UNIVERSITY OF NAIROBI

SCHOOL OF LAW

MASTER OF LAWS 2012/2013

GPR 699: RESEARCH PROJECT

LEGAL AND REGULATORY CHALLENGES FACING THE GROWTH OF E –COMMERCE IN KENYA

PRESENTED BY

MUNYALO ROBINSON NTHULI

G62/79946/2012

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTERS OF LAWS UNIVERSITY OF NAIROBI

SUPERVISOR; LEONARD OBURA ALOO

JUNE 2016

DECLARATION

I MUNYALO ROBINSON NTHULI do hereby declare that this research is my original work and that the same has not been presented for an award of a degree before by anyone else within Nairobi University or any other University or educational institution.

Munyalo Robinson Nthuli

Signature…… Date …9TH JUNE 2016

This thesis has been submitted for examination with my approval as university supervisor.

Leonard Obura Aloo

Signature…… Date ……9TH JUNE 2016

DEDICATION

This thesis is dedicated to my wife Caroline Munanie Nthuli, my children Victor, Melisa and Fiona, my supervisor Leonard Obura Aloo, lecturers and my fellow scholars who were a great inspiration to me.

ACKNOWLEDGEMENT

I acknowledge the effort of the unconditional support of my supervisor, employer, the head of the academic programmes, friends and colleagues. Thanks for being available for me and your encouragement to complete on time.

Thanks to my family for understanding and standing with me during the entire period of my study. You gave me the hope and desire to go on. Thanks a lot.

Finally, l thanks my academic acquaintances for their encouragement, and to anyone who in any one way contributed to the completion of this study. Thank you all.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION AND BACKGROUND ON THE LEGAL AND REGULATORY FRAMEWORK GOVERNING ELECTRONIC COMMERCE IN KENYA

CHAPTER 2

LEGAL AND REGULATORY FRAMEWORK GOVERNING ELECTRONIC COMMERCE IN KENYA

CHAPTER 3

EFFECTIVENESS OF E -COMMERCE LAW, AND LEGAL CHALLENGES IN KENYA

CHAPTER 4

CONCLUSIONS AND RECOMMENDATIONS

Abbreviations

ARCC ……..……..African Regional Centre for Computing
E-commerce…….…….....Electronic Commerce
B2B .....…….…….....Business to Business
BPO .....…….…….....Business Processing Outsourcing
C2C .....Consumer to Consumer Businesses
CCK .....……Communication Commission of Kenya
G2B ..…….……...…….....Government to Business
ECtHR.....European Court of Human Rights
EDI …….……..……Electronic Data Interchange
ECD ……..……..Electronic Consumer Directive
EASSY …….……..East African Submarine Systems
EAC …….…….……..…….....East African Community
E-SIGN ……Electronic Signature in Global and National Commerce Act
GCCN.....Government Common Core Network
GSMA ……..Global System for Mobile Communications Association
ICT …..…….……..……Information Communication Technology
ICPEN .....International Consumer Protection and Enforcement Network
IMF.....International Monetary Fund
ITU ……..……International Telecommunication Union
ISPs ……..……..Internet Service Providers
KPTC.....Kenya Posts & Telecommunication Corporation
KE-CIRT..... Kenya Computer Incident Response Team Coordination Centre
KeNIC ……..…Kenya Network Information Centre
NCS …….…National Communications Secretariat
NCSMP ……..……National Cyber Security Master Plan
NCRP.....National Central Reference Point
(NC-CIRT).....Northern Corridor Cyber Incident Response Team
NGOs.....Non Governmental organisations
NOFBI .....National Optic Fibre Backbone Infrastructure
NSSUSL …….National Conference of Commissioners on Uniform State Laws
OECD…….Organisation for Economic Co-operation and Development
OTPS …… .… Online Transaction Platform Services (OTPS Standards)
RBV …….……..……..…….Resource Based View
SADC ……..……..Southern African Development Community
SEACOM ……..…….……...South East African Communications
TEAM …….……...East African Marine Systems
UETA ……Uniform Electronic Transaction Act
UNCITRAL ……..United Nations Commission on International Trade Law
U.S ……. ……..…….……..….United States of America
ICC .....……..…….International Chamber of Commerce
WIPO .....World Intellectual Property Organisation
WTO ……..……..……..World Trade Organization
EU …….……. European Union
APEC …….…….……..... Asia-Pacific Economic Cooperation
ECOWAS …….....Economic Organisation of West African States

LIST OF STATUTES

Copyright Act, Cap 130 laws of Kenya.

Industrial Properties Act No 3 of 2001.

Law of Contract Act Cap 23 laws of Kenya.

Kenya Information and Communication Act No 2 of 1998 and as amended in 2009 and 2013 Cap 411A.

The Constitution of Kenya, 2010.

The Evidence Act Cap 80 Laws of Kenya.

The Consumer Protection Act, 2012.

The National Payment Systems Act, 2011, No 39 of 2011.

The Penal Code Cap 63 laws of Kenya.

Trade Marks Act, Cap 506 laws of Kenya.

POLICY

National Information & Communications Technology (ICT) Policy 2006.

REGULATIONS

The Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010.

The Kenya Information and Communications (Numbering) Regulations, 2010.

The Information and Communications Technology Sector (Amendment) Policy Guidelines 2013.

The Kenya Information and Communications (Consumer Protection) Regulations, 2010

INTERNATIONAL INSTRUMENTS

U.N Convention on the use of Electronic Communications in International contracts2005.

UN Convention against Transnational Organized Crime, 2003.

UNCITRAL Model Law on Electronic Commerce.

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.

OECD Guidelines for Consumer Protection in the Context of Electronic Commerce.

UNCITRAL Draft Model Law provisions on electronic transferable Records.

ICC e Terms 2004: ICC Guide to electronic contracting.

The Hague Conference on Private International Law.

INTRODUCTION AND BACKGROUND OF THE LEGAL AND REGULATORY FRAMEWORK GOVERNING ELECTRONIC COMMERCE IN KENYA

1.1 Introduction

The term e-commerce has no internationally accepted definition.[1] OECD define e-commerce as all forms of transaction relating to commercial activities, including both organisations and individuals, which are based upon the processing and transmission of digitised data, including text, sound and visual images.[2] It is doing business over the Internet, selling goods and services which are delivered offline as well as products which can be digitised and delivered online, such as computer software.[3] It is business occurring over open, non-proprietary networks such as the internet including the related infrastructure.[4]

The WTO in November 1998 defined e-commerce as the production, distribution, marketing and sale or delivery of goods and services by electronic means.[5]

E-commerce has also been defined as commercial activity dealing directly with the trading of goods, services and other related business activities, in which electronic communication medium plays a central role.[6] These activities include the communication of information, management of payment, negotiating financial instruments, and transport.[7]

In April 2000, OECD member countries endorsed two definitions of electronic transactions based on narrower and broader definitions. The method by which the order is placed or received determines whether the transaction is an internet transaction (conducted over the Internet) or an

---

1 OECD, report *on information, computing and communication policy, measuring e-commerce* [1997] p 3, 5. OECD is an international economic organization of about 34 countries founded in 1961 with the aim of stimulating Economic progress and world trade.

2 Ibid p 6.

3 OECD ,*report on e-commerce: impacts and policy challenges* p 194.

4 Jonathan Coppell, e-*commerce: impacts and policy challenges* [1999] p 3.

5 Alessandra Colecchia, *defining and measuring e-commerce, Issues for discussion*, OECD, 21 April, p 5.

6 OECD , report on the conference on empowering e-consumers strengthening consumer protection in the internet economy, Washington D.C., 8-10 December 2009 p 6. (OECD consumer protection report)

7 Peterson Obara Magutu, Michael Mwangi & others, *e-commerce products and services in the banking industry: the adoption and usage in commercial banks in Kenya*, Ibima publishing journal of e- banking systems [2011] p 1.

electronic transaction (conducted over computer-mediated networks) the mode of payment notwithstanding.[8] In the broad definition,

> *"An electronic transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organisations, conducted over computer mediated networks. The goods and services are ordered over those networks, but the payment and the ultimate delivery of the good or service may be conducted on or off-line".*[9]

The same definition has been adopted by several writers including Jeffrey F.Rayport, Bernard J Jaworski[10] , John Humphrey, Robin Mansell, Daniel Paré, and Hubert Schmitz.[11] I will for the purposes of this research also adopt this definition.

The narrow definition is the same as the broad definition save that the transactions are *''conducted over the Internet."*[12] It thus excludes orders received or placed by telephone, facsimile or conventional email.

The Kenya Information and Communications Act[13] defines the term "electronic" as relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

James N. K. Kinuthia and David M. Akinnusi view e-commerce as a technology mediated exchange between parties with electronically based intra organisational activities facilitating such exchange.[14] All definitions agree over its fundamental aspect, which is doing business over the internet, using computers and electronic means of communication.

---

[8] OECD , report measuring the information economy 2002, annex 4 , the OECD definitions guidelines for the interpretation of the definitions of electronic commerce p 89 .

[9] WTO, *e-commerce in developing countries opportunities and challenges for small and medium-sized Enterprises* [2013] p 2.

[10] Jeffrey F. Rayport and Bernard J Jaworski, *introduction to e-commerce* (2nd edition MC Graw Hill 2003) p 4.

[11] John Humphrey ,Robin Mansell ,Daniel Paré, Hubert Schmitz, *the reality with e-commerce in developing countries* (2003) p 7.

[12] Ibid p 89.

[13] Chapter 411 A laws of kenya.

[14] James N. K. Kinuthia and David M. Akinnusi ,*the magnitude of barriers facing e-commerce businesses in Kenya*

E-commerce therefore embraces several forms of transactions[15] including information exchange, electronic funds transfers, electronic stock exchange activities, commercial auctions, co-operative design and engineering, electronic bidding, direct consumer sales and after-sale services between businesses (B2B)[16] ,importer and exporter or even Consumer-to-consumer companies (C2C).[17]

It has several advantages including a wider choice of products and services, lower prices, diffusion of new information and technology, sales promotion, customer services, collaboration of supply chains, convenience, no restricted business hours,[18] as well a chance to deal directly with the manufacturers. There is increased speed, efficiency, and significant cost savings.[19] Firms in all regions of the world are able to connect to global networks, and to compete more effectively.[20]

E-commerce has also facilitated globalization. Its interactive nature[21] has led to unprecedented level of interaction between consumers from all over the world on websites such as EBay, Amazon, PayPal, Google ads, among others.[22]

Different kinds of e-business models

The "Brick and mortar" companies are those that have a presence only in the physical world. Their presence in the internet is not for conducting e-commerce. They use the website for passive promotional purposes rather than to engage in online commercial activity.[23]

Academic Journal, vol 4 (1) February 2014 p13.

15 Ritendra Goel, *e-commerce*,(new age international publishers limited reprint 2009) p 15-16.

16 OECD consumer protection report 2009 (n 6) p 6.

17 Ibid p 6.

18 Boateng, R. Molla, A., Heeks, R. and Hinson, R. (2011), advancing e-commerce beyond readiness in a developing economy: experiences of Ghanaian firms, journal of e-ccommerce in oorganizations, p 8.

19 Thomas J. Smedinghoff, *the legal challenges of implementing e-transactions* 2008.

20 Mansell Robin, *electronic commerce: conceptual pitfalls and practical realities*. Prometheus, (2003) 21 (4). p 429-447. available at: http://eprints.lse.ac.uk/3534/LSE Research oonline: May 2008, accessed on 15/11/2012.

21 Richard T. Watson, Pierre Berthon, Leyland F. Pitt, and George M. Zinkhan, *electronic commerce; the strategic perspective* (2008) p 8.

22 OECD consumer protection report 2009 (n 6) p 10.

23 Professor Michael Geist, *a guide to global e-commerce llaw*, internet protocol (IP) attachment 4 page 1.

The Bricks and clicks companies combine a physical offline presence with one online while Pure-play companies or "dot-coms" operate exclusively online. An example is Amazon.com and Monster.com.[24]

1.2 Background

E-commerce can be traced way back to when businesses first used telex, telegram, telephone and fax. Standardisation of business information exchanged digitally was achieved using Electronic Data interchange (EDI).[25] The early 1990's saw commercialization of Internet and the advent of open computer technology. It later developed from a single buyer-seller connection to a multiple buyers-sellers exchange. [26]

Internet was first introduced in Kenya in 1990 by NGOs, Kenyans in the diaspora, western ex-patriates, International Gateway operators and as well as Internet Service Providers (ISPs) such as Form net and African online.[27]

In October 1995, the Africa Regional Centre for Computing (ARCC) established the first full Internet services connection in Kenya. The Kenya Posts & Telecommunication Corporation (KPTC) was the monopoly of the infrastructure locally and internationally. [28] The Kenya Information and Communication Act (KICA), 1999 provided a very important legislative framework of dismantling the monopoly as a result of provisions of Section 5(5) of the said Act. The provision clearly provided that the rules, guidelines and regulation established were not to create a monopoly or a duopoly in operating telecommunication system or service.

In July 1999, the government officially liberalized the sector regulated by CCK (now *Communication Authority of Kenya*). However, Telkom Kenya, was allowed monopoly to operate

---

[24] Ibid p 1.
[25] Lawrence C. Leung1, Sung-Chi Chu1, Yer Van Hui2, and Waiman Cheung, *the evolution of e-commerce* . websites, a conceptual framework and analysis center of cyber logistics, business administration, Chinese U. of Hong Kong 2.
[26] Ibid p 1.
[27] Michel M. Murungi *Cyber law in Kenya*, Kluwer Law International 2011, p11.
[28] Ibid, p 35.

an Internet backbone for five years, until 2004 when it was liberalised hence growth of the number of ISPs.[29]

There has been growth of internet users after Kenya connected to the rest of the world through the optic cables which included the East Africa Marine Systems (TEAM), the East Africa Sub-marine Systems (EASSY) and the South East Africa Communications (SEACOM).[30] In July 2009, SEACOM, reached Kenya, Tanzania and South Africa. It also reached some landlocked countries such as the Rwanda Uganda, Mozambique by the use of cross border backhauls, hence faster and cheaper Internet.[31]

In 2010, EASSy became operational along the East and South African coasts. It links South Africa with Sudan, with landing points in Mozambique, Madagascar, the Comoros, Tanzania, Kenya, Somalia, and Djibouti [32] hence an increase in international bandwidth and consequential lower costs.[33] The internet users have also increased from about 7,832,352 users in the year 2010 to about 29,672,419 in the year 2015 as confirmed by table 1.1 below.

Table 1.1 Trend of internet users between year 2010 and 2015.

Internet usage 2010-2015

Year	June 2010	June 2011	June 2012	June 2013	June 2014	June 2015	Variation 2010-2015 (%)
Internet users	7,832,352	12,538,030	14,032,366	19,654,925	22,319,684	29,672,419	278.84

Source ITU data base

[29] Ibid, p 36.
[30] The ICT Board connected Kenya 2017 master plan p 5.
[31] UNCTAD report 2012 , harmonizing cyber laws and regulations ,the experience of EAC p 3.
[32] Murungi (n 27) p 11-12.
[33] David Souter and Monica Kerretts-Makau, *Internet governance in Kenya – an assessment for the Internet society*, September 2012, p 7.

The international bandwidth usage rose from 847,464 in June 2014 to 1,668,561 as at June, 2015 [34] with possibility of more growth as seen in Table 1.2 below [35]

Year	June 09	June 10	June 11	June 12	June 13	June 14	June 15	Percentage variation 09-15 (%)
Total International Internet Bandwidth	**1,677.15**	**20,384**	**305,174.50**	**574,704**	**844,359**	**847,464**	**1,668,561**	**99,367**

Table 1.2 International Internet Bandwidth usage, between June 2009 and June, 2015

Source: CA, Operators' Returns

There was growth in registration of domain name from 20,085 in June 2012 to 47,704 as at June, 2015, an increase of approximately 137.51 percent as shown in Table 1.3.

Table 1.3 Growth in the number of domain names[36]

Year	June 12	June 13	Jun 14	June 15	Variation between 2012-2015 (%)
No. of Domain Names	20,085	27,374	33,381	47,704	137.51

Source: CA Kenya Network Information Centre (KeNIC)

The growth in internet and mobile data subscriptions as at June, 2015 is shown in Table 1.4 below. It shows that there was a substantial increase in internet and mobile data subscriptions and total internet users. [37]

[34] CCK website ,quarterly sector statistics report, quarter of the financial year 2013/14 (July-Sept 2013), p 24. (CCK July-Sept 2013 quarterly report)
[35] CCK website, quarterly sector statistics report second quarter of the financial year 2014/15(June-June 2015) p27.
[36] CCK website, quarterly sector statistics report second quarter of the financial year 2014/15(June-June 2015) p29.
[37] CCK website, quarterly sector statistics report second quarter of the financial year 2014/15(June-June 2015) p23.

Table 1.4 Trend of internet and mobile data subscriptions and total internet users as at June, 2015[38]

Year	June 2009	June 2010	June 2011	June 2012	June 2013	June 2014	June 2015	%variation between 2009-2010
Total Internet Users	1,997,832	7,832,532	12,538,030	14,032,366	19,654,925	22,319,684	29,672,419	1385

Source: CA, Operators' Returns

There has also been an increase in mobile phone use in kenya. Development of e-commerce in Kenya is closely linked with mobile phone use and money transfer. During the period 2009-2015, the total number of mobile subscribers rose from 17,362,357 million to 34,794,457 [39] as evident from Table 1.5 below;

Table 1.5 Mobile Subscriptions

Year	June 2009	June 2010	June 2011	June 2012	June 2013	June 2014	June 2015	Variation in 2009-2015 (%)
Total Mobile Subscribers	17,362,357	20,119,304	25,279,768	29,703,439	30,549,422	31,830,003	34,794,457	100.40

Source; CCK Operators returns

M-payment is being used for various processes, including paying for goods, services, paying bills, receiving salary and money transfers which can be either national or international. [40]It is a great solution to the absence of financial institutions in many areas of Africa as there are over 735 million SIM cards being used in Africa.

