the draft Proclamation enforces certificate issuing agencies to establish key escrow and key recovery of crypto keys. On the other hand, keeping digital signature passwords of certificate issuing agency or installing recovery system would not have any business and security benefits. Therefore, it is proclaimed in the law that the certification bodies cannot have a backup of digital signature passwords or recovery system and it shall only be kept in the hands of the beneficiaries.

The crypto infrastructure is the prime activity to be mentioned in relation to preventing electronic risks and create reliability in the cyber environment. This infrastructure, being part of e-government strategy, is reaching completion and it is anticipated to provide several businesses and governmental services via electronic method and implement electronic trade in a safe and reliable manner. As the national PKI construction is decisive for providing the services identified by the strategy, it is amongst the top priority projects to implement the strategy. The objective of the infrastructure, as stated on the strategy, is to identify and assure the true identity of the actors in the electronic business, assure data or service accuracy, provide non-repudiation of all relationships in the service, and maintain confidentiality. This infrastructure cannot be complete by itself. No statement is made as to how the infrastructure must be implemented and what sort of technical requirements and working procedures are required.

Scope of the law

The draft Proclamation is designed in a manner that may be applied to all electronic message exchange. There is a range of e-signatures with different degree of safety and security. Participating parties can choose their e-signature based on their interest. As far as it is not stipulated in other laws, participating bodies can agree on which type of electronic signature they want to rely on. The draft Proclamation also shows that it is not possible to enforce digital or e-signature in principle.

In the draft Proclamation, in the definition of terminologies part, article 2(13), root certificate authority means the legally authorized body entitled to execute duties and responsibilities under article 10. Under article 9, information and networking security agency is mandated to serve as a root certificate.

As discussed earlier the Ministry of Communications and Information Technology is the principal government organ in charge of ICTs in general. However, INSA is the root certification authority. In relation to which governmental institution need to be Root CA, taking into consideration the nature of the work, the administration capability, the cost it requires, legal support and ability to cope up with future technologies, INSA is chosen as a Root CA.

Therefore, the reason the Agency is executing its duty under root certificate authority is that:

- The Agency shall work as Root Certificate Authority and policy institution as well as to regulate cryptographic products and their transaction, set necessary criteria and develop operating procedures, develop and implement cryptography infrastructure.
- The Agency is working by taking the national responsibility for crypto infrastructure as owner and it is empowered to develop and install crypto infrastructure.[118]
- The sector involves complex security issues which are the responsibilities of the Agency.
- The Agency is in a better position in terms of technology and human resource in relation to administering the infrastructure, safeguarding the security, preparing standards and supporting certificate agencies.

Root Certificate Authority will be established legally: highest level of trust will be put upon it and will carry out regulatory activities. Whereas the detailed responsibility listed under the draft Proclamation is kept, Root Certificate Authority is responsible for licensing certificate bodies, supervising the service and systems of certificate bodies, ensuring the safety and trust of cryptosystem and prepare standards, guideline, and working procedures that certificate bodies should follow.

[118] Supra note at 104, Accessed on: April 15, 2016.

Punishment Standard

In addition to the substantive issues, the Agency is working on incorporating punishment standards for violations of the draft Proclamation. In standardizing the punishment, different countries laws and different proclamations have been considered as inputs. For instance, a person who fails to submit the relevant documents and materials as referred to in Article 34 or submits false records shall be punished by rigorous imprisonment from seven to twelve years and fine from sixty thousand to one hundred twenty thousand Birr. The same punishment also applies to Certificate Authorities when they fail to submit the relevant document and material to Root Certificate Authority. Different penalties are also stipulated in the miscellaneous part of the draft e-signature law.

The draft Proclamation, however, contains a number of limitations including its failure to deal with all types of e-signature but confines itself to a particular form.

Chapter Five

Conclusion and Recommendations

5.1. Conclusion

Information and Communication Technology (ICT) is a ground-breaking tool in modern day socio-economic and political affairs as well as day-to-day activities of humans. From a business viewpoint, it enables various actors in commerce to get access to information easily and timely, and helps them make informed decisions. The Internet as an ICT tool and, flowing from it e-commerce, has greatly bridged the time within which transactions are concluded, thus reducing costs and increasing profit-making.