Tables 1.6 below confirm the mobile money transfer service continued tremendous growth between June 2011 and June 2015.[41]

[38] Ibid p 21.
[39] Ibid p 8.
[40] Diane Mullenex and Anne-Sophie Mouren *m-payment in Africa: great means to great ends*, December 2012 regulatory communications p 22.
[41] CCK website, quarterly sector statistics report second quarter of the financial year 2014/15(June-June 2015) p 12.

Table 1.6: The trend on the mobile money transfer service during the period June 2011- June 2015.

Year	June 2011	June 2012	June 2013	June 2014	June 2015	Variation between 2011-2015
Subscriptions	17,395,727	19,509,702	24,840,404	26,611,077	27,742,040	59.48
No of Agents	42,313	49,079	88,466	109,286	129,357	205.71

As at 16th April 2012, the IMF recommended that the Kenyan legal framework needs to be enhanced, including incorporating M-PESA operations as part of the National Payments Systems. It also underlined the great need for updating the security systems.[42]

E-Commerce in Kenya

Kenya has not experienced the desired growth in e-Commerce even with the significant growth of infrastructure and passing of some laws. Whereas the role of internet in commercial advertisement and marketing is recognized and its potential appreciated,[43] very few transactions are conducted entirely through the internet.[44] One reason is lack of trust and ignorance of available remedy in the event of breach or disputes.[45]

Its slow trend was witnessed with the shutting down of the electronic commerce site Kalahari.co.ke sometime in October 2009 only two years after its launch.[46] It was an online store, whose concept was similar to the world's largest e-commerce platform, Amazon.[47]The main

[42] Diane Mullenex (n 42) p 22.
[43] MNTE News Africa at http://www.itnewsafrica.com/2007/06/e-shopping-is-kenya-ready-for-business/ accessed on 15/11/12.
[44] Lillian Edwards and Charlotte Waelde ,*Law and the internet* , 3rd edition ,Hart publishing, Oxford and Portland oxford, 2009 p 4.
[45] Ritendra (n 15) p 26.
[46] Business news 26th October 2009 http://www.standardmedia.co.keaccessed 27/11/12.
[47] Lillian Edwards (n 46) p 89.

reason for closures was performance below expectation and low profit. The same applied to South African media giant Naspers.[48]

The question remains, why the low margins yet the site boasted of 14 million users and over 3 million products and services listed. [49] The internet users have continued to grow and stood at 19.1 million between July and September 2013.[50] The population that had access to internet services reached 47.1 per 100 inhabitants in the same period while the number of subscriptions grew by 2.5 per cent to reach 31.3 million.[51] E commerce has however not grown at the same rate.

1.3 Justification of the Study

Rapid growth of technology has given rise to a new mode of commerce which has created a global and borderless commercial activity. There has been growth in trade not only in goods but also services such as airline and hotel booking and financial services, including online banking. Copyright-based industries have also promoted e-commerce by developing new types of products and content. Opportunities for further growth appear substantial.[52]

The rationale for the study is establish the effectiveness of the current Kenyan e-commerce laws since despite rapid Internet growth, infrastructure, low cost data, growth of mobile money transfer, online retailing, enacting and harmonise the law, e commerce in Kenya continues to progress very slowly compared to that of the developed and leading developing countries. This has to change if vision 2030 is to be realised and if Kenya is to become the BPO top destination in Africa.[53]

As early as 2008, Marcel Werner[54] and the Kenya ICT Federation[55] anticipated e-commerce would add 1% to Kenya's GDP[56], hence its importance to the economy. An adequate

---

48 Business news (n 48).
49 Ibid.
50 CCK July-Sept 2013 quarterly report (n 36) p 6.
51 Ibid p 6.
52 OECD consumer protection report (n 6) p 7.
53 Murungi (n 27) p 25-26.
54 Then chairman of Kenya ICT federation.
55 Kenya ICT federation, legislation and regulation for e-commerce in Kenya, KIF advocacy project 2008.

legal and regulatory framework is required if the benefits of e-commerce are to be realized. This study is therefore important because it seeks to find out whether the legal and regulatory framework governing e-commerce in Kenya is favourable, effective and identify its deficiencies if any.

The study will also be beneficial to the policy makers on ICT sector. It is intended to recommend ways in which legislation can be amended to ensure that e-commerce is secure and build confidence among the customers and businesses to ensure fair trade, privacy, secure payment mechanisms and morality.[57]

The study is timely in view of the lack of focused literature on the legal and regulatory framework and its effectiveness with regard to e-commerce in Kenya. The issues arising are also topical and contemporary in modern world as the rapid change in technology has caused a great challenge to the law, which is not able to change as fast.

1.4 Statement of the Problem

The ease and reliability of communication has facilitated the development of international trade and e-commerce, globally recording billions of dollars in sales. [58] There is enormous opportunity to exploit e-commerce and the advantages ICT services play in economic, social and political spheres.[59]

As a regional economic, social and political hub, Kenya has a significant role to play in promoting e commerce. One of the main objectives of The Vision 2030, Kenya's economic blueprint, is to make Kenya a Business Process Outsourcing and call centre destination. [60] To achieve this, Kenya must take up the challenge and compete with India, Philippines and China

---

[56] Kenya's ICT Board on e-commerce, ICT board website accessed at 05/04/2013.
[57] John Dickie ,*producers and consumers in Eu e-commerce law*, (2005 Oxford: Hart) p 111.
[58] OECD consumer protection report (n 6) p 8.
[59] UNICTAD report 2012 (n 33) p iii.
[60] The Kenya vision 2030, popular version government printer p 14.

which are the leading BPO and contact centre destinations, by deliberately creating an enabling legal environment for e-commerce.[61]

Towards this end, the Government had a national ICT master plan, for the period 2008-2012. The Ministerial strategic plan 2013 -2017 outlines the roadmap and implementation strategy to make ICTs more accessible and affordable to the wider population.

There has also been a regional and national commitment towards providing a modern legal framework to interface between the physical and digital space. [62] The law has been identified as a critical factor for the effective implementation of e-commerce strategies at national and regional levels [63]as well as keep abreast the dynamic changes in the communication sector and e - commerce at large[64].

The East African region has also encountered a revolution in mobile use and mobile money service in particular M-Pesa by Safaricom,[65] the largest mobile network operator in Kenya.[66] This is also seen as an opportunity for growth in the financial sector and e commerce in general.

However despite all the above and the improved infrastructure, growth in the number of intent users and the enactment of some law, there has been no significant growth of e-commerce.[67] Kenyans has not been able to generate significant e transactions as[68] there are very few transactions contracted and concluded entirely through the internet. Kenya is therefore yet to reach its potential in e-commerce and the sluggish growth can partly be attributable to lack of effective

[61] Wakama Abby, Kenya's cyber law being developed, *the standard newspaper* (online edition), Published on Sunday ,Aug 5th, 2007<http;/www.itnewafrica.com accessed 05/04/2013.(Wakama Article)
[62] UNICTAD report 2012 (n 33).
[63] UNCTAD, report 2013, harmonizing cyber laws and regulations: the experience of the EAC op cit p 3. (UNCTAD, report 2013)
[64] Zeinab Karake, Lubna Qasim, *Cyber law and cyber security yin developing and emerging economies*, Edward Elgan publishing 2010.
[65] UNCTAD, report 2013 (n 65), p 18.
[66] Safaricom website accessed 7/4/2013.
[67] Murungi (n 27) p 11-12.
[68] Wakama Article (n 63).

legal and regulatory framework. There are concerns of fraud [69]hence the need for this study on the effectiveness of the legal and regulatory framework.

Time has come for Kenyan businesses to reform its online presence and exploit the market opportunities in e-Commerce.[70]The goal is yet to be realised hence the need for this study to address the effectiveness of Kenya law to support and increase growth of e-commerce.

1.5 Theoretical Framework

E-commerce can be viewed from different theoretical perspectives including the Public interest theory, trust theory; transaction cost theory, functional equivalence theory, the technological neutrality, as well as the Resource-based view among others. All these theories are quite intertwined.

The Public interest theory holds that regulation is necessary to respond to demand by the public for the correction of inefficient or inequitable market practices.[71] It hypothesizes that regulators pursue the best interests of the consumers of the products of firms in a regulated industry. [72] E-commerce must be regulated by the government to achieve the same. Arrows[73] and Baumol[74] in making a case for this theory argues that wherever there is a market failure, it should be responded to by use of Government Regulations. Nelson however sees this theory as in adequate to the extent that market players will more often than not develop mechanism to fill in the gaps identified in the market system.[75] Posner also argues that the theory makes an assumption that the Government Regulations will be effective and efficient is resolving the market failure which is not the case.[76] Joskow & Noll argue that the assumption that the Government Regulations

---

69 Muthoki Mumo, "Trade via Internet yet to pick up despite cables", daily nation Tuesday, Jan 15 2013 at 02:00.
70 Business news (n 48).
71 Richard A. Posner, theories of economic regulation, Nber working paper series, May 1974, p 2.
72 David D. VanHoose, e-commerce economics 2nd edition, Taylor and Francis, 2011, p 287.
73 Arrow, Kenneth J. (1985), 'The Potentials and Limits of the Market in Resource Allocation', in Feiwel, G.R. (ed.), Issues in Contempory Microeconomics and Welfare, London, The Macmillan Press, 107-124
74 Baumol, William J. (1952), Welfare Economics and the Theory of the State, Cambridge Massachusetts, Harvard University Press.
75 Nelson, Philip (1974), 'Advertising as Information', 82 Journal of Political Economy, 729-754.
76 Posner, Richard A. (1974), 'Theories of Economic Regulation', 5 Bell Journal of Economics and Management Science, 335-358.

will bring efficiency in doing business is not always correct as concepts such as procedural fairness reduces efficiencies.[77]

One of the key objectives of a legal framework is to build trust and confidence. Lack of trust is still one of the biggest concerns and barriers for Internet consumers and without it development of e-commerce cannot reach its full potential. The trust theory is meant to improve certainty and ensure that both consumers and businesses are confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are and that transaction mechanisms are available, legal and secure.[78]

In an e-commerce environment, trust is more difficult to build [79] and critical for success than in traditional commerce. Trust is a long-term proposition and a dynamic process that must be built over time[80] though easy to lose.[81]

Ronald Coase, a leading economist came up with the transaction cost approach theory.[82] He defined transaction cost as the cost of providing for some good or service through the market rather than having it provided from within the firm. These are costs that people incur when they exchange products, assets, information, negotiate contracts and when they monitor contractual agreements to ensure that terms of agreements are enforced.[83] The transaction costs affect e-commerce and the internet business model.[84]

The transaction cost theory relates to both the service provider and the customer process.[85] It influences the customer value. The trustworthiness and uncertainty of e-commerce by consumers can be significantly affected either positively or negatively by the transaction costs.[86]

---

77 Joskow, Paul L. and Noll, Roger C. (1981), 'Regulation in Theory and Practice: An Overview', in Fromm, Gary (ed.), Studies in Public Regulation, Cambridge, MA, The MIT Press, 1-66.

78 Communication to the European parliament, the council, the economic and social committee and the committee of the regions, *a European Initiative in electronic commerce*, paragraph 35, 15/04/97.

79 Ibid p 3.

80 Ibid p 30.

81 Head, M., and Hassanein, K. (2002). "*Trust in e-commerce: evaluating the impact of third-party seals*", quarterly journal of electronic commerce, 3(3), p307-325.

82 Rana Tassabehlyl, applying e-commerce in business 2005, Sage Publisher's ltd, p154.

83 David D. Vanhoose, e-commerce economics, Rutledge 2011 p 112.

84 Ibid p155.

85 Frauendorf, Janine. *Transaction cost theory*. DUV, 2006, p 53.

86 Coarse, Ronald H. (1937), 'The Nature of the Firm', Economica, 4, New Series, November, pp. 392.

Reducing the consumer's transaction costs[87] such as travelling costs, is likely encourage them use e-commerce more. Likewise, an efficient legal framework is crucial as it can check and control the vices of fraud, privacy intrusion and hence increase trust and certainty.

This theory can create uncertainties given problems of definition and quantification. The maximizing equation described above may be too difficult to operationalize in its full form, except in relatively discrete and limited circumstances.

Recent writings on the theory of the firm sometimes use transaction cost to refer indiscriminately to organizational costs whether these arise from within the firm or across the market. This rather inept language forces textual discussion to make distinctions that would be better left to single-word labels.

The functional equivalence theory is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.[88] It is meant to ensure that an electronic record to receive the same legal recognition as paper based documents.

It strives to create legal results which are similar if not identical; regardless of the medium of communication [89] and that any electronic version enjoys the same level of legal recognition as a corresponding handwritten or hard copy. [90]

A legal framework governing e-commerce should be technologically neutral. The law should not discriminate between different forms of technology which ensures there is no stifling any technology or unfairly favouring one technology over another. This ensure that the law is not rendered redundant once a new technology is produced. The law should always accommodate future technological developments. [91]

---

[87] Ibid p 392.
[88] Paragraph 51, Explanatory note by the UNCITRAL secretariat on the U.N Convention on the use of electronic communications in international contracts, UN Publication sales no. E.07.V.2,
[89] S. Eiselen, the UNECIC ; international trade in the digital era 2007 p22.
[90] Use of Electronic Signatures in federal organisation transactions version 2.0 January 25th ,2013 p5.
[91] Ibid 21.

The non-discrimination theory ensures that e-communication and contracts are not discriminated against in favour of traditional paper based ones and are recognised by the law. A legal framework should provide the manner in which a contract can be formed electronically and how parties to such contract can be identified.

The resource-based view theory addresses e-commerce in the context of competition, resources and economic development. It addresses two main questions on what resources can contribute to a firm competitive advantage and how these resources enable a firm to achieve superior performance and keep competitive in its industry.[92]

It looks at a firm as a combination of various resources and capabilities and suggests resources are rare, valuable, imitable, and not easily substitutable, can contribute to superior firm performance and sustained competitive advantage.[93] It focuses on the impact of internal firm resources on firm performance.[94]

E-commerce can be a tool to enhance firms or businesses compete in the market more effectively.[95] Standard and effective domestic law that does not contradict the model international law encourage business growth and investors.[96] Businesses face increasing pressure to conduct their transactions in electronic form due to the benefits, competition among other motivators.[97]Firms incorporate ICT resources and assets to improve performance.[98]

Resource-based view ensures firms develop specific resources and capabilities to support their business operation. For example, a good relationship with customers and partners, well-established reputations, acceptable legal and regulatory frameworks and fast market

---

92 Jay Barney, Firm resources and sustained competitive advantage, Journal of management 1991 vol 17 no1, Texas A&M University p 9-120.

93 Ibid.

94 Yi Wang and Xinping Shi, *towards a theoretical framework of e-business value creation: the dynamic capabilities perspective* 122.

95 Mansell Robin (n 20) .

96 Richard T. Watson, Pierre Berthon, Leyland F. Pitt, and George M. Zinkhan, Electronic commerce; the strategic perspective (2008), op cit p 8.

97 Thomas J. Smedinghoff (n 19).

98 Yi Wang and Xinping Shi, *towards a Theoretical Framework of E-Business Value Creation: The Dynamic Capabilities Perspective* op cit, p 122.

responsiveness are especially critical factors for firms engaging in e-business and adds value creation.[99]

One of the critiques of the resource-based view is that it has no managerial implication or operational validity .It seems to tell managers to develop and obtain valuable, rare, inimitable, and non-substitutable resources and develop an appropriate organization, but it is silent on how this should be done [100]The theory's applicability is too limited as it only applies to large firms with significant market power.

The value of a resource is too indeterminate to provide for useful theory. Critics argue that RBV is a tautology that fails to fulfil the criteria for a true theory. It does not contain the law-like generalizations that must be expected. Rather, it stands on analytic statements that are tautological, and that cannot be tested.[101]

Governments and stakeholders have to work together to ensure that e commerce benefits are fully realised, which includes finding ways to boost consumer confidence in online transactions particularly through effective legislation. Adequate disclosure, assured data protection, privacy and security are also key in this regard.[102]

The identified theoretical framework advances an understanding of the nature and unique roles of e-business in firm performance, the role of the law to remove uncertainties and competitive advantage. Firms aim at survival and success in the uncertain and changing legal environment and should broaden their vision and focus on the critical function of e-business as a capability-enabler within organizations.[103]

---

99 David J Teece, Gary Pisano, Amy Shuen; Dynamic capabilities strategic management, models of strategy emphasizing resource based perspective p 513.

100 Jeroen Kraijenbrink, JC Spender and Aard Groen, *The resource-based view: A review and assessment of its critiques* University of Twente, 2009.

101 Ibid

102 OECD consumer protection report (n 6) p 6.

103 Ibid.

1.6. Literature Review

Reed[104] observes that the geography of the internet is purely virtual and it pays no heed to geographical boundaries. The parties to an internet transaction are thus faced with overlapping and often contradictory claims that national law applies to some part of their activities. Zittrain[105] points out that the internet permits such extraordinary information access and manipulation by individuals across distances.

Reed sees the country of origin regulation principle as the only regulatory model capable of resolving the conflicts between multifarious and overlapping claims by national jurisdictions to regulate particular internet activities especially taxation of goods and services.

Souter and Kerretts-Makau[106] describe the relationship between global and national governance of the Internet as complex. The Internet is seen as inherently global rather than national in character. In practice, however, national governance arrangements are also highly significant especially in technical areas such as management of country level domains (ccTLDs); the underlying infrastructure and at the interface between the Internet and other policy domains which are subject to national laws and social norms.

Walden[107] has written on computer crime and digital investigations. He notes that with expansion of telecommunication, there is always need to make the legal regulatory framework less complex. He also states that there is need to adopt international best practices in modelling the legal framework. Horne and Waelde[108] discussed two main challenges for cross border litigation being expensive as well as the aspect of delay making it not viable for small claims.

Edwards and Waelde [109] argues that the use of the internet has changed the world into a global village raising questions and arguments whether it has abolished national jurisdictions and boundaries.

---

104 Chris Reed, *Internet law*: text and materials, 2nd edition, Cambridge University Press, 2004.
105 Jonathan L. Zittrain, internet law series: jurisdiction (foundation press, New York, 2005).
106 David Souter and Monica Kerretts-Makau, *internet governance in Kenya – an assessment for the internet society*, September 2012, p 3.
107 Ian Walden, Computer crime and digital investigations ,oxford university press 2007.
108 Lillian Edwards (n 46) p 26.
109 Ibid.

Tassabehlyl, [110] looks at the foundations of technology on which e-commerce is built and argue that in the 21st century business, it is no longer acceptable or good business practice for technology to be the sole responsibility of IT departments. He asserts the `dot com' phenomenon and frameworks have emerged as a result and that security is the largest inhibitor to e commerce.

Vanhoose [111]addresses the economic issues associated with using computer-mediated electronic networks. He discusses IPRs in a digital environment, regulatory issues in electronic markets, public sector issues, online banking and finance, digital cash, international electronic trade, and the implications of e-commerce for aggregate economic activity among other issues.

Coase,[112] came up with the transaction cost approach theory. The transaction costs determines the business model of e-commerce.[113] He defined transaction cost [114] and argue that the trustworthiness and uncertainty of e-commerce by consumers can be significantly affected either positively or negatively by the costs.[115]

The UNECIC, aims at establishing legal certainty in international trade by providing solutions and harmonising rules on electronic communications for international transactions.[116] However these Rules have still not removed the perceptions about legal uncertainty which has to be balanced with other principles such as flexibility and good faith.[117]

Bingi, *et al* [118] see challenges facing global e-commerce in four dimensions that is economic, technological, social, and legal. Almeida, et al [119] listed factors hampering growth of e-commerce as lack of national security, skills, confidence, high cost as well as insufficient infrastructure. They stressed the need for legal and regulatory framework for the promotion of e-commerce.

---

[110] Rana Tassabehlyl , *applying e-commerce in business*, sage publishers ltd 2005.
[111] David D. Vanhoose (n 80).
[112] Coase, Ronald H (n 83) .
[113] Ibid p155.
[114] David D. Vanhoose (n 80) p 112
[115] Coase, Ronald H (n 83) p. 392.
[116] UNECIC Preamble .
[117] S. Eiselen, the UNECIC (n 86) p20 and 21.
[118] Prasad Bingi , Ali Mir & Joseph Khamalah, *The Challenges facing global e-Commerce, Information Systems Management* (2000) .
[119] Guilherme Alberto Almeida de Almeida, Alfonso Avila, Violeta Boncanoska, (March 2007) promoting e-commerce in developing countries internet governance and policy - discussion papers diplo.

Laudon and Traver [120] addressed internet security, payments and cyber wars and how hacking is a major security concern even to governments.

Rayport and Jawoski [121] and the UNCTAD 2003 Report, discussed e- commerce generally in terms of infrastructure which include technologies, media, capital, and public policy. They discussed issues of e commerce security and market place and argued that Consumers hesitate to disclose confidential data such as their home address, social security number, and credit card number over the Internet. They question the sufficiency of the safeguards that protect their privacy from being breached or their money from being stolen.

They argue that Cultural diversity and local needs of consumer needs to be taken into account while designing e-commerce sites. The preferences of many different customer groups is a major challenge for developers and customization tends to be rather expensive.

The lack of sophisticated translation tools does not allow an easy translation of Web pages from English, the dominant language of the Web, into local languages. These tools are slowly being developed and other languages are coming online.

Bingi, *et al* [122] see new technologies such as the Internet as a highly disturbing force that shocks the existing norms in a society. New laws have to be enacted to take care of the new problems or issues that technology introduces into the society.

Goel [123] as well as Kakooza [124] has looked at technology, its prospects and advantages. It has changed not only trade but banking worldwide hence the need for harmonised laws. The problems of e- commerce to him include security, costs, legal issues, lack of skill, uncertainty, jurisdiction and lack of information on what to do in the event of breach or disputes.

Lemley, et al[125] see the law of e-commerce as a vague, poorly defined and in some cases not different from the law of commerce generally. They argue that contracts, disputes, tax issues,

[120] Kenneth C Laudon and Carol Guecio Traver, e- commerce 2011(7th edition Pearson education ltd) .
[121] Jeffrey F. Rayport and Benard J jaworski (n 10).
[122] Ibid.
[123] Ritendra Goel (n 15).
[124] Kakooza ACK (2009). embracing e-commerce in Uganda: prospects and challenges. university law review,1:2.
[125] Lemley, Menell, Merges and Samuel, *software and internet law* (aspen law & business, 2000).

and payment systems each have its own legal infrastructure, and in large part applying law to e-commerce is simply a matter of applying those rules to a new environment.

Bell and Ray [126]pointed out that there has over the years been liberalization of telecommunication in most states hence the need for harmonization and liberalization.

De Kerros [127] and Jobodwana [128] dealt with the slow progression of e-commerce in Saudi Arabia. The major challenges are technology, infrastructure, consumer behaviour, payment systems; the usage of post office Box systems rather than residential postal addresses, the speed, access, unclear regulations, under-developed customer and after-sales services, lack of trust, lack of know-how, organizational structure, logistics, cost, and lack of government support. Tatjana de Kerros further states that effective online banking is a crucial determinant to enabling the growth of e-commerce activities.

Kraemer et al.[129], Goyal [130] and Gikandi and Bloor [131] stressed the need to maximize the benefits of its youthful demographics and turn itself into the knowledge hub of the world through the application of ICT in all aspects of life .

Gikandi and Bloor established the factors that influence the adoption and effectiveness of e-banking in Kenya as lack of resources, constant change in technology, time to develop systems, accessibility and lack of use of Internet by the general population.

Kinuthia and Akinnusi**[132]** named economic and social situations, infrastructure, legal and political environments as the most formidable internal and external organisational factors affecting electronic commerce in Kenya.

---

[126] Robert S.K. Bell and Neil Ray, *European union electronic communication law* (oxford university press 2004).

[127] Tatjana de Kerros *report e-commerce in Saudi Arabia: driving the evolution, adaption and growth of e-commerce in the retail industry* Orloff 2012 .

[128] Jobodwana ZN , *e-commerce and mobile commerce in South Africa: regulatory challenges*. J. Int. Commercial law technol Vol. 4, Issue 4 (2009) .

[129] Kraemer KL, Jennifer GJ, Jason DJ *Impacts of globalization on e-commerce adoption and firm performance: a cross-country investigation* (2002).

[130] Goyal KA , *Impact of globalization on developing countries* , Int. Res. J. Finance Econ. 2006.

[131] Gikandi JW, Bloor C *adoption and effectiveness of electronic banking in Kenya. e-commerce applicatio*ns 9(4):277–282. (2010).

[132] James N. K. Kinuthia (n 14).

The 2002 Kenya policy [133] emphasized the crucial need to counter the info-communications sector which is very dynamic. It called for a policy regime that is responsive, dynamic, and stable and an effective regulatory regime.

Machaira et al[134] identified challenges like leadership characteristics, adoption of new electronic strategies, infrastructure, competition and technological positioning as the factors affecting e commerce on Tour Travel firms in Nairobi.

Magutu et al [135]argued that a true cross-functional structural orientation requires participative teamwork and cooperation throughout all levels and across functions, an objective that is very difficult to accomplish.

Murungi describes the then regulatory regime for the ICT Industry as the product of political, legislative and administrative initiatives over a period of time. The writer has addressed aspects of cyber law including intellectual property rights, competition, electronic transactions, privacy, computer crimes, ICT infrastructure and related contracts. [136]

Magutu, et al[137] explored the challenges faced and benefits that accrue from the adoption and usage of e-commerce products and banking services by commercial banks in Kenya.

Gichuki [138] discussed the challenges of electronic commerce on tax policy in Kenya and that development issues cannot be envisaged without considering the impact of information technology on them. E-commerce is such one development. Gichuki and Kipyetor[139] looked at taxation of e-commerce and the challenges posed by the concept of permanent establishment.

---

[133] Telecommunications policy in transition, *Mainstreaming Kenya into the global information economy , institute of economic affairs* 2002 P 54.

[134] Dr. Wanjau Kenneth Machaira N. Rebecca and Agodo Eunice *factors affecting adoption of e- commerce by small medium enterprises in Kenya* (2012),

[135] Peterson Obara Magutu , Joel Kiplagat Lelei , Ali Okiti *Nanjira African journal of business & management* (Ajbuma) Aibuma Publishing http://www.aibuma.org/journal/index.htm Vol. 1 (2010),accessed on 15/1/12.

[136] Murungi (n 27) p 48.

[137] Peterson Obara Magutu, Michael Mwangi & others (n 7).

[138] E. Njaramba Gichuki ,*challenges on electronic commerce on tax; towards a sustainable tax policy on e-commerce for sustainable development in kenya* (2007).

[139] Jemutai Kipyetor Grace, *Taxation of e-commerce, the challenges posed by the concept of permanent establishments* (2005).

All the studies reviewed explored the factors affecting e-commerce with the results indicating serious internal and external factors. However, none of the literature above has taken a look at the specific legal and regulatory framework of the current e commerce law in Kenya and its effectiveness as is being proposed in this study.

The study intends to address the issue of the slow growth of e commerce in spite of the development infrastructure, the law, harmonisation and growth of internet users. The issue of jurisdiction, disputes and whether Kenya is able to deal with preventive, adjudicative and enforcement need to be addressed.

1.7 Objectives of the Research

1) To establish the current national and international e-commerce laws and policies that apply in Kenya.

2) Critically examine the legal and regulatory framework governing e commerce in Kenya, its effectiveness and challenges.

3) To identify and come up with recommendations on the legal, regulatory framework to ensure faster growth of e commerce and build confidence in the consumers.

1.8 Broad Argument Layout

Today, each country strives towards the creation of an open, competitive Electronic Marketplace.[140] This requires an effective legal infrastructure that supports the seamless location, transfer, and integration of business information in a secure and reliable manner.

The slow growth and development of online retailing in Kenya compared to that of developed and leading developing countries has been associated with fear arising from inadequacy and ineffective law and the failure of the system to effectively address all the issues touching on e

[140] Mary brady, Steve Trus , *challenges in electronic commerce,* http;//www.itl.nist.govt/div897/stff/brady/ec/nist-ec.html accessed on 5th November 2012.

commerce. There is urgent need to identify these legal and regulatory factors affecting e-commerce and recommend appropriate action.

1.9 Hypotheses

The study proceeds on the following hypotheses;

1) The current e-commerce laws and policies in Kenya are not adequate to enhance the required growth in e commerce.

2) Although the government policy has been to encourage and support growth of e commerce, the existing law is yet to effectively facilitate such good intentions and the country has not realised its potential nor has it been able to cope with rapid technological changes and emerging challenges.

3) A combination of legal, the social, cultural, political, organisational, and economic factors have led to the slow growth of e commerce in Kenya. However, addressing the legal aspect would resolve most of the challenges the country faces in the slow growth in e-commerce.

1.10 Research Questions

The questions that this research seeks to answer are: -

1. What are the current laws governing e-commerce in Kenya?

2. Are the said laws effective to create a favourable environment for the growth of e-commerce?

3. Are there any gaps and weaknesses on the current laws that have led to the slow growth and which create barriers to the development of e-commerce?

4. What improvements can be made on the legal, regulatory and institutional framework to ensure faster growth of e commerce?

1.11 Research Methodology

This study is intended to be exploratory predominantly based on review of literature. Both primary and secondary sources of data will be utilised by looking at the law and relevant literature. The research will be conducted in the following ways;

i. library-oriented,

The main mode of research shall be secondary with the main source being library based. Reference will have to be made to the relevant statutes and any available books on the subject. Books, Journals, publications, international treaties and conventions will be looked.The primary source is important as there is need to look at Kenyan law as well as law in other jurisdictions since e -commerce, its law and challenges apply across board.

ii. internet

The issues and concerns arising on e-commerce are of a global concern. The internet will be a crucial source of information as there is need to refer to websites for international bodies such as UNCTAD, OECD, UNICITRAL, ICC, WTO, EU, APEC, Council of Europe and the EAC.

iii. Empirical sources

Although there is very scarce litigation on issues touching on e -commerce, it will be necessary to refer to a few case law to illustrate the practical challenges that arise in the event of breach or disputes arising in e commerce transactions.

1.12 Limitation of the study

The study is limited to the legal aspect only and will not be able to address the other social, economic, political, organisational and cultural aspects behind the slow growth of e-commerce in Kenya.

There are very few local books and publications on the subject under research. Most of the available cases on e -commerce are foreign as there has not been any substantial

litigation locally touching on the issues that arise.

The study is not a comparative study and it does not purport to be a comprehensive evaluation of the effectiveness of the legal and regulatory framework of e- commerce in Kenya. The research does not purport to establish countries with progressive legal frameworks on e commerce. However, it relies on foreign case law to examine how countries have addressed various legal issues.

1.13 Chapter Breakdown

1.10 Chapter One: Introduction and background of the legal and regulatory Framework governing electronic commerce in Kenya

This chapter lays out an introduction and the background to the study. It justifies the study and identifies the research problem to provide a perspective of the study, there is a theoretical framework which is put in its proper context, by the literature review. The objective of the study and the broad argument is given followed by the hypothesis. The posed research questions follow with a view to answering the research problem. The research methodology and limitations have also been outlined in this chapter.

2.10 Chapter Two: The legal and regulatory framework governing electronic Commerce in Kenya

This chapter shall analyse the legal and regulatory framework governing e commerce in Kenya.

3.10 Chapter Three: An analysis of the effectiveness of e -commerce law, and legal Challenges in Kenya

This Chapter will address the effectiveness e -commerce law, and legal challenges facing Kenya in enforcing the law and to what extent they inhibit growth of e-commerce in Kenya;

4.10 Chapter four: Conclusions and Recommendations

The conclusion and recommendations towards enhancing effective legal and regulatory framework of e commerce in Kenya.

CHAPTER TWO

2.0 LEGAL AND REGULATORY FRAMEWORK GOVERNING ELECTRONIC COMMERCE IN KENYA

2.1 INTRODUCTION

E-commerce legislation is important as it facilitates transactions within the country and across its borders. It creates the much-needed sense of certainty like that for traditional paper-based physical business transactions.[141]

More emphasis has of late been put in developing e commerce legal frameworks as e-commerce technologies offer significant advantages over traditional business practices.[142] The law has to change with time to accommodate the new commercial practices to existing structures of national and international law and [143]balance the requirement of paper which consistently limits the acceleration of e-commerce.[144]

Commercial activities depend on laws that regulate execution of contracts, their validity, conditions, enforcement, limits of liability, and resolution in case of conflict. There is need to enact, amend and harmonise legislation [145] to enable it apply to such new forms of trade.

Passing such legislation to the adoption of e commerce is also an important indicator of economic success.[146] It is crucial to address fear and uncertainty [147]which is one of the main reasons behind the sluggish growth of online retailing. Others include the inadequacy of the law among other social, economic, political, organisational and cultural aspects.[148] In this new

---

[141] Paragraph 51, explanatory note by the UNCITRAL secretariat on the UNICIC, UN publication sales no. E.07.V.2.

[142] OECD ,*Report on cconference on empowering e-consumers strengthening consumer pprotection in the internet economy* , Washington D.C., 8-10 December 2009.

[143] Boss, Amelia H, *Searching for security in the law of e-commerce.* Nova Law Review 23.2 (1999): pg 58

[144] Ritter, Jeffrey B. and Judith Y. Gliniecki, *international electronic commerce and administrative law: the need for harmonized national reforms.* Harv. JL & Tech. 6 (1992): p 263-264.

[145] Thomas J. Smedinghoff, the legal challenges of implementing e-transactions 2008, op cit.,p14.

[146] 1st Africa e Business, case studies 2005-2006.

[147] Coase, Ronald H. (1937), *'the nature of the firm',* economica, 4, New Series, November, p. 392.

[148] Prasad Bingi , Ali Mir & Joseph Khamalah (2000), *the challenges facing global e-commerce*, information systems management journal p3.

borderless and transient sphere, the consumers' needs to feel protected in aspects of fair trade, privacy, secure payment mechanisms and morality. [149]

2.2 THE KENYAN ICT POLICY

Kenya appreciates the importance of e-commerce and has an ICT Policy. Its policy objectives are to encourage and accelerate investments and growth in IT hardware, software, Internet, training, IT enabled services, telecommunications and electronic commerce.[150]

It also provides for strategies the Government would use to achieve the policy objectives. The Government has undertaken to enact legislation, carry promotional campaigns, raise public awareness on potential opportunities and promote collaboration with the international community in developing an equitable framework for e-commerce.[151]

2.3 HISTORICAL BACKGROUND OF THE LEGAL FRAMEWORK IN KENYA

The Communications Authority roles include to license, regulate the use of the licence and other telecommunications services in the country.[152] The Cabinet Secretary for ICT is given powers to issue to the Authority general guidelines relating to the operation under the Kenya Information Communication Act.[153] The Commission which was the predecessor of the Authority was established after the Communications Act unbundled the KPTC into five separate entities including the[154]Authority , the National Communications Secretariat, Telkom; Postal Corporation of Kenya and Communications Appeals Tribunal.

Section 5(4) of the Act mandates the Authority in the performance of its functions to have regard to any policy guidelines and Kenya's obligations under any international treaty or agreement relating to the provisions of telecommunication, radio and postal services.

---

[149] John Dickie ,*producers and consumers in EU e-commerce law,* (2005 Oxford: Hart) p 111.
[150] Ibid Section 3.2 (g) .
[151] Ibid Section 3.3.2 .
[152] Section 5 Act no 1 of 2009.
[153] Section 5C of the Kenya Information and Communication (Amendment) Act, 2013.
[154] Kenya information and communications act no. 2 of 1998.