E-commerce is the basic and contemporary concept that embraces a complex amalgam of technologies, infrastructures, products and services. It describes the process of buying, selling, transferring or exchanging products, services and information through computer networks, principally the internet.

Successful use of ICTs, however, depends on, inter alia, a legal framework to support electronic transactions. Ethiopia, as many other jurisdictions, has encountered legal issues with respect to e-commerce activities. This study has examined the existing regulatory framework in Ethiopia regarding e-commerce and e-signature. It has analyzed the current statutory rules and the draft e-commerce and e-signature laws.

There is lack of suitable legal and regulatory framework for e-commerce and e-signature. Ethiopian current laws do not accommodate electronic contracts and signatures. The country has not yet enacted legislation that deals with e-commerce including enforceability of the validity of electronic contracts and digital signatures.

Most laws related to signature are limited to issues outside the realm of electronic world. The current regulatory system on signature could not effectively address problems and regulate the business in such a way that promotes the task of efficient oversight and supervision for smooth and sound e-commerce practice. The soon to be enacted draft e-commerce and e-signature laws only serve as part of the legal solution to myriad legal issues.

Both e-commerce and e-signature can only operate effectively if the physical telecommunication infrastructure in Ethiopia is improved and the regulatory framework is standardized. Apart from domestic problems hindering the development of e-commerce, the thesis analyses other legal initiatives aimed at creating an environment for promoting and regulating the development of e-commerce and e-signature at global and regional levels. The analysis comprises two perspectives, namely, a global outlook (representing efforts made by United Nations agencies, especially UNCITRAL) and a regional viewpoint, which was further sub-divided into the perspective of developed region (the EU) and developing region (SADC).

From these perspectives the study identified how the various global initiatives such as the Model Laws, Directives and frameworks, could be used to solve problems in domestic legal regimes.

The global perspective is further intended to identify rules that could facilitate trans-border transactions and establish a basis upon which domestic legal regimes could be harmonized to accommodate technological developments. Overall, the study argues that if e-commerce is to flourish, states must strive to establish a global regulatory environment that provides certainty and predictability for e-contracts. In addition, they must seek to promote trust and confidence among the businesses.

Needless to state, the Internet has revolutionized communication and/or connection among peoples all over the world. The Internet has also come to play a crucial role among business communities globally. People have relied on internet networks to exchange business-related information thereby curbing necessary expenses which might occur in the process of transactions. In due course, the move evolved into e-commerce in the 1970s as corporations began to share information with one another.

In advanced economies, stock exchange and a number of companies have been engaged in conducting transactions using computer networks. Nowadays, very many companies conduct sales through e-commerce reaching customers in many countries around the world. However, in Ethiopia the practice is yet undeveloped. In other words, business activities are carried out in a traditional way. Many people lack the knowhow on how to do business electronically. Hence, they prefer to proceed in a traditional manner. Though there are tendencies towards electronic commerce there is no law governing it as a legal means of transaction. Thus, the absence of legal

framework to guide such form of commerce has contributed considerably to its underdevelopment.

Apparently, e-commerce has a number of advantages compared to the traditional one. It is not a must to appear in person in electronic commerce whereas in traditional business physical appearance is unavoidable. Here the government needs to promote the latest form of business. The media is also expected to work towards enhancing awareness of the public in the area. Obviously, it is very easy to transact internationally in e-commerce than in the traditional business. Companies that sell their products electronically have better chance of getting customers all over the world. Consumers could choose the product they need without going to the marketplace thereby saving transportation cost and possible expenses that might occur in their journey. Consumers would not travel to product place if they do not need it. Hence, people need to know where e-commerce takes precedence over the customary form of business so that they could make informed decisions. All aspects of the electronic commerce need to be explained including e-signature and other prerequisites in promoting it.

In this regard, electronic business and electronic commerce is imperative in raising awareness. Many people tend to confuse the former with the latter to the extent of using them interchangeably.

Nevertheless, it should always be noted that e-commerce is one form of e-business. In other words, e-business is broader that it encompasses e-commerce. Regulating activities over the Internet might not be as easy as in the customary business transaction. To ease the task of e-commerce, particularly in Ethiopia, it is worth ensuring consumer rights constitutionally. The only way the government could promote the business is, therefore, through adopting appropriate legal framework. In doing so, it is possible to build trust among suppliers and consumers to transact electronically. If the required legal framework is in place, people wouldn't be uncomfortable to engage in e-commerce even across borders. By the time dissension occurs in the process of transaction trust couldn't always be a remedy. Legal steps have to be there in order to settle conflicts peacefully. E-commerce day –to-day activities need to be governed by special rule and regulation because of its uniqueness.