The Act enhanced the regulatory scope and jurisdiction of the Authority, and effectively transformed it into a converged regulator especially with regard to e commerce. The enactment of the Act and subsequent amendments took into account the

a) *EAC Legal Framework for Cyber laws 2008,*
b) *UNCITRAL Model Law on Electronic Commerce,*
c) *The 2005 United Nations Convention on the use of Electronic Communications in International Contracts and the,*
d) *OECD Guidelines among other international treaties or agreements.*[155]

2.4 East African Community Legal Framework for Cyber laws 2008

The EAC became the first region in Africa to adopt a modern and effective regional harmonized framework for cyber laws in 2009[156] with a goal to meet the need of the region to support the regional integration and e-commerce.

The EAC Task Force on Cyber laws in cooperation with the support of UNCTAD prepared the legal framework for the EAC in two sets of phases.[157] Phase one covered electronic transactions, electronic signatures and authentication, cybercrime as well as data protection and privacy adopted in 2010.[158] Phase II covered intellectual property rights, competition, e-taxation and information security and was passed by the EAC in 2012.[159]

2.5 UNCITRAL Model Law on Electronic Commerce

The United Nations Commission on International Trade Law developed the International "Model Law" governing electronic transactions in 1996. The model law has served as the basis for legislation enacted in several countries including Kenya. It was meant to promote harmonization and unification of international trade law and remove unnecessary obstacles caused by

[155] Guidelines for consumer protection in the context if electronic commerce 2000.
[156] UNCTAD Report 2012, *harmonizing cyber laws and regulations; the experience of the E.A.C* p iii.
[157] Ibid p iii.
[158] UNCTAD Report 2008, draft EAC legal framework for cyber laws p 4.
[159] UNCTAD Report 2011, framework for cyber laws in EAC phase 11 p 2.

inadequacies and divergences in the law affecting trade.[160] It was to guide state enact commercial laws that are accessible and predictable.[161]

The traditional paper based law imposed restrictions on the use of modern means of communication by prescribing the use of the words "written," "signed" or "original" documents. [162]The Model Law adopted a functional equivalent approach to address the restrictions.

2.6 2005 U.N. Convention on the use of electronic communications in international contracts and the Kenya law.

The 2005 UNICIC *(the "Convention")* is the leading international legal instrument governing international e-commerce transactions. The General Assembly adopted it on 23 November 2005 by resolution 60/21 and was opened for signature on 16 January 2006.[163]

The purpose of the Convention was to offer practical solutions for issues related to the use of electronic means of communication in connection with international contracts.[164]It was not intended to establish uniform rules for substantive contractual issues that are not specifically related to the use of electronic communications. [165] It seeks to promote certainty and predictability in international contract, enhance the principles of non-discrimination, technological neutrality and functional equivalence which are key elements of e-commerce.

The Convention does not attempt to define a computer-based equivalent to any particular kind of paper document but enables an electronic communications to enjoy the same level of legal recognition as corresponding paper documents performing the same function.[166]

It only applies to all electronic communications exchanged between parties whose places of business are in different States when at least one party has its place of business in a Contracting

[160] Paragraph 123, guide to enactment of the UNCITRAL model law on e- commerce (1996)
[161] Current issues of e-commerce law, Professor Michael Geist, University of Ottawa, Faculty of law op cit p3.
[162] Boss, Amelia H (n 138) pg 58
[163] Explanatory note (n 136) Paragraph 1.
[164] Ibid Paragraph 3.
[165] Ibid Paragraph 4.
[166] Ibid paragraph 51.

State.[167] Its scope of application is restricted [168]as it focus of the Convention is on the relations between the parties to an existing or contemplated contract and not to the exchange of communications or notices between the parties to a contract and third parties.[169]

2.7 The Kenya Information and Communication Act (KICA)

This Act [170]is the main statute that regulates e-commerce in Kenya. It establishes the Communications Authority whose functions include to [171]

(a) facilitate e-transactions;

(b) eliminate barriers such as uncertainties on writing and signature requirements;

(c) promoting public confidence, integrity and reliability of e-records and e-transactions;

(d) foster development of e-commerce in any electronic medium and develop sound frameworks to minimize forgery and fraud in e-commerce.

The development of the law hinges on the fact that barriers to e-commerce at both the global and national level are to a great degree the vestiges of a commercial law system based on paper.[172] The law seeks to address several aspects of e commerce including transactions, consumer protection, e -signatures, identity, attribution, data protection, online crime, intellectual property, taxation, admission of evidence, security, offences and jurisdiction.

2.8 Electronic Transactions

A legal contract requires the consent of both parties. In an online environment, the acceptance of an offer is made by the "mouse click on icon" method. A "click wrap" agreement is made when the terms and conditions of the contract of sale are shown on a commercial website.

---

[167] Article 1.
[168] Article 2.
[169] Explanatory note (n 136) Paragraph 15.
[170] Cap 411A.
[171] Section 83C of cap 411A.
[172] Boss, Amelia H,(n 138) p 587.

The term 'electronic transactions' is not confined to commercial agreements for the purchase of goods, products or services, but also encompasses interactions with government and administrative bodies, in either a commercial or non-commercial context. [173]

Section 83G[174] similar to Article 8 of the Convention gives legal recognition to electronic communications. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.

Section 83H of the Act adopted from Article 8 (1) clarifies that the form in which information is presented or retained cannot be used as the only reason for which it can be denied legal effectiveness, validity or enforceability. [175]Section 83I of the Act provides on the retention of information in original form and that that requirement is met if it is an electronic record while Section 83M provides on the acknowledgement of receipt.

The criteria for assessing integrity is whether the information has remained complete and unaltered save for any change that arises in the normal course of communication, storage and display.[176] These should be applied with care as t he adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security and the costs than in a paper-based environment[177].

The Kenyan law however limits the scope of on e- transactions by excluding its application to any law requiring writing or signatures in matters relating to the creation or execution of a will, negotiable instruments and documents of title.[178] The Cabinet Secretary is given the power to order or modify the provisions of subsection (1) by adding or removing any class of transactions or matters.

[173] Ibid P 6.
[174] Cap 411A laws of Kenya .
[175] Explanatory note (n 136) Paragraph 129.
[176] Article 9 (5).
[177] Explanatory note (n 136) Paragraph 134.
[178] section 83 b of cap 411 a

2.9 Formation and validity of contracts through Data messages

The model law[179] and the Act[180] provide that an agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages. ICC e-Terms 2004 confirm that the use of electronic messages shall create valid and enforceable rights and obligations between them. They are admissible as evidence, provided that they are sent to addresses and in formats, if any, designated either expressly or implicitly by the addressee.[181]

There has been a debate as to the extent to which parties offering goods or services through open, generally accessible communication systems, such as an Internet website, are bound by advertisements made in this way.[182] The UNICIC (2005)[183] confirmed that a proposal to conclude a contract made through electronic means which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems amounts to invitation to make offers rather than an offer whose acceptance binds the offering party.

Automated message systems for contract formation are recognised regardless of whether a natural person reviewed or intervened.[184] Such contract shall not be denied validity or enforceability. The Convention allows participation by regional economic integration organizations which can assume rights and obligations of a contracting state.[185]

The limitation is that the provisions of the convention apply to contracting states or may become a contracting state to the 1958 convention on the recognition and enforcement of arbitral awards, and convention on the limitation period in the sale of goods, among others.[186]

[179] Article 11.
[180] Section 83K and 83J cap 411a laws of Kenya.
[181] ICC e-Terms 2004 , Article 1.
[182] Explanatory note (n 136) Paragraph 197.
[183] Recommendation 5
[184] Art 12.
[185] Art 17.
[186] Ibid.

2.10 The Evidence Act[187] and e-commerce

Section 106 of the Act address a key emerging issues on technological development which is the admissibility of electronic records in a court of law.[188] Section 106B (2) outlines the conditions that must be met.

In order to prove that an electronic signature is that of the person by whom it purports, the court may direct that person or the certification service provider to produce the e-signature certificate and verify the signature purported to have been affixed.[189] A court shall presume that every electronic record or agreement containing the e-signatures of the parties was so concluded and was not altered [190] unless the contrary is proved.[191]

Section 106 has been applied by the Kenyan Courts in several cases. The possible objections were evident in the case of *Nonny Gathoni Njenga and Ano –vs- Catherine Masitsa and Another*.[192] In this case, the Plaintiffs sought the defendant's committal to prison for contempt of Court. The Respondent raised an objection on the admissibility of the DVDs the Plaintiffs intended to rely on by arguing it was secured illegally, constituting an infringement of property rights and that they were taken not from one show but a series over a period of time in contravention of the property rights of Bauhaus Limited.

In reply, the Plaintiffs submitted that under section 106 A and B of the Evidence Act, the only lawful obligation impressed on a party tendering evidence on ICT was to tender a Certificate of the Person responsible for rendering that evidence on ICT form.

The court referred to S.106 B and considered the case of *Republic .V. Barisa Wayu Matuguda* [193]were it observed that:

> *". . . any information stored in a computer. . . which is then printed or copied. . . shall be treated just like documentary evidence and will be admissible as evidence without the*

[187] Cap 80.
[188] Section 106B (1).
[189] Section 106D.
[190] Section 106F.
[191] Section 106G (1).
[192] HCCC No. 490 of 2013.
[193] [2011] eKLR.

production of the original. However, section 106B also provides that such electronic evidence will only be admissible if the conditions laid out in that provision are satisfied."

The court went on to state that:

"..... for electronic evidence to be deemed admissible it must be accompanied by a certificate in terms of section 106B (4). Such certificate must in terms of S.106B (4) (d) be signed by a person holding a responsible position with respect to the management of the device.... Without the certificate this CD is inadmissible as evidence."

The judge on 12th March 2014 held that the said DVDs were inadmissible in evidence as there was no such certificate attached though the Plaintiffs were at liberty to later produce such certificate and the Court would then be able to examine the evidence and evaluate the said DVDs as well as its authenticity.

In the case of *Marble Muruli –vs Hon Wycliffe Oparanya,*[194] the court took a more flexible and general approach. It applied the constitution and the wider rules of natural justice. The respondents argued the CDs did not meet the requirements of S.106B and was possible to manipulate. Justice Said J. Chitembwe noted the objection was grounded on technicalities and reasoned that even if the CDs were produced and watched by the court that did not mean that the court would automatically be convinced with what it would see.

The court was also guided by the case of [195]**,** where Justice Muchelule disallowed the production of a CD as there was no evidence to show that the computers used in its were operating properly and noted that each case has to be determined on its own circumstances.

The judge also addressed his mind to the case of *Obanda V Republic* [196] which had held that the tape recorder, cassette and script of the cassette were all admissible as evidence produced. They were produced subject to confirmation that the recorder worked properly.

[194] Kakamega Election Petition HCCC No. 5 of 2013.
[195] Kisumu election petition number 2 of 2013.
[196] [1983] KLR 507.

2.11 CONSUMER PROTECTION ACT AND OECD GUIDELINES

E-commerce has become an area of focus for OECD because of its trans-border nature and its potential to all countries in economic growth, trade and improved social conditions. OECD has developed policy on ICT infrastructure, taxation, consumer protection, network security, privacy data protection, as well as emerging markets and developing economies.

The OECD Guidelines for Consumer Protection are designed to help ensure the theory of functional equivalence is achieved as well as eliminate some of the uncertainties that both consumers and businesses encounter when buying and selling on line.[197]

In Kenya, consumer rights are enshrined in a number of Parliamentary Acts, all of which have since being consolidated by the Consumer Protection Act.[198] This Act has been developed from the said OECD Guidelines and the EAC Task Force Framework among others with a view to meet the criteria set out in the guidelines. [199] The Sale of Goods Act is specifically designed to protect the consumer against the unfair trading practices.

The OECD Guidelines[200] also known as the general principles have been widely adopted internationally and in Kenya to provide a clear level of protection to consumers in a cyberspace environment . They include:

i. Transparency and effective protection.[201]
ii. Fair business, advertising and marketing practices by giving information in a clear, conspicuous, accurate and accessible manner. [202]Failure to do so would be deceptive [203]
iii. Businesses should provide accurate, clear and accessible information about themselves sufficient to allow their identification and location easily.[204]

[197]Information Society, *guidelines for consumer protection in the context of electronic commerce*, OECD, p 3.
[198] The consumer protection act, 2012.
[199] Part iii - Unfair Practices.
[200] Part two of the Guidelines.
[201] Recommendation of the OECD council concerning guidelines for consumer protection in the context of electronic commerce, guidelines p 4. (OECD recommendations)
[202] Ibid p 4.
[203] Ibid p 14-15.
[204] Ibid p 15.

iv. Provide accurate and accessible information of the goods or services offered; sufficient for consumers to make an informed decision whether to enter into the transaction or not[205]and maintain an adequate record of such information.[206]

v. The consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.[207]

vi. Dispute resolution and redress, the applicable law and jurisdiction need to be clear. [208]

vii. Cancellation right are vital, without reason and within a specified time period [209] though parties have the freedom to derogate by mutual agreement on certain matters.[210]

viii. A consumer has certain protections from liability for fraudulent payments made in the consumer's name, unless negligence is proved. Vendor should perform the contract within a minimum specified period of time or be liable to fully refund the consumer.[211]

These guidelines are technology-neutral, encourage private sector initiatives, participation by consumer representatives, and emphasise the need for co-operation among governments, businesses and consumers.[212]

The Guidelines however apply only to business-to-consumer transactions and not to business-to-business [213] as they are meant to protect the final consumer of goods and services procured through electronic commerce. [214]

In compliance with the guidelines Section 12 (1) of the Act provides on unfair practice, misleading advertisement and the remedy to rescind or sue for damages.[215]

[205] Information Society, *guidelines for consumer protection in the context of e- commerce*, OECD, op cit p17.
[206] Ibid p 16.
[207] Ibid. p17.
[208] OECD recommendations (n 195).
[209] OECD recommendations (n 195) 3.
[210] Ibid p 7.
[211] Ibid p 16-17.
[212] Ibid p 3.
[213] Ibid p 13.
[214] Part one of the guidelines
[215] Section 16.(1) of the consumer protection act, 2012.

The Act provides for disclosure of information on internet agreement[216] which can be text-based internet communications[217]. The consumer[218]has to be provided with an express opportunity to accept or decline the agreement and correct errors before entering into it [219]. He may cancel it any time from the date it is entered into until seven days after he receives a copy.[220] A supplier is required to deliver a copy of the agreement in writing to the consumer within the prescribed period after entering into it [221]

Section 9 provides on unsolicited goods or services. A recipient of unsolicited goods or services has no legal obligation in respect of their use or disposal.[222] .The supplier may not demand payment unless; if at the time of consumption the consumer reasonably believed that the goods or services were meant for his consumption. [223] The consumer may demand a refund of the payment. [224]

The Act clarifies and defines "unsolicited goods or services[225] and the regulation make it an offence for[226] one without the prior consent of the subscriber to send electronic mail for purposes of direct marketing disguising or concealing the identity of the sender, or without a valid address to which the recipient may send a request that the communications cease.

Section 89 (1) establishes the Kenya Consumers Protection Advisory Committee. However, none of its members is from the Communication Authority of Kenya.

There is little being done by governments, businesses and consumer representatives in educating consumers about electronic commerce and to increase business and consumer awareness of the consumer protection framework that applies to their online activities.[227]

---

[216] Ibid Section 31.
[217] Ibid Section 2 (1).
[218] Ibid Section 31 (1).
[219] Ibid Section 31 (2).
[220] Ibid Section 33 (1).
[221] Ibid Section 32 (1)
[222] Ibid Section 9(1).
[223] S Ibid ection 9 (2.
[224] Ibid Section 9 (7).
[225] Ibid Section 9 (8).
[226] Regulation 17.
[227] Information society, *guidelines for consumer protection in the context of e- commerce,* OECD, p 19.

2.12 Electronic Signatures

Section 83O provides on the compliance with requirement for a signature. [228] It is met in if an electronic signature is used that is as reliable as was appropriate for the purpose for which the electronic message was generated or communicated.

Under Section 83P, the requirement for authentication by affixing a signature shall be deemed to have been satisfied if such information is authenticated by means of an advanced electronic signature affixed in such manner as may be prescribed by the Minister. Under S.83R, the minister, can, in consultation with commission make regulations for electronic signatures.

The law places some responsibilities on the signatory to safeguard his electronic signature [229] by exercising reasonable care to prevent unauthorized use of his or her signature, creation data, and, in the case of that data being compromised.

The Commission may grant licences to an applicant to provide electronic certification services.[230] His responsibilities includes issuing , renewing; suspending , reinstate or revoke certificates; conduct personal identification of subscribers; publish accurate information relating to certificates, ensure protection of private information and safekeeping of data security among others.[231]

S.83D prohibit operating an electronic certification system; or update a repository or administer a sub-domain in the Kenya country top level domain (.ke ccTLD), unless licensed under Section 83E. The Regulations, [232] provides on Licence for electronic certification services.

The Regulations prohibit geographic discrimination in recognizing electronic signatures. Certificates and electronic signatures issued within a particular country will have the same legal

---

[228] Section 83O of the Act applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
[229] Article 8 of the UNCITRAL model law on electronic signatures with guide to enactment 2001.
[230] Section 83E (1).
[231] kenya information and communications (electronic certification and domain name administration) regulations, 2010 Regulation 7.
[232] Ibid Regulation 3.

effect as those issued outside it where there is an equivalent level of reliability as measured by international standards, which level they can agree in accordance with applicable law.

However, legal recognition to transactions may be denied on considerations of public policy or as consumer protection so demand. Internationally, the liability of a certification provider is limited to issues relating to [233]the accuracy and assurance, of all information at the time of issuance of the certificate.

Regulation 18 on the other hand provides on the confidentiality of a certification service provider[234] but may, pursuant to an order of the court, disclose information relating to a subscriber without the consent of the subscriber.

2.13 Identity, Authentication and Attribution

Consumer-related transactions on the internet often occur between parties who have no pre-existing relationship.[235] Issues arise as to a person's identity and capacity to enter an electronic contract[236] hence the need for authentication.

Section 83l (1) of cap 411a appreciates the difficulties of proof that would otherwise arise, and the section resolves the issue of attribution by way of presumptions.

Attribution is therefore likely to continue been a big challenge with regard to electronic communications and resultant electronic contracts.

2.14 Data Protection and Online Crime

Data protection though not a new concept, has become an increasingly important issue in the digital age due to e-commerce. Sensitive information stored or shared over the internet can be easily intruded by hackers, viruses or be disseminated to third parties, without authorization, for

[233] Regulation 11 (2)
[234] Regulation 18 (2).
[235] Ashit, S. and Parveen N. "*Legal Issues in E-Commerce*," at p. 4.
[236] Ibid p 5.

some illicit or improper commercial benefit. There is urgent need to have effective laws to guard the same as it is the focal point of individual autonomy.

Companies on one hand argue that their ability to gain information will help them have greater understanding of the consumer's needs. However the law should not allow companies to use this information as they want and the importance of the right to privacy is confirmed by the Constitution of Kenya, 2010.[237]

Kenya does not have a data protection law as the Data Protection Bill of 2013 which was meant to give effect to Article 31(c) and (d) of the constitution, to regulate the collection, retrieval, processing, storage, use and disclosure of personal data and connected purposes is yet to be tabled in parliament or passed into law.

There is therefore real and apparent danger that the privacy of citizens is been eroded through the Internet; without any legal protection or remedies.

2.15 Intellectual Property Rights

Traditionally, IPRs have always been deemed territorial in nature. Earlier laws were designed to protect IPRs in the physical world. The practical implication of these characteristics of IPRs law is that the proprietor of say a patent or trademark has to register or enforce his rights in a particular territory or country.

The internet makes the duplication or dissemination of IPR protected works easy, instantaneous and anonymous. This makes the enforcement IPRs in the virtual, boundless and exterritorial world of e-transactions exceptionally difficult feat.

The EAC Framework appreciated the challenges and recommended Partner States to reform national copyright and related laws to ensure it reflects the use of digital technologies, taking into account the WIPO Copyright Treaty (1996) and other relevant international instruments under

[237] Article 31.

which Partner States have obligations[238] and balancing these interests in a manner that facilitates the development of e-commerce.[239] Intellectual property and e-commerce intersect at many levels and generate a broad range of issues for policy- makers.[240]

IPRs have also been given recognition in the 2010 constitution. Article 11 (1) of the Constitution recognizes culture as the foundation of the nation while Article 11 (2) recognise literature, arts, traditional celebrations, role of science and indigenous technologies in the development of the nation and promote the intellectual property rights.

Section 35 of the copyright Act gives remedies in the event of Infringement which include filing suit and seeking [241]damages, injunction, accounts; or delivery of any article in the possession of the defendant which appears to the court to be an infringing copy.

Due to online anonymity and false names, the Act allows the offended party to bring action against a name purporting to be the author or joint author appearing on copies of a literary as published, who shall be presumed, to be the author unless the contrary is proved.[242]

It is an offence for any person who causes a literary or musical work, an audio-visual work or a sound recording to be performed in public at a time when copyright subsists in such work or sound recording and where such performance is an infringement of that copyright .[243]

A person who has in his possession, custody or control two or more infringing copies of a work in the same form, shall, unless the contrary is proved, be presumed to be in possession of or to have imported such copies otherwise than for private and domestic use.[244]

[238] Recommendation 1.
[239] Ibid P 4.
[240] Ibid P 5.
[241] Section 35 (4).
[242] Section (9).
[243] Section 38 (2).
[244] Section 38 (3).

2.16 E-commerce and taxation

The internet blurs location, value and character of economic activity, making application of either residence-based or source-based taxing rights difficult and double taxation more likely. An internet environment also make it difficult to know if a customer is acting as a business or a consumer [245] hence not clear whether to use self-assessment mechanism, input tax or output tax for businesses.

The VAT Act [246] recognises e-commerce and technology and define information technology. Section 8 (3) widely defines electronic services as any of the services provided or delivered through a telecommunications network.

The issue of permanent establishment of supply[247] and fact that taxation can be done through application of IT is provided for in the Act.[248] Section 38 (1) approves an application for registration; returns, statements, payments, notices or any act to be carried out by use of information technology. The law however gives the Commissioner power to exempt [249]any person or class of persons from carrying out tax formalities and procedure by use of IT.

Section 39 (1) of the Act gives the Commissioner the powers to establish and operate a procedure for electronic filing of tax returns, other documents and service of notices without the filing or delivery of any equivalent document or counterpart in paper form.[250]

The Act promotes personal data protection and information cannot be divulged to any other person, without the prior written consent of the Commissioner[251]and contravening these amounts to committing an offence. [252]

[245] Ibid p 21.
[246] VAT act of 2013 cap 469 laws of Kenya .
[247] Part iv of the act.
[248] Part x of cap 49 laws of Kenya .
[249] Section 38(2).
[250] Section 39 (5).
[251] Section 39 (7).
[252] Section 39 (8).

The Customs and Excise Act [253] makes its an offence for anyone to [254] attempt or to gain access to any tax computerised system or uses or discloses such information so obtained for a purpose that is not authorised; or use, disclose, publish, or otherwise disseminates such information,

The major challenges in Kenya include the lack of attention to e-commerce as a unique industry in the VAT Act and the lack of unique policies to regulate the sector. There is lack of proper and adequate resources, and their usage, within the taxation authority to monitor the industry.

2.17 Security

Online fraud and crime remains a big obstacle against harnessing the full potential of ICT. Criminals often make a counter-invention to each noble advancement in ICT. A proper legal regime on e-transactions, must have effective sanctions against such vices such as identity theft; phishing; online defamation, online fraud; and impersonation among others.

An adequate and effective legal framework should have capacity to deal with e commerce issues, national network security, cyber-crime and terrorism; and to establish mechanisms for international cooperation to combat cross-border crimes and collaboration with the relevant institutions. [255]

Under Section 83N, a record shall be deemed to be a secure electronic record from the point and time of verification. This is not enough and the law should ensure that entities will ordinarily address security risks related to the recording and processing of e-commerce transactions through their security infrastructure and related controls. The state should however still retain overall control of security matters which cannot be left to private companies.

[253] Section 159C (1) of the Act.
[254] Section 40 (1).
[255] Ibid Section 2.11.

A consumer over charged through a credit card can request,[256] the issuer to cancel or reverse the charge and any associated interest or other charges [257] when payment is made contrary to the Act and can commence action against to recover the same, interest and other charges. [258]The law [259]defines payment instrument as any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services, or otherwise make payment.

The Central Bank may, by notice in the Gazette, designate a payment system if it is of the opinion that the payment system poses systemic risk; is necessary to protect the interest of the public; or is in the interest of the integrity of the payment system. [260]

There is also a payment system body whose objects is to manage and regulate, all matters affecting payment instructions .It provides to the forum for consideration matters of policy, act as a medium for communication and deals with and promote interests of members to foster co-operation among them.[261]The rules of the body empower it to allow a bank, an institution or a branch of a foreign institution that is not a Central Bank settlement system participant to clear on behalf of other banks, foreign institution, and their branches that are not a Central Bank settlement system participant: [262]

Regardless of these efforts by the central Bank on the payments systems, security risks remain a key challenge to e transactions in general and Kenya has to do more to enhance security.

2.18 Offences

Various laws have created various offences with a view to improve on security. Section 27 (1) and 2), [263] deals with the use of confidential information for personal gain. It is an offence for any officer of the Central Bank or employee of a payment system to make use of any information

[256] Section 83 (4).
[257] Section 83 (1).
[258] Section 83 (6).
[259] The national payment systems act, 2011, no 39 of 2011.
[260] Ibid Section 3 (1).
[261] Ibid Section 8.
[262] Ibid Section 8 (2) d.
[263] Act no 39 of 2011

acquired in the performance of his functions for his personal gain or give misleading advertisements. [264]

It is an offence to access to computer data or system unauthorized [265]or with intent to commit offences[266] However; the issue of intent has always been a private state of mind and can always raise challenges especially when it comes to proving.

It is also an offence to modify computer material without authority. [267]Section 83X (3) however exempts from liability a person acting in reliance of any statutory power.

Being in possession of any data or program with the intention to commit or facilitate the commission of an offence is an offence.[268]The same applies to any person who discloses any password, access code, or any other means of gaining access to any program or data for any wrongful gain and unlawful purpose [269] However this does not appreciate that most disclosures of passwords, access codes among others is done through force, robberies or even kidnappings. There is need to exempt any person disclosing any such information under those circumstances.

It is an offence of unlawful possession of devices and data[270] to manufacture, sell, procure for use, import, distribute or makes available a computer system or any other device for the purpose of committing any offence under sections 83U to 83Z.

Under Section 84B one commits an electronic fraud offence if he fraudulently causes loss, alteration, deletion or suppression of data; interference with functioning of a computer system, with intent to procure for himself or another person, an advantage.

Any person who knowingly creates, publishes or otherwise makes available an electronic signature certificate for fraudulent or unlawful purpose commits [271]an offence. The same applies to

[264] Ibid Section 29 (1).
[265] Section 83u of cap 411a.
[266] Section 83v.
[267] Section 83x.
[268] Section 84a (3).
[269] Section 83z..
[270] Section 84a.
[271] Section 84e.

unauthorized access to access protected systems[272]. It is an offence to intentionally conceal destroys or alter any computer source code, programme, system or network.[273]

Re-programming[274] changing identity, interfering with the operation of the mobile identity, amounts to an offence. It was meant to curb the rampant mobile sets theft which find their way back into the market after been re-programmed. Despite having this strict law, mobile theft and reprogramming is still very common in Kenya.

The law now regulates the registration of SIM-Cards. [275] An operator before selling a Sim card it is required to obtain from natural persons and from corporate persons all their details .Any Sim card lost or stolen should be reported to a telecommunications operator or police.[276]

Damage to ICT infrastructure through economic sabotage or theft, renders them unreliable or unusable until repaired. To mitigate this negative trend, legal revisions have been introduced through the Energy[277] and communications Act[278] to have such damage recognized as an economic crime and increased the penalty to a fine of not less than five million shillings or to imprisonment for a term of not less than ten years, or both.

Complementary proposals to amend the Scrap Metal Act have been made to require licensing of scrap metal dealers and introduce a tighter operations regime.

2.19 Jurisdiction

Companies that engage in e-transactions could easily be overwhelmed by a deluge of legal claims in multiple jurisdictions based either on the information in their website or defects in the products they sell. This poses serious challenges with regard to planning and product design, as different countries have different contract, tort, consumer protection, licensing and regulatory laws

[272] Section 84f.
[273] Section 84 c
[274] Section 84h
[275] Section 27a. (i)
[276] Section 27 c.
[277] Cap 314 laws of Kenya.
[278] Cap 411a laws of Kenya.

as well as environmental protection standards. The claims could arise in tort, contract, taxation, statutory or regulatory compliance requirements.

Some e-commerce related issues which give rise to jurisdictional challenge include adherence to national and international privacy; the legality of particular activities, such as Internet gambling; money laundering; and violation of intellectual property rights.

The ICC e Terms 2004 and the ICC Guide to electronic contracting offers a response to some of these challenges. By agreeing to abide by ICC eTerms 2004, the parties intentionally agree to contract electronically[279] and do not have a dispute about the technical means by which they had contracted.

Secondly, ICC recognises that the speed and ease of electronic contracting bring with them not only opportunities but also concerns which can be allayed in-house, through sensible, practical and flexible precautions, rather than through international legislation or through contract terms. [280]Parties can signify their intention to agree to ICC eTerms 2004 [281] by

a) incorporating ICC eTerms 2004 by reference into any contract
b) indicating the types of contract and the periods to which it will apply and
c) Exchange electronic messages indicating that they agree to ICC eTerms 2004.

The effect of the eTerms , is safeguarded by the basic principle of freedom of contract.[282]. However, the ICC terms have their limitations in that they;

a. are not themselves the contract between the parties, setting out the substantive rights and obligations. These will be contained in the contract itself, which ICC eTerms 2004 facilitate but not replace.

b. do not resolve all the possible issues which may arise regarding the conclusion of the contract. This are dealt as per the standard and contract terms. [283]

[279] ICC e-terms 2004,ICC guide to electronic contracting, p 2.
[280]Ibid p 2.
[281] Paragraph b.1, p 5.
[282] Ibid paragraph b.2, p 6.

The purpose of ICC eTerms 2004 is to provide uniform terms that allow the parties to contract electronically without running the risk of one or other of them later raising the electronic nature of their contract as a ground for its invalidity.[284]

2.20 Conclusion

The laws on technology keep on changing with changing times raising a tremendous challenge globally, which are being dealt with nationally and internationally. Solutions to the issues arising arise beyond national concerns and would thus have to be more acceptable to the majority of the states.

It is for this purpose why the UN developed the harmonised Model law and Conventions to guide nations address their e- commerce concerns which apply across national borders.

More worryingly, courts and tribunals have occasionally denied legal recognition to electronic documents due to complex procedure to have it admitted and in spite existence legal framework recognising the same. Some states are yet to establish legal or administrative mechanisms for the cross-border exchange of information on mutual legal recognition of incorporation certificates, licenses, requirements and permits.

There is also need for the respective states to continue to closely follow international developments on the law on e commerce towards finding internationally acceptable and harmonised legal rules to address the continuing challenges.

[283] Ibid paragraph b.3.
[284] Paragraph b.3, p 7.

CHAPTER 3

AN ANALYSIS OF THE EFFECTIVENESS OF E -COMMERCE LAW, AND LEGAL CHALLENGES IN KENYA

3.1 Introduction

E-commerce law should be enacted in such a way as to ensure practical solutions for e commerce issues in both local and international contracts.[285] The old trend of establishing uniform rules for substantive contractual paper based issues is changing as evident from the legislation so far enacted to address technological development and as covered in the previous chapter.

Kenya has been at the forefront in the region in formulating e-commerce policy and legislation. The law is meant to reaffirm the principle of functional equivalence where substantive rules are needed in order to ensure the effectiveness of electronic communications.[286]

There has also been an effort to harmonize e-commerce legislation through the EAC Framework. It is this laws that this chapter examines and analyse its effectiveness and whether the desired progress has been achieved.

3.1.1 EFFECTIVENESS OF E -COMMERCE LAW, AND LEGAL CHALLENGES IN KENYA

3.2 Online contracts, Terms, Conditions, Policies and Laws

At the moment, most online agreements are drafted by private businesses without any state control. Current e-commerce law does not generally address or have standard form electronic contracts. Consumers do not have an equal playing or bargaining power and most terms are unilaterally imposed without any remedy.

[285] Paragraph 3, explanatory note by the UNCITRAL secretariat on the UNICIC , UN Publication Sales No. E.07.V.2.
[286] Ibid Paragraph 4.

The Communication Act recognises e-transactions and information even when in electronic version. It however exempts certain transactions such as the creation or execution of a will, negotiable instruments and documents of title.[287]Such limitations do not exist in countries like Australia where even electronic transfer of land is recognised.

There are no local cases nor are there many reported cases dealing with electronic contracts internationally. The foreign cases interpret the significance of shrink-wrap software license contracts where it is argued that accessing the software constitutes acceptance of the terms. [288]

The lack of consistent body of case law analyzing the rights and responsibilities of the parties to electronic contracts reflect the absence of any broad consensus regarding how Kenyan contract law should be adapted to apply to new forms of transactions. There is also considerable support preserving a role for government oversight in online markets.

In the early shrink-wrap cases, US courts showed a reluctance to enforce strict standard form contracts. In the case of *Arizona Retail Systems, Inc. v. Software Link, Inc.*[289], the court held that shrink wrap license might be part of the contract with regard to the first sale of a copy of software. The licensee placed an order by telephone after having inspected the first copy. The licensor did not insist in that phone call that the terms in the form contract were part of the agreement. The shrink wrap license terms were deemed not to be included in the subsequent telephone order contract.

In later cases, however, courts have been more willing to enforce all the terms in shrink wrap licenses. In *ProCD, Inc. v. Zeidenberg*, [290] the facts were that ProCD used to sell computer software and the defendant bought some with the intention of having a good price arbitrage. Every box containing the product declares licensing agreements on each CD when prompted. It limited use of operation to non-commercial purposes. The defendant bought the software and used it for

[287] Section 83B.
[288] Unfair contract terms directive 93/13/EEC, [1993] O.J. L 95/29, Annex to Art. 3 (3).
[289] 831 F. [1993} Supp. 759.
[290] 86 F.3d 1447 (7th Cir. 1996).

commercial purposes, re-selling it on the Web. ProCD brought this suit against Zeidenberg for infringing the terms of use agreement.

The Defendant's argued that the Package of software is the "offer" and the customer "accepts" by paying the asking price when he buys the good. He argued he could not agree or be bound to hidden terms though he had a chance to return the product.

The court rejected the buyer's claim and held that the terms of that shrink wrap license were not unconscionable and therefore enforceable because no contract was formed until the buyer "accepted" the terms of the license by agreeing to keep the software. [291]

The *Hotmail Corporation v. Van$ Money Pie Inc.*,[292]was the first case were it was implicitly held that a click wrap contract, specifically a "Terms of Service" e-mail agreement, is valid. It also addressed other issues such as Jurisdiction and Venue.

In *Mortenson Company, Inc. v. Timberline Software Corporation*,[293] the Supreme Court held that the limitation on consequential damages contained in a shrink wrap license was enforceable against a licensee who submitted a construction bid $1.95 million less than it should have been due to a malfunction by the software.