These days, the cyber space has come to be the preferable route for millions of people around the world to exchange business information and thereby buy and sell goods. Taking this notion into consideration, it is not difficult to assume the vitality of the internet in making progress. Here the government of Ethiopia has to take the necessary steps to enable the country reap the benefit from e-commerce. Failure to promote this latest form of transaction could hold the country back in many ways because those who rely on it could register fast and robust growth. This is all about introducing ICT facilities to commerce. Reliance on e-communications enables the country to disseminate information to reach another corner of the world in a fraction of a second.

In Ethiopia, due attention has to be given to developing infrastructure to speed up the move to creating one political and economic community. Developing nations that couldn't transact electronically at this time may lag behind in becoming part of the global business community in the years to come. Thus, it needs to be promoted as a modern form of business transaction.

As Ethiopia's ICT is still at a low level, much needs to be done to realize its involvement in electronic commerce.

Concerted effort has to be made by engaging concerned public institutions and the media. Overcoming obstacles towards expanding ICT facilities is instrumental in paving the way for better e-commerce practice. Appropriate technologies have to be applied consistently to bring about change in promoting electronic commerce.

Since e-commerce is getting popular from time to time the government of Ethiopia needs to open its doors to adopt a law which enables citizens and the country at large to take part in e-commerce. Those who transact in this way in Ethiopia are doing the business without getting guarantee or rights protection as a consumer. Though they could benefit somehow they would be in a sense of insecurity all the time as the required regulation is not in place. Nothing would be helpful than adopting the legal framework to facilitate conditions for the development of e-commerce and e-signature. Enacting e-commerce law is mandatory even to conform to the latest international business trends. The nation's e-commerce and e-signature draft law should be developed in a way which helps in forging ideal cyber communication among suppliers, consumers and the government.

5.2 Recommendations

To curb legal certainty and create undependable business solution with respect to e-commerce it is necessary to back it up with comprehensive e-commerce and e-signature laws, and other consumer protection laws so that electronic transaction, electronic message, electronic records will have legal effect and admissibility before courts of law.

In order to address the problems identified in this study, Ethiopia needs to be guided by a set of recognized principles as in other countries. The purpose of adhering to such international best practices is to promote and ensure global consistency, alignment and harmonization.

National laws on e-commerce and e-signature based on the UNCITRAL model laws are required in order to ensure that digital signatures can be used with confidence in e-commerce transactions.

The new regulation must give emphasis for the institutional framework. It should establish an institution responsible for maintaining the integrity of the public key infrastructure.

Laws alone will not suffice and thus, law enforcement personnel ought to be adequately equipped with necessary legal, technical and human capabilities and latest trends of e-commerce by subjecting them to regular and special e-commerce and e-signature training courses.

It is also advisable that the law enforcement agencies should promote e-commerce and e-signature awareness and establish effective means to offer tips for safe online transaction and provide timely information relating to e-commerce transactions to the public. It is also recommended that the Ethiopian government has to establish user friendly and accessible reporting mechanisms.

Finally, I recommend the topicality of the issue of e-commerce and e-signature across all stakeholders in general and the academia and civil societies in particular. In this regard, the government should support researches, forums and workshops to be held on the issue.

Bibliography

Books

1. Abdulhadi, M. Alghamid, *The Law of E-commerce, E-contract, E-business*, Aunhor house, 2011.
2. Alan, Davidson, *The Law of Electronic Commerce*, 1st ed., Cambridge University Press, 2009.
3. Dennis, Campbell and Susan, Woodley, *E-commerce: Law and Jurisdiction*, 1st ed., Springer, 2002.
4. Efraim, Turban, David, King, Dennis, Viehland & Gae, Lee, *Electronic Commerce: A Managerial Perspective*, 4th ed., Prentice Hall, 2006.
5. Kalakota, R. & Whinston, A.B, *Electronic Commerce: a Manager's Guide*, Addison Wesley, 1997.
6. Kenneth, C.Laudon, *E-commerce: Business, Technology, Society*, 3rd ed., Prentice Hall, 2007.
7. Lucas, Bergkamp, *European Community Law for the New Economy*, Antwerp, 2003.
8. Rana, Tassabehji, *Applying E-commerce in Business*, Sage publication, 2003.
9. Schneider, Gary P., *Electronic Commerce*, 7th ed., Thomson Learning, 2007.
10. Stephen, Errol Blythe, *An E-commerce Law for the World: The Model Electronic Transactions Act*, Xlibris, 2012.