In *Hill v. Gateway 2000, Inc.*[294] the Judge held that the preprinted form contract enclosed with a computer Hills had ordered by telephone from Gateway was enforceable as the purchaser had not exercised his right to return the same within 30 days if terms were not acceptable. The court of appeal held that in order for an arbitration clause to be valid, the purchaser need not receive notice of the clause apart from the terms and conditions of sale and the clause need not be otherwise prominent or stand out. Secondly, an allegation that an arbitration clause is part of a scheme to defraud does not render that clause unenforceable.

---

[291] *ProCD, inc. v. Zeidenberg*, 1996 908 f. supp. 640
[292] 47 U.S.P.Q. 2d 1020, 1998 WL 388389.
[293] 140 Wash.2d [2000] 568; 998 P.2d 305; 2000 wash. lexis 287 (wash. 2000).
[294] 105 F.3d [1997] 1147.

In *Edmond v. Gateway 2000, Inc.*[295], a court stayed the proceeding before it and required a consumer to submit to arbitration a dispute regarding the adequacy of the customer service based on the terms of a service contract. However, in *Brower v. Gateway 2000, Inc.*,[296] an appellate court in New York held that, although the terms of the preprinted form contract were generally enforceable, its arbitration clause was unconscionable and unenforceable as arbitration to ICC was excessively costly and deterred individual customers from invoking arbitration process.

In *Klocek v Gateway, Inc.*,[297] the court refused to dismiss the plaintiff's complaint based on a mandatory arbitration clause. It rejected Judge Easterbrook's reasoning in *Pro-CD* and *Gateway* as unpersuasive. If a contract was formed at the time of a telephone order, then the printed form shipped inside the box with the computer would only be an offer by Gateway to modify the terms of already formed and the mandatory arbitration provision in the contract would not be binding.

There has not been a common agreed position to address these challenges. Enforceability of online transaction including the arbitration clauses are still a challenge in view of their practicability and expense. The law should not wait for the consumer to retain the merchandise beyond the 30-day period to justify an unlawful transaction and make it enforceable even if there was no disclosure.

3.3 Privacy and protection of data

The Constitution guarantees **e**very person the right to privacy.[298] . It does not however provide the mechanism to ensure this provision is realised.

Cap 411A [299] address issues of privacy and data protection in very general terms. It does not appreciate that personal data remains to be the fuel of the internet economy, with a wide range of digital products and services made available for free, but in reality being offered in return for

[295] 29 Conn. 2001, L. Rptr. 456. *Westendorf v. Gateway 2000*, Inc., 41 Ucc Rep.
[296] 246 A.D.2d 246, 37 U.C.C. Rep. Serv. 2d (CBC) 54 (N.Y. App. Div. 1998)
[297] 104 F. Supp. 2d 1332 (D. Kan. 2000); later dismissed on other grounds, 2000 WL 1372886 (D.Kan. 2000
[298] Article 31 of the constitution of Kenya 2010.
[299] The Kenya information and communications Act.

the grant of rights to use the customer's data for marketing purposes. The law need to control such use and abuse of personal data, impose obligations on those processing such data and grant rights to the individual whose data is being processed.

The Act gives the Cabinet Secretary Powers to declare any computer system a protected Information System. This is not adequate as it leaves a question and uncertainty on the status of the undeclared systems engendering trust in e-commerce transactions.

The Act provides that an electronic record shall be deemed to be a secure electronic record from the point of time of verification.[300] It guarantees no clear protection of the individual from illegal collection and use of personal information by either the government or private companies.

Kenya does not have a data protection law and systems in place yet consumers do not realize that when they go browsing on the Internet, they leave behind "digital footprints" in the form of cookies or even permanent files that can collect data about the user's identity, address, age, income, interests, and online purchases.[301]

The Internet is one of the biggest data-collection machines and marketers want to gather as much personal information as possible[302] yet there is no effective remedy to internet users as the current laws are not effective in curbing the vice.[303] E-commerce Information from census databases, telephone companies, motor vehicle databases, health and education records, and credit reports, is not protected. The holders can compile and sell data that would be prohibitively expensive to gather by traditional means.[304]

Using online technology to gather, exchange and sell personal information about consumers is illegal in many countries such as European Union. European consumers have the right to check on data that is held about them and to prevent its use.

[300] Section 83N of the kenya information and communications (amendment) act.
[301] Zugelder, Flaherty and Johnson, 2000.
[302] Ibid.
[303] The economist, 1998).
[304] Business week, 1999b.

E commerce is a global concern and UNCTAD has been in the forefront to ensure countries enact laws with regard to e-transaction laws, consumer protection, privacy, data protection, and cybercrime. These laws are essential to create trust online and to secure electronic transactions. There is considerable variation as to the legislation, its adequacy and effectiveness in different regions and countries .The adequacy and effectiveness of the law is generally high in developed countries, but inadequate in many other parts of the world as confirmed by the table below [305]

	Countries (number)	**E-transactions Laws (%)**	**Consumer Protection Laws (%)**	**Privacy and data protection laws (%)**	**Cybercrime laws (%)**
Developed economies	**42**	**97.6**	**85.7**	**97.6**	**83.3**
Developing economies					
Africa	**54**	**46.3**	**33.3**	**38.9**	**40.7**
Eastern Africa	**18**	**38.9**	**16.7**	**27.8**	**50**
Middle Africa	**9**	**22.2**	**22.2**	**22.2**	**11.1**
Northern Africa	**6**	**83.3**	**33.3**	**50**	**66.7**
Southern Africa	**5**	**60**	**40**	**20**	**40**
Western Africa	**16**	**50**	**56.3**	**62.5**	**37.5**
Asia and Oceania	**48**	**72.9**	**37.5**	**29.2**	**56.3**
Eastern Asia	**4**	**75**	**50**	**25**	**50**
South-Eastern Asia	**11**	**81.8**	**81.8**	**54.5**	**72.7**

[305] *UNCTAD : Cyberlaws and regulations for enhancing e-commerce 14 January 2015 : Case studies and lessons learned Note by the UNCTAD secretariat 12*

Southern Asia	**77**	**22**	**44**	**46**	**6.7**
Latin America and the Caribbean	**33**	**81.8**	**54.5**	**48.5**	**63.6**
Central America	**8**	**75**	**87.5**	**37.5**	**37.5**
South America	**12**	**83.3**	**75**	**66.7**	**75**
Caribbean	**13**	**84.6**	**15.4**	**38.5**	**69.2**
Transition economies	**17**	**100**	**11.8**	**88.2**	**70.6**
All economies	**194**	**74.7**	**47.4**	**55.2**	**60.3**

The law in Kenya has not addressed all issues on personal data arising from mobile phones use. For instance, blue tooth uses short-range wireless signals and can link a mobile phone to a headset, a keyboard or a mouse to a computer and a laptop to a printer, among others. Its use presents the following privacy threats:

i. Blue snarfing, which is the unauthorized access to personal data.
ii. Blue bugging, which allows an unauthorized person to take control of another person's phone, allowing them listen to conversations, make calls and send messages
iii. Blue jacking, which is the sending of unsolicited messages via the Bluetooth technology, to other Bluetooth-enabled devices.

Further, law in Kenya does not clearly define what constitutes processing of personal data nor does it lay specific rules to allow monitoring of personal data. In *Bodil Lindqvist,*[306] the CJEU held that "the act of referring, on an internet page, to various persons and identifying them by name or by other means constitutes 'the processing of personal data within the meaning of Article 3 (1) of Directive 95/46".

[306] 218 C CJEU [2003], C-101/01 *Para 27, 68 and 69.*

There is a challenge of a balance between personal data and the right of freedom of expression envisaged in the constitution .In the case of In *Z. v. Finland*[307], the applicant's ex-husband, who was infected with HIV, had committed a number of sexual offences. He was subsequently convicted of manslaughter for knowingly exposing his victims to the risk of HIV infection. The Court ordered the full judgment and documents to remain confidential for 10 years despite requests from the applicant for a longer period of confidentiality. These requests were refused by the Court of Appeal, and its judgment contained the full names of both the applicant and her ex-husband. The ECHR held protection of medical data as of fundamental importance to the enjoyment of the right to respect for private and family life. It concluded that granting access to the applicant's identity and medical condition as described in the Court of Appeal's judgment after a period of only 10 years after passing the judgment would violate Article 8 of the ECHR.

The scope of the Kenyan 2013 draft Bill is limited as it addresses personal information held by public authorities but does not come out clear with regard to private entities. National data protection laws across the world, apply to both public bodies and private bodies such as corporations and non-profit bodies.

A weak data protection law substantially limits the usefulness of the law as a means to enhance international trade and affects the country when it comes to dealing with other states. The European and many other countries have laws that limit the transfer of personal information for outsourcing and other reasons to only countries with adequate data protection laws, which is why many countries in Africa, Asia and Latin America have adopted laws recently.

Kenya has to protect journalists who publish personal information in the public interest, by putting in specific exemptions for information collected for journalistic, academic for media or artistic purposes.

In addition, the right of individuals to obtain their own records is limited by broad exemptions such as for national security, commercial and economic reasons. It should have fewer exemptions

[307] 304 ECtHR, Z –VS-Finland No. 22009/93, 25 February 1997, paras. 94 and 112; see also EctHR.

when individuals demand access to their own information since it is a right designed to protect the persons 'own rights.

A large number of regulations and judicial interpretations have provided privacy protection, but their contents are scattered in different laws. The general principles of civil law do not provide the concept of right to privacy. It does not entitle citizens to lodge a complaint or get legal relief as an independent civil right when right to privacy is infringed yet such relief is available under the right of portrait and reputation. Right to privacy is seen as a constitutional matter than a civil claim.

The existing laws regarding citizens' right to privacy and data production is inadequate and cannot meet the need of increasingly advanced technology in e-commerce era. More threats to right to privacy are coming out, such as wiretapping, surveillance and video.

The fears that adopting such strict laws would slow the growth in transatlantic e-commerce [308]may not be correct as there has been tremendous growth in ecommerce due to consumer confidence.

3.4 Consumer protection right

The Consumer Protection Act has not been able to achieve the desired results. For instance

a) There are no limits in collection of personal data. Much of it is obtained unlawfully and without the knowledge or consent of the data subject.

b) personal data may not be relevant to the purposes alleged nor is purpose disclosed at time of collection. It is not accurate, complete and kept up-to-date.

c) The limitation principle to ensure Personal data should not be disclosed, made available is yet to be realised.

[308] Jacobson, 1999.

d) There is challenge of protecting data against risks such as loss, unauthorized access, destruction, use, modification or disclosure.

e) Kenya does not have a general policy of openness, practices and clear policies on data and

f) The office of the intended data controller is not effective, there is no data accountability systems, infrastructure nor are there ways to verify data.

In the case of *Minnesota v. Granite Gate Resorts, Inc.*, [309] the Minnesota Attorney General brought suit under the state consumer protection statute alleging that the defendant, a Nevada resident, was liable for deceptive trade practices, false advertising and consumer fraud on the Internet. The defendant's unsuccessful argument was that, as a Nevada resident, he was not subject to personal jurisdiction by the Minnesota courts. This confirms that Consumer protection laws can be used by the states to prosecute fraud, even prospective fraud on the Internet.

The courts have also been faced with a challenge of interpreting what constitutes trade or commerce, consumer fraud and deceptive business practice. In the *Juno Online Services, L.P. v. Juno Lighting, Inc.*[310] the court held that the mere registration of a domain name, without setting up a web site or e-mail service, does not constitute "trade or commerce" or amount to "deception" as required by the Illinois consumer fraud and deceptive business practice statute.

The Consumer protection law lacks clarity and does not provide clear legal sanction to the failure of a supplier to give the required information or to confirm receipt of an order by the consumer. Sections 12 and 32 of the Act address disclosure, unfair trade practices as well as internet agreements in too general terms that may not be practical on a case to case basis. The law gives a general support for disclosure to consumers and does not give any guidelines on how this is to be achieved practically.

[309] 569 N.W.2d [1997] 715.
[310] 979 F. [1997] Supp. 684.

The only direct consequence of a failure to inform the customer on the Web is for the customer to withdraw from the contract, ask for reimbursement [311] or seek damages .However in practice, these remedies may not be practical nor is the ability to litigate internationally.

These sanctions are not sufficient to enforce the law and different countries may be forced to tighten them. Legal consequences such as the invalidity of the contract or a right to payment of damages may easily interfere with national contract law structures. There is need to ensure that the law is harmonised, respected by all parties and an effective disputes resolution mechanism.

The slow growth of e-commerce has been contributed to by lack of trust. Potential customers are still reluctant to transact electronically and do not trust how safe they are especially in giving their credit card details.

The need to continually improve and pass more laws to govern e transactions and in particular consumer protection is a global concern as evident through the efforts by the

a) International Consumer Protection and Enforcement Network (ICPEN) countries who have with a view to check online fraud initiated the Fraud Prevention project through a series of education campaigns run every year under one theme but focusing on an issue relevant to each individual participating agency.

b) African Consumer Protection Dialogue (the 'African Dialogue') which is an effort on behalf of African governments, NGOs, and the U.S. Federal Trade Commission to create informal opportunities to interface with each other, and the rest of the world on consumer protection issues. At its inaugural Conference in August 2009 in Johannesburg, South Africa, participants decided upon a set of priority initiatives which included among others the gathering of African consumer laws and creating a legal framework toolkit for African consumer legislation.

[311] This mechanism has its roots in the distance selling directive, art. 6. litigation.

c) The objectives of UNCTAD's work on consumer protection include among others to assist countries in achieving adequate legal framework and institutions and for the protection of consumers and to Promote policies that strike a balance between consumer protection and minimizing costs to business.

d) UNCTAD offers technical assistance and capacity building support in several areas including drafting of consumer protection policy, laws and related regulations and guidelines;

The global mapping of consumer protection legislation indicates that many developing and transition economies still lack relevant laws[312] Out of the 119 countries for which data are available, 90 (of which 56 are developing or transition economies) have adopted consumer protection legislation that relates to e-commerce. Regionally consumer protection legislation in Africa is particularly low. Only 18 of the 54 African countries have adopted such laws.

3.5 Intellectual property rights

E-commerce has a tremendous impact on IP related issues hence why they are being addressed in legislatures, judiciaries and international fora. The scope of copyrights affects how e-commerce evolves.

Efforts have been made to ensure effective protection and enforcement of rights in the digital era. Copyright industries are also adapting their business methods and use of technology to exploit digital opportunities, while guarding against new risks.

The effectiveness of intellectual property laws is complicated as appreciated and evidenced by the different solutions employed in various jurisdictions. The WIPO treaties mandate signatory countries to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the

[312] UNCTAD, 2015

exercise of their rights under the treaties or the Berne Convention and that restrict acts, in respect of their works, which are not authorised by the authors concerned or permitted by law.

It remains a challenge as to what would be "adequate" legal protection and effective legal remedies and how a fair balance between this protection and fair use can be struck.

The Constitution recognises the role of science and indigenous technologies in the development of the nation; and promote IPRs of the people of Kenya. It has not however given ways how these goals are to be realised.

Though the Act creates certain offences,[313] the law has not been able to cope with the fact that works of intellectual property are being digitized at an incredible pace. One person can send millions of copies all over the world.[314] While it is straightforward to protect 'physical' works with patent and copyright laws, the nature of digital technology encourages copying of digitized intellectual property works, virtually instantaneously, without perceptible degradation in quality.

In order to establish an enforcement framework for online IPRs, the Copyright Act[315] recognizes a computer generated programme to be within the scope of a literary, dramatic, musical or artistic work.

The Industrial Property Act[316] anticipates receipt of industrial designs presented in the form of 'drawings, photographs or other graphic representations' for registration and custody with the Kenya Industrial Property Institute. It however does not specifically cite electronic formats hence not clear as to whether it falls within the broad scope of 'other graphic representation'.

It is therefore evident that the interface between trademarks and domain names in cyberspace is relatively unexplored in Kenya. With the increased adoption of the Internet for business and commerce, and the related enhancement of the commercial value of trademarks in cyberspace, there is need for development of cyber laws in Kenya to address upcoming issues.

313 Section 38 of the copyright act.
314 Intellectual Property on the Internet", A survey of issues. [Copyrights and Related Issues], http://ecommerce.wipo.int/survey/.
315 Cap130 laws of Kenya.
316 Act No 3 of 2001.

3.6 Dispute resolution

ICT knows no borders and geographic location of the contracting parties .The Communications Act[317] is a domestic legislation and does not address the issue of jurisdiction especially where foreign subjects are involved. The 2010 Regulations [318] establishes the dispute resolution tribunal which is only limited to domestic disputes and does not address key e commerce issue especially where cross border disputes arise.

The cross-border enforcement of consumer protection requires effective cooperation between the national enforcement agencies. Some national authorities have set up semi-formal cooperation mechanisms and networks to serve as non legal, political channels of cooperation. For example, ICPEN is a network of public authorities involved in the enforcement of fair trade practice laws and other consumer protection activities, comprised of 56 member countries and organizations including 24 developing countries. Its main objective is to identify ways to prevent and redress deceptive marketing practices in an international context.

It has developed the econsumer.gov initiative to enhance consumer protection and consumer confidence in ecommerce. The website invites individuals to file complaints online at a single location (http://www.econsumer.gov). As of 2014, it comprised 30 national authorities, all of which are also ICPEN members. In 2013, the initiative received 23,437 complaints, many of which related to cross-border transactions.

3.7 Jurisdiction and applicable law

The question of jurisdiction is of importance since the manner in which Kenya may exercise its jurisdiction over foreign subjects for wrongs committed by or against its citizens over the internet must be properly stated in law. In cross-border disputes, the eventual inability for national jurisdictions to enforce foreign judgments may be an additional complication. [319]

[317] Chapter 411 A Laws of Kenya.
[318] Kenya Information and Communications (Dispute Resolution) Regulations, 2010
[319] UNESCAP trade and investment division, staff working paper 02/07.

There are no decided cases in Kenya but courts elsewhere have generally accepted the vision of a borderless Internet as evidenced by their reluctance to consider the possibility that geographic distinctions might be possible online. The *American Library Association's (ALA) v. Pataki* [320] case was a 1997 US case challenging a New York state law that sought to regulate obscene content found online. The court argued that the Internet is wholly insensitive to geographic distinctions and users of the Internet neither know nor care about the physical location of the Internet resources they access.

Although the court's view of the Internet may have been correct at the time, things are changing. Providers increasingly care about the physical location of Internet resources and the users that access them, as do legislators and courts who may want real space limitations imposed on the online environment. In the business world, Canada's Jump TV has garnered considerable publicity for its use of geographic identification technology to limit its Internet retransmission signal to Canadians.

The question of extra-territorial jurisdiction over Web content was raised where Felix Somm, ex-manager of CompuServe Deutschland, was cleared on appeal of pornography charges brought against him in Germany after newsgroups carried on parent company content. The judge determined that it was technically impossible for Somm to close the illegal newsgroups in question. Following in the footsteps of the CompuServe's case, Yahoo argued that it was technically impossible to block only French citizens from access to its online auctions should the auctions contain objectionable items. The Kenyan domestic law is silent on these issues.

3.8 The international rules or treaties that govern Internet jurisdiction

The Hague Conference on Private International Law has been actively working toward developing an international convention on jurisdiction and enforcement of judgements. It has attempted to address a range of issues including jurisdictional rules for consumer and business transactions. The primary issue of contention surrounds on whether to adopt a "country of origin" or "country of destination" jurisdictional approach to Internet consumer disputes.

[320] 969 F.[1997] Supp. 160

The United States, support a "country of origin" approach while most European countries, support a "country of destination" approach that ensures that consumers can always sue in their home jurisdiction. The middle ground is to allow businesses to confine their online activities and thus their legal risk to a limited number of jurisdictions, while ensuring that consumers retain the right to apply their local consumer protection laws to e-commerce transactions.

Kenya has not taken any stand domestically and it is unclear to consumers and the business community on which approach to apply in the event of a dispute. It has not dealt with any case touching on jurisdiction in e- commerce issues.

Courts in the US and around the world have been somewhat inconsistent. Some courts have been willing to assert jurisdiction to virtually any website accessible within their jurisdiction. Others have adopted the "Zippo test" which is a more cautious approach that sets some limits on when a court will assert jurisdiction over a foreign or out-of-state entity whose ties to the jurisdiction are limited to the Internet.

3.9 The Zippo test

It arose out of a Pennsylvania federal court case involving a trademark dispute over the zippo.com domain name. The issue before the court was one of personal jurisdiction arising out of a claim of trademark infringement and dilution.

Rather than using Internet analogies as the basis for its analysis, the Court focused on the prior, somewhat limited Internet case law, generating the following conclusion:

> "*With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages. The cases are scant. Nevertheless, our review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a*

defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet website which is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website."

Although the Court may have conveniently interpreted some earlier cases to obtain its desired result, its critical finding was that the jurisdictional analysis in Internet cases should be based on the nature and quality of the commercial activity conducted on the Internet.

The Canadian courts signalled their approval of the Zippo approach in *Braintech Inc. v. Kostiuk.*[321] This was a 1999 British Columbia Court of Appeal case, involving a series of allegedly defamatory messages posted on a stock chat site by a British Columbia resident.

When the company returned to British Columbia to enforce the judgment, the British Columbia courts examined the appropriateness of the Texas court's assertion of jurisdiction over the dispute. Adopting the passive versus active test by citing directly from the Zippo case, the Court of Appeal ruled that the Texas court had improperly asserted its jurisdiction. It argued that the postings were passive in nature and thus provided insufficient grounds to grant the Texas court authority over the case.

By 2001, many courts were no longer strictly applying the Zippo standard but rather were using other criteria to determine when assertion of jurisdiction was appropriate. Courts in the US moved toward a broader, effects-based approach when deciding whether or not to assert jurisdiction.

321 (1999), 171 D.L.R. (4th) 46 (CA) [leave denied [1999] S.C.C.A. No. 236.

Courts are now relying increasingly on the effects doctrine that was established by the US Supreme Court in *Calder v. Jones*.[322] That doctrine holds that a court may assert jurisdiction over an out-of-state entity where the effects of that entity's activities are felt within the court's jurisdiction.

In the *Yahoo –vs- LICRA* **[323]** case, a French judge asserted jurisdiction over Yahoo, ordering it to implement technical or access control measures blocking auctions featuring Nazi memorabilia hosted on the California-based Yahoo.com site from French residents. Yahoo reacted with alarm, maintaining that the French court could not properly assert jurisdiction over the matter as its primary target was the US audience and was governed by US law and was not intended for a French audience. The company felt confident that a French judge could not credibly assert jurisdiction over the site.

The judge had however commissioned an international panel to determine whether the technological means were available to allow Yahoo to comply with an order to keep the prohibited content away from French residents. The panel reported that though such technologies were imperfect, they could accurately identify French Internet users at least 70 per cent of the time.

Based on that analysis, Judge Gomez ordered Yahoo to ensure that French residents could not access content on the site that violated French law. Failure to comply with the order would result in fines of USD 13 000 per day. Soon after, Yahoo removed the controversial content from its site, but the company proceeded to contest the validity of the French court's order in a California court.

In the *Hotmail Corporation v. Van$ Money Pie Inc.* [324] the trial Court held that it had subject matter jurisdiction over this action as well as supplemental jurisdiction over the state law claims and personal jurisdiction over the defendants as the defendants had engaged in business activities in or directed in California.

[322] 465 U.S. 783 (1984) 465 U.S. 783.
[323] 169 F. [2001] Supp. 2d 1181.
[324] 47 U.S.P.Q. [1998] 2d 1020, 1998 WL 388389

In the recent Court of Appeal case of *Tamiz –vs goggle*[325] , M Tamiz complained to Google about comments on the 'London Muslim' blog hosted by Google which he contended were defamatory in nature. He asked Google to remove that blog. He also sought permission to serve proceedings on Google in California for defamation occurring between his request to Google and the taking down of the offending blog. Agreeing with Google, the Court of Appeal declined jurisdiction and permission to serve on Google in California.

It is therefore not clear nor is there a general accepted practice on how to deal with jurisdictional challenges. Most issues are global and have no geographical boundary. So far, there is no international treaty or a worldwide law governing Jurisdiction.

3.10 Attribution.

Section 83L of the Kenyan law provide on attribution. It is often difficult to identify the actual perpetrator because the computers from which the attack appears to originate will themselves have been taken over and used to relay and magnify the attack commands. This problem of attribution is much deeper and the single provision in the law does not fully address the problem. More provision and /or rules need to be promulgated to address the issue.

3.11 Electronic Payment and the lacuna in the law

E-commerce requires a secure and efficient electronic payment system to develop. With new technology, such payment takes place using a transmission medium not under the control of the financial system. It is therefore necessary to take steps to ensure the security of the messages sent along such a medium.

In April 2011, the Central Bank of Kenya launched the cheque truncation project meant to replace the physical movement of cheques. However the Cabinet Secretary has been given powers to add or remove any class of transactions or matters.[326] These are wide sweeping powers that can

[325] 2013 EWCA Civ 68.
[326] Section 83B (2) of cap 411A laws of Kenya .

be vulnerable to abuse. There is need to ensure consultation with the Communication Authority and stakeholders and to give reasons for such decision to enhance certainty.

Documentation is still important in e-banking due to its nature of man to machine interaction. A terminal receipt is required after any electronic transfer transaction to certify the amount, date, time and balance in the consumer's account. It is a breach of the bank's obligations to its customers not to produce the receipt. This is a common occurrence in Kenya but there is no clear law to guide the consumers on the remedies available. This is made worse by the fact that a similar transaction over a bank-hall counter will in all occasions be evidenced by an audit trail.

The same apply to ATMs. The Bank's obligation to provide a terminal receipt is an implied term of the contract between the cardholder and the financial institution. In the U.S, production of a receipt at an ATM is regulated, and, forms part of the contract and cannot be misapplied by the parties of the contract and breach invites legal liability.

The security concerns remain an important impediment to expanding e-commerce services, hence the reluctance of customers to provide online information about their credit cards. [327]

3.12 Mobile banking

The Central Bank of Kenya intends to retain its liberal approach to regulating mobile money, as it feels that this position has enabled Kenya to take the lead in this space. It has however introduced a number of new regulations that will codify the guidelines that the Bank has been informally enforcing, including a new set of consumer protection rules to ensure more safeguards in the event of service provider insolvency.

The 2010 Agent Banking guidelines finally allow banks the use of non-bank agents, who are not to be exclusive to one bank. Key players are quickly converging, though there is one set of rules for banks and another for MNOs. This has given rise to the issues of systems stability and systemic risk which the government should address urgently.

[327] WTO, 2013, e-commerce in developing countries opportunities and challenges for small and medium-sized enterprises pg 12.

There is also concern that the issue around systemic risk is largely focused on mobile money data records, rather than the safety of the pooled funds involved. Mobile money accounts are prepaid, and the amount of cash in the system must match the amount of e-value, so that a parallel currency is not being created.

The Finance Act, 2011 was meant to compel the registration of subscribers to telecommunication services to improve security.[328] There are however enforcement challenges as simcards are still available in the streets and those selling them do not effectively register and collect all personal details of the buyers.

3.13 Cybercrime and Security

Despite the creation of the various offences under Cap 411A, the country still faces challenges. The offences created are still new hence the need to continue re-looking at the laws, policies, technical standards, enforcement and cybercrime reporting. International standards as well as international cooperation are necessary to address the global extent of cybercrime.

The Kenyan Ministerial Strategic plan[329] admits that some of the emerging issues and challenges the ICT sector has faced in the implementation of the vision 2030-based strategic plan include inadequate legislation, safeguards against crime and ICT media abuse.

The Kenya, the Cyber Security Policy is currently steered by the ICT Authority through the National Cyber Security Master Plan. The key elements of the policy address are Training & Awareness, Economic Impact, Governance, Policy and Legal framework. [330]

To address the security issue, the government through the CCK established KE-CIRT, the Kenya Computer Incident Response Team Coordination Centre, part-funded by the ITU, which brings together government agencies, the Central Bank and Internet expertise from KENIC, TESPOK and KENET to address cyber-attacks. The Kenya Information and Communications

[328] Section 27A Cap 411A Laws of Kenya.
[329] Ministerial strategic plan 2013 -2017 pg 5.
[330] Ibid p 40

(Amendment) Act 2014 expanded the mandate of the Authority with respect to electronic transactions to include cyber security. Though the said Act promoted and facilitated efficient management of critical internet resources and developing a framework for facilitating the investigation and prosecution of cybercrime, it was still not adequate hence the efforts to draft the draft, Cyber-Crime and Computer Related Offences Bill 2014.

The draft Cybercrime Bill is an initiative of the Office of the Director of Public Prosecutions. It seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime. There are efforts to ensure the bill is compatible with international and comparative standards for the protection of freedom of expression and the right to privacy. The draft is wanting in areas such as

a. the provisions dealing with 'content-related' offences fall well below international standards on freedom of expression. In particular, the Bill provides for incredibly broad speech offences that could have a devastating effect for freedom of expression online in Kenya.
b. It also provides for unduly broad offences against computers and other computer-related offences.
c. The definition of computer system should closely follow the definition contained in the Cybercrime Convention and in particular, the definition of computer system should make explicit reference to 'automatic processing of data';

Cybercrime laws are rapidly being enacted and Kenya should not be left behind. As of November 2014, 117 countries (of which 82 developing and transition economies) had enacted such legislation, and another 26 countries had draft legislation underway[331]. However, more than 30 countries had no cybercrime legislation. Africa is the region for which the largest number of countries still needs to adopt cybercrime laws.

Cybercrime is not a domestic issue only as it presents complicated cross-border enforcement and jurisdictional problems. Efforts are needed in the area of law enforcement and in

[331] UNCTAD, report 2015.

strengthening the capacity of computer emergency response teams. International coordination and cooperation are critical in this context to create a safe business environment promoting faster responses and the sharing of information, thus giving countries the opportunity to react quickly and efficiently in combatting cybercrime.

Developing regions at different levels of cyber legislation maturity have made significant advances in preparing cyberlaws through various approaches. The growing sophistication of cyber legislation calls for increased coordination and collaboration among regulatory and statutory authorities at national and regional levels as well as close public–private dialogue for the legislation to be successfully enacted and enforced.

3.14 Offences

The increasing reliance on ICTs has been matched with the increase of cyber-related offences, posing a big challenge for law enforcement. The Internet allows crimes to be committed across boundaries and be computer generated unlike traditional offences that happen in real time.

There is some leniency on the sentences and punishments for computer related offences as compared to paper based related offences. For instance, fraud under the Penal Code attracts imprisonment for 3 years. However, electronic fraud under Section 84B of the KICA, attracts a maximum punishment is Kshs. 200,000 or maximum of 2 years in jail, or both.

The Communication Authority was in 2013, given powers pursuant to Article 157(12) of the Constitution, to undertake prosecution of any offence under cap 411A. [332] This is very important as the Authorities does not need to rely on the Attorney General's office to investigate and prosecute.

However, the Authority is yet to make full use of this law as it has not so far done much. Cyber-crimes are on the rise with most transactions and payments increasingly been made online and fraudsters have unsurprisingly adapted techniques to dip into the new financial flows.

[332] Section 40 of the Kenya information and communications (amendment) 2013 amendment of no. 2 of 1998 by Inserting a new sections 104 and 105.

One important cases on online fraud is that of *People v. Lipsitz,*[333] in which a New York court held that the defendant was subject to personal jurisdiction and liable for violating New York consumer protection laws, even though the defendant conducted its magazine subscription business globally over the Internet. The Respondent argued that the Attorney-General and the court had no jurisdiction over his Internet activity, a position which the Court rejected.

The accused was using various assumed business names and sold magazine subscriptions from a location in Staten Island, New York using several different names. There were affidavits and complaints, by local residents and individuals from other States complaining that the magazines never arrived; or arrived after an extremely extended delay. Requests for refunds were met with false promises to refund, investigate or not returning or hanging up calls. The respondent in defence argued the problem lay with the publisher and, even after that, often failed to remedy the deficiency.

The court stated in summary, that for Internet consumer fraud claims, the Internet medium is essentially irrelevant, for the focus is primarily upon the location of the messenger, his other business operations and whether what was purchased is delivered. In this case, the entire enterprise was firmly based in New York State.

The Attorney-General was said to have clear authority to seek to restrain illegal business practice by a local business in relation to both in-State and out-of-State residents, notwithstanding that these practices occur on the Internet. There were no geographical restrictions upon the consumer complaints hence a basis for an enforcement action. Accordingly, all complaints, including those from the residents of Israel and the Virgin Islands, were held to be properly before the court. The Attorney-General's mandate was held to be broad as he can commence enforcement actions even if no complaints were to exist.

The Kenyan law does not come out clear on how to deal with such a scenario and in particular were there are intestate and out state players

[333] 663 N.Y.S.2d [1997]468.

3.15 E –Taxation

The tax challenges are not unique to the application of the international tax regime to e-commerce. They are similar to other challenges of applying current legal doctrines to cyberspace.

The main challenge in applying the law is that the internet blurs the location, value and character of economic activity, making application of either residence-based or source-based taxing rights more difficult and double taxation even more likely. Double taxation in cross-border e-commerce increases its cost relative to domestic e-commerce and to conventional commerce, hindering its global development hence the importance of an economic union such as the EAC,[334] to address and overcome such challenges.

The issue of jurisdiction always arises as to which governmental entity shall have the authority to tax a transaction that spans several jurisdictions. The Kenyan law on ecommerce taxation needs to comprehensively address the e-commerce challenges of avoiding either double-taxation or non-taxation and to avoid disparate treatment of offline versus online transactions.

The law of taxing e-commerce income should emerge in an evolutionary, rather than revolutionary, manner hence mixed system of Integrative Adaptation Model for taxing international ecommerce income.[335]

The Integrative Adaptation Model adapts the existing international tax regime instead of changing it completely. The model is integrative in the sense that it borrows from adaptations made in other legal regimes as applied to the Internet to meet the special characteristics of e-commerce. [336]

[334] EAC framework for cyber laws phase ii 2011, p 17.
[335] Rifat Azam, e-commerce taxation and cyberspace law; Virginia journal of law and technology 2007, Vol. 12 No 5.
[336] Ibid.

3.16 The relevance of the concept of a "permanent establishment"

Section 8 (1) of the VAT Act provides on the doctrine of permanent establishment[337] which is both complicated and critically important from a tax policy perspective. Many states use the doctrine as the basis for their right to levy corporate income or sales taxes and therefore a key determinant for whether a country may tax an online business.

The doctrine is still problematic as e-commerce enterprises can sell their products or services worldwide with very limited physical presence in any particular consumer's country. They can operate without agents because they can directly, easily, and cheaply contact customers worldwide without a physical presence. The concept of fixed place is therefore meaningless in e-commerce business because it can be located anywhere and can conduct business everywhere.

The enforcement of the international tax regime on e-commerce thus faces many difficulties. The global character makes it difficult for any one country to monitor and tax e-commerce income. International cooperation is needed but such cooperation is not easy, given the conflicting interests of different countries.

In addition, the virtual nature of e-commerce makes it difficult to monitor and control e-commerce transactions even if countries are cooperating. The limited physical presence of the transaction and the limited physical assets of an e-commerce corporation outside the Internet make it difficult to reveal the business's transactions and income, which in turn makes it difficult to enforce the business's tax duties even if such duties were clearly determined. Furthermore, the anonymity of e-commerce makes it hard for tax authorities to discover the existence of ecommerce transactions, the parties involved and details of the transactions themselves.

Internationally, the OECD approach is still based on the territorial location of the server hence not giving any solution. There is no real economic allegiance between the place of the server and the production of the income. Reliance on the location of the server will open the door to tax manipulation.

[337] Section 8 (1).