Articles

1. Coppel, Jonathan, "E-commerce Impact and Policy Challenge", OCED, Volume 36. 2000.
2. Halefom H. and Kinfe M., "The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media", Mizan Law Review, Vol. 9, 2015.

3. International Telecommunication Union, "Internet from the Horn of Africa: Ethiopia Case Study", *ITC*,2002. Available at <http://www.itu.int/osg/spu/casestudies/ETH-cs1>

4. International Trade Forum, "Secrets of Electronic Commerce: A Guide for Small and Medium-Sized Exporters", 2nd ed. *ITC*, 2009.

5. Nnaemeka, Ewelukwa, "Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for E-commerce in Africa", *European Journal of Law Reform*, 2011. Available at <http://www.acicol.com/__temp/Dr_N.pdf>.

6. Stephen, E. Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United Stats: Promotion of Growth in E-Commerce with Enhanced Security", *Richmond Journal of Law and Technology*, Volume 11 Issue 2 Articles 3, 2005.

7. United Nations, "Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures 2001", *United Nations Publication*, 2002.

8. United Nation Commission on International Trade Law, "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods", *United Nations Publication*, 2009.

9. Z A Z,, "Electronic Data Interchange (EDI) and Formation of Contract: A Malaysian Perspective", International Journal of Law and Information Technology , 1999.

Laws and Policies

Domestic

1. FDRE Science, Technology and Innovation Policy, February 2007.

2. FDRE Science, Technology and Innovation Policy, February 2012.

3. Civil Code of the Empire of Ethiopia, Proclamation No. 165, Negarit Gazeta, 1960.

4. Authentication and Registration of Documents Proclamation, Negarit Gazeta, Addis Ababa, Proclamation No. 922/2015, 15th February 2016.

5. Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, Proclamation No. 603/2008, Negarit Gazeta, Addis Ababa, 24th October 2008.

6. Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, Proclamation No. 691/2010 (as amended in 2011), Negarit Gazet, Addis Ababa, 24th January 2010.

7. Information Network Security Agency Re-establishment Proclamation, Proclamation No. 808/2013, Negarit Gazeta, Addis Ababa, 2nd January 2014.

8. Proclamation to Provide for a Warehouse Receipts System, Proclamation No. 372/2003**,** Negarit Gazeta, Addis Ababa, 14th October, 2003.

9. National Payment System Proclamation, Proclamation No. 718/2011, Negarit Gazeta, Addis Ababa, 18th July 2011.

Foreign

1. The European Community Framework for Electronic Signature, 1999, Directive 1999/93/EC available at

https://www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf.

2. Electronic Commerce Directive of the European Parliament and of the Council, Directive 2000/31/EC, available at

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0001:EN:PDF.

3. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, 1999, available at
http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

4. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, 2001, available at http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsige.pdf.

Internet Sources and Other Sources

1. http://www.uky.edu/classes/MKT/390/slides/whatec.ppt.

2. http://www.statista.com/markets/413/e-commerce/

3. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SC/pdf/sc_workshop_mombasa_lemecha_en.pdf

4. http:// www.most.gov.et.

5. Addis Fortune Megazine , available at < http//www. Addis fortune.net/articles/ethiopias-tech-industry-emerges/>.

6. Bryan A. Garner, *Black's Law Dictionary*, rev. 9th ed.,St. Paul, Minn, 2009.

7. Draft Proclamation of E-commerce Law.

8. Draft Proclamation to Provide for Electronic Signature.

9. UNCTAD, E-commerce and Development Report, New York and Geneva, 2015.

10. UN-General Assembly Resolution 2205(XXI) of December 1966 Establishing- United Nations Commission on International Trade Law.