3.17 Liability of Internet Service Providers

Kenya lacks clear Regulations on ISP and no specific policy guidelines describing how ISPs would be liable and under what circumstances. The question of liability of providers of hyperlinks, location tools and provision of Adwords need to be properly addressed domestically. Lack of proper legislation can lead to a range of unlawful acts such as libel, intrusion of privacy, intellectual property and trademark infringements, misleading advertisement, unfair competition, and breach of contract.

The potential problems are compounded by the lack of harmonised legislation on the obligation for the ISPs to retain traffic data and related to claims for information.

Intermediary liability has emerged as an important issue in recent years. This is because with governments and regulators generally frustrated with their lack of control over Internet activities, the potential for intermediaries, particularly ISPs, to carry out the regulatory function is viewed by some as a possible solution to Internet regulation. There are times when technological implementation falls to the ISP, if to anyone at all.

The law in Kenya at the moment has all of the risk in e-commerce transactions lying with the provider of the transaction and in most cases the credit cards providers. These entities protect themselves from online threats and fraud through insurance policies making the transaction expensive to the consumers who ultimately pays indirectly for this liability as transactional fees.

Such a shift of legal liability would certainly erode e-commerce confidence in consumers and in particular discourage new entrants to online shopping. It is technical and difficult to come across criminal prosecutions for online copyright infringement and computer hacking.
An ISP can be exempted from liability for stored information if he:

> *Does not have actual knowledge of unlawful activity or information; and upon obtaining such knowledge, it acts expeditiously to remove or to disable access to the information.*

The defence will however only apply to circumstances where recipients of the service were not acting under the authority or the control of the service provider.

A host is more exposed in some civil proceedings because a lower level of knowledge is required. The issue of information been apparent to the ISP as unlawful calls for constructive knowledge, rather than actual knowledge, which may be difficult to establish.

The *L'Oreal v eBay the CJEU* case gave guidance as to the circumstances in which a website operator would not be able to rely on the host defence. It provided a standard test by which one can measure whether or not a website operator could be said to have acquired an 'awareness' of an illegal activity or information in connection with its services.

The courts must ask whether "a diligent economic operator would have identified the illegality and acted expeditiously". Accordingly, while there is no obligation to monitor the content of a website, a service provider should not turn a blind eye to how its services will be used. When it gains awareness of any unlawful activity or information it must act expeditiously to remove or disable access to affected content.

The hosting exemption does not apply in civil proceedings that do not seek damages or another pecuniary remedy. So if a lawsuit seeks an injunction only, to stop doing something, the website operator cannot rely on the exemption.

UK Regulations do not include the prohibition on a monitoring obligation. However, in *Twentieth Century Fox Film Corp v British Telecommunications plc*[338] in response to an application for an injunction, BT argued that granting it would contravene the Directive. The injunction which was granted called for BT to prevent its subscribers from accessing "Newzbin2", which provided links to pirated films of Twentieth Century Fox. The order did not require BT to actively monitor content but block access to Newzbin2 via automated methods, which BT was already utilising to prevent access to child pornography. The Court said to the extent that this amounts to monitoring, it is specific rather than general.

[338] [2011] EWHC 1981 CH.

In the Court of Appeal case of *Tamiz –vs goggle*[339], M Tamiz complained to Google about comments on the 'London Muslim' blog it hosted, contending it was defamatory in nature and asked Google to remove that blog. The Court of Appeal declined jurisdiction and permission to serve on Google in California. Mr Tamiz' case failed on the facts given the small number of people who would have viewed this blog post in the relevant period.

It was argued that a publisher for defamation purposes is not co-extensive with a 'data controller. The cases raise the question whether it is right to hold Google to account for its role in making false, inaccurate or misleading personal information available to members of the public.

Internet Service Providers have the capability to track all malicious activity going in and out of their network and take necessary action. If ISPs were to co-operate in creating a clean cyber space in Kenya, there would be a significant change in the Cyberattack landscape[340]

Though notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by over censoring potentially illegal content.

Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences.

Despite the current laws and Regulations, there is still some uncertainty, particularly in relation to the extent to which ISPs should monitor content provided to them by their users. ISPs

[339] 2013 EWCA Civ 68.
[340] Ibid p 19.

are not monitoring information but wait until they receive a takedown notice. It is therefore necessary that a code of conduct be produced requiring ISPs to proactively remove radical extreme content posted online, which would necessitate that material is monitored.

However, requiring a ISPs to filter and takedown content that may be offensive has been put under scrutiny. In the case ***Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs***[341] the European Court when confronted with the issue whether an ISPs can be required to filter or pull down information though dealing with taking down copyright violation found that such a requirement would infringe on the right to do business as it would require very costly systems. Further, it would lead to violations of customers' right of protection of the personal data and right to receive information.

In the case of, ***Cartier International AG and Others v BskyB and Others***,[342] the issue of an ISPs being ordered to block or take down trademark infringing material was determined. In the above case, the United Kingdom held that for an order of take down to be given it must be determined whether the ISPs involved intermediaries, whether the operators of the targeted websites are in infringement and whether the operators use the ISPs' services to infringe.

Given the crucial role of ISPs in the ICT industry, particularly in ICT penetration, there is the need to eliminate the liability for defamation. It would be a big blow against the flow of knowledge and the expansion of the Internet for defendants in defamation litigation to interpret the activities of ISPs as "publication". Therefore, in developing the regulations with regard to take down orders the holdings in the above two cases may give crucial insight.

The law also lacks the simplicity and clarity to the common man which has added to the uncertainty.

[341] C -70/10
[342] [2015] 1 All ER 949

3.18 Unsolicited Commercial Communication

Marketing by email or text messaging, whether solicited or unsolicited, must clearly identify that it is a commercial communication, the person on whose behalf it is being sent; and if appropriate, that the communication is a promotional offer or game, and make conditions clear, unambiguous and easily accessible.

The law of Kenya is not clear on these aspects. The Kenya and Communication (Consumer Protection) Regulation, 2010 does not prohibit unsolicited commercial communications to a customer. Regulation 3 thereof which provides for the rights of a consumer can hardly be interpreted to mean that there is such a prohibition. There is no law to ensure that any unsolicited commercial communication sent by a service provider is clearly and unambiguously identifiable as such as soon as it is received".

The Court of Appeal in the case of *Greg Rosolowski Plaintiffs and Appellants, V. Guthy–Renker Llc*,[343] stated that the advent of electronic mail has brought with it a flood of commercial advertising, some of it misleading, false, deceptive, fraudulent and unwanted hence the need for anti-spam legislation.

The Court held that a header line in a commercial email advertisement does not misrepresent the identity of the sender merely because it does not identify the official name of the entity which sent the email, the domain name if traceable from an online database, provided the sender's identity is readily ascertainable from the body of the email, as was the case here.

[343] The Court of Appeal, second district, division 3, California b250951 decided: October 29, 2014.

Conclusion

Legislators face a challenge of assessing the relevance and efficacy of traditional contract law doctrine in light of technological innovation to come up with effective legislation that accommodates technology.

Competitive pressures will encourage businesses to seek to replace humans with automated contracting processes, but automated processes may embody technical norms that are not altogether consistent with law or public policy.

The turmoil in the realm of information privacy law and practice is an indication of the kind of controversy in the realm of contract law as new, more powerful electronic commerce technologies come into widespread use. Mechanisms to keep the development of technical standards in tune with both competitive market forces and the requirements of law and public policy will have to be found.

Kenya needs to do more in enacting and amending the current laws to counter the e commerce challenges.

Cap 411A is a good piece of legislation because the country is now able to prosecute cyber-crime offenders. However, it is not comprehensive since it does not, for example, address extra-territorial crime while in the cyber world jurisdiction is a key issue. It remains a challenge as the internet is a global portal and therefore it is not always easy to ascertain exactly where a crime has been committed and what national law has jurisdiction over the offence.

CHAPTER 4

CONCLUSION AND RECOMMENDATIONS

4.1 Introduction

Kenya has not only made progress in terms of electronic cash transfer, mobile money and laws but also in ICT infrastructure by connecting to the international broadband highway through four sub-marine fibre optic cables, connecting major towns through the National Optic Fibre Backbone Infrastructure (NOFBI) and Government Common Core Network (GCCN).[344]

Electronic contract, evidence and signatures are now admissible in evidence. However regardless of all these the desired levels in commerce growth is yet been realized,

This research set out several objectives one of which was to establish the legal and regulatory e-commerce framework in Kenya, which has been dealt with in chapter 2. It also purposed to examine the effectiveness of the said legal and regulatory framework, which was done in chapter 3.

The study proceeded on the hypotheses that the current Kenyan e-commerce laws are neither adequate nor effective to enhance the required growth in e commerce. Though the government policy is to encourage and support the faster growth of e commerce, the existing law is yet to effectively facilitate such good intentions and has not been able to cope with rapid technological changes and emerging challenges.

The hypotheses of the research is that there is need to develop more policies and legal framework that can effectively change the current trends and build confidence in the consumers and businesses, to not only use the internet as a source of information, but also use it to buy and pay for the goods and services on the internet.

[344] The Ministerial strategic plan 2013 -2017 p 3.

The Government has to adopt and harmonise foreign laws and come up with an all-inclusive policy which takes into account a combination of the legal, social, cultural, political, organisational, and economic factors which have led to the slow growth of e commerce in Kenya.

All the research questions have been answered. The questions on whether there any gaps and failures on the current laws that have led to the slow growth and which create barriers to the development of e-commerce has also been confirmed in the affirmative.

This chapter seeks to address the last research question on what is the best way forward and what recommendations can be made on the legal, regulatory and institutional framework to ensure faster growth of e commerce, change trends, build confidence in consumers and businesses and encourage them buy and pay for the good and services online.

4.2 Recommendations

The issues and challenges associated with e-Commerce in Kenya and the world in general is a reality. States, stakeholders, businesses and firms should devise appropriate strategies and laws that will help in overcoming these challenges. In the light of the above; the research proposes the following recommendations.

4.2.1. Effective Data Protection Law

Though Kenya has a general provision on data protection in the constitution and consumer protection law, the provisions are still lacking and there is always a challenge when it comes to enforcement. The data protection bill has not yet been passed into law.

In the global digital economy, personal data have become the fuel driving much commercial activity online making security of the said data a growing concern to Governments, enterprises and consumers alike. An adequate and supportive legal environment especially with regard to e-transaction laws, consumer protection, privacy, data protection, and cybercrime is essential to create trust online and to secure electronic interactions between enterprises, consumers

and public authorities. Kenya is one of the counties that has lacked behind when it comes to data protection law. By November 2014, 105 countries (of which 65 developing countries) had put in place legislation to secure the protection of data and privacy (UNCTAD, 2015). Another 34 developing countries had draft bills pending enactment.

Kenya should enact strict laws to ensure data protection and improve confidence to online users. The law will also give guidelines on maintaining logs and Registers for internet usage. It should ensure easy tracing by checking the logs derived from the ISPs and ensuring access to the user details are not denied by ISPs on jurisdictional grounds or allegations that its logs have expired or overwritten. The police should easily secure legal orders in each jurisdiction where a relevant carrier or ISP is located.

In Kenya, there are cyber cafes everywhere. There should be law to ensure and enforce compulsory maintenance of registers for recording personal details of all customers who use their internet services.

There is need to balance the right for consumers to withdraw personal information or that allowing individuals to have their data deleted and / or withdraw if they consent with the rights of other chain of players to whom the data may have been given. The drafters of the data law must ensure the bill is compatible with international and comparative standards for the protection of freedom of expression and the right to privacy.

Commercial entities and persons in countries with data protection legislation will always feel exposed and avoid transacting electronically with Kenyans due to lack of data protection. Existence of law in Kenya, even if not harmonised laws of such countries, would cause a feeling of safety as the principles of conflict of laws would be applied in resolution of dispute emanating from e commerce transaction.

4.2.2 Courts should prefer a reasonable interpretation of Section 106 of the Evidence Act

Section 106A and 106B of the Evidence Act deals with proving the contents of an electronic record and the procedure through which such records can become admissible in evidence. Courts have over the years grappled with different interpretations and applications of this section.

When the Section of the law was initially enacted, it was intended to govern criminal prosecutions. However, with time, civil and commercial matters are now relying on the sale section especially where electronic evidence is concerned. It is against the Rules of Natural Justice to shut down a party unheard. Article 159 of the Kenyan 2010 Constitution requires courts to dispense justice without undue regard to technicalities. Article 50 gives the right to a fair hearing. Applying Section 106 to shut out parties on the grounds that the devises used were not authentic or the gadgets used have not been described or certified will be tantamount to obstructing substantive justice.

The requirement for production of a certificate from the service provider to show that the computers used in the production of the evidence were operating properly is also vague and should be done away with.

The Section law should be amended or interpreted in general terms to remove any restriction to computer generated evidence especially with regard to commercial matters. The civil procedure Rules with regard to documentary evidence should apply. All evidence should be laid before the trial judge to assess its evidential value and decide the case on merits and whether to call any further evidence or the person to explain how he processed the evidence like in a paper based trial if the doctrine of functional equivalence is to be achieved.

4.2.3 Recognise in the domestic e-transaction laws the aspects of consumer protection, data protection, cybercrime laws, other agencies and regional mechanisms.

The consumer protection Act is a domestic legislation which does not address cross border issues. There is a need to set up consumer protection agencies in several developing countries and to strengthen existing ones. Kenya and other developing counties should join various regional mechanisms for online consumer complaints and enforcement to facilitate cross-border e-commerce. This would require an agreement between consumer protection agencies in a given region, complemented by appropriate investigation and referral tools. Linking up agencies through networks such as ICPEN can help national agencies to keep abreast of new legal regional or international developments, as well as to share experiences and bring out solutions for e-commerce users.

Such coordinated regional mechanisms for online consumer complaints and enforcement of consumer protection laws do not only resolve the dilemma of cross border disputed but also is an avenue for alternative dispute resolution and redress schemes. They are affordable and easy to use.

These would also apply to other laws such as e-transaction laws, consumer protection, data protection, and cybercrime laws. The Computer Emergency Response team need to be strengthened financially, technically and by infrastructure and liaise with other international bodies to prevent and combat cybercrimes, cyber warfare and cyber terrorism. Towards this end Kenya is to sign the Northern Corridor Cyber Incident Response Team (NC-CIRT). However, more needs to be done to bring all other regional blocks and trade agreements on board if the benefits are to be realised.

African and developing countries should ratify the relevant e commerce law conventions and create a permanent point of contact in an effort to foster cooperation of law enforcement agencies around the world such as has been done by Interpol who have created a contact point network, currently featuring the National Central Reference Point (NCRP).

4.2.4 Pass into law the draft, Cyber-Crime and Computer Related Offences Bill 2014.

The Kenya Information and Communications (Amendment) Act 2014 expanded the mandate of the Authority with respect to electronic transactions to include cyber security. It promoted and facilitated efficient management of critical internet resources and developing a framework for facilitating the investigation and prosecution of cybercrime. KICA was still not adequate hence the efforts to draft the draft, Cyber-Crime and Computer Related Offences Bill 2014 which is yet to be passed into law. It seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime. There are efforts to ensure the bill is compatible with international and comparative standards for the protection of freedom of expression and the right to privacy a s well as ensure

a) the provisions dealing with 'content-related' offences fall well below international standards on freedom of expression.
b) Avoid unduly broad offences against computers and other computer-related offences.
c) Improve it to closely reconcile with the Cybercrime Convention.

4.2.5 Create certainty on electronic contracts

Section 83 J of Kenya Information Communication Act confirms that e commerce laws will not apply in situation where any other law expressly provides for a different method for the formation of a valid contract. This provision is too general and takes away the power of the state to protect the interest of its consumers and traders involved in e transactions. The doctrine of freedom to contract should not be a ground to oppress consumers.

The law should thus be allowed to intervene depending on the circumstance of each particular case especially if the terms of a shrink wrap contract are oppressive.

4.2.6 Enhanced Sentences and resources for training of judicial officers

Most e transaction related offences are punishable for three years. Whereas the imprisonment and fines ought to be enhanced, there should be a provision that the convict must surrender the benefit obtained as a result of committing the offence. This will act as very good deterrent as there will be no motivation to commit such offences since no benefit will be accrued.

There is need to make work of investigators easier by balancing the constitutional right of privacy and the issuance of warrants of arrest. The investigator should also be accorded a reasonable measure of immunity from claims that may arise against them during investigation.

Further, forensic laboratories need to be established through legislation. Further, for extra-territorial cybercrimes, the Mutual Legal Assistance Act[345] can be applied.

The law once passed has to be effectively enforced. More investment on research and coordinated training with other countries to ensure transnational cases are pursued quickly and seamlessly. This will equip them with legal and required technical knowledge to enforce cyber laws. Training should extend to prosecutors, lawyers, magistrates, judges and investigators. Specialized workshops can address emerging issues even as we introduce a curriculum to the universities, the Kenya school of law and the judicial training school for those who are already judges and magistrates.

Reporting and access points and cybercrime cells in police stations is needed to facilitate effective investigations of cybercrime cases. Several recognized forensic laboratories are necessary as they will have the mandate to prepare forensic reports in cybercrime cases to enhance efficiency in handling the increasing volume of cybercrime investigation cases.

Officers should be trained on live data forensics; a subject area which ensures data can be seized from a suspect's computer while it is still running and taken it to a laboratory for analysis. This will help protect and preserve sensitive evidence that can be easily destroyed, deleted, or

[345] Act No 36 of 2011

modified. For instance, digital photographs can be altered in ways that may be difficult to detect. As a result, law enforcement officials must be cognizant of how to gather, preserve, and authenticate electronic evidence in an authentic manner that will be completely admissible in a court of law.

4.2.7 Improve the Law Governing ISPS

Kenyan law and guidelines on liability of ISPs is too general. It does not practically address the challenges of liability for defamation, copyright infringing, defamatory, vulgar, and harmful content streamed through their infrastructure where they have not assumed any obligation to monitor and intercept harmful internet traffic.

Given the crucial role of ISPs in the ICT industry, particularly its penetration, there is the need to eliminate the liability for defamation. It would be a big blow against the flow of knowledge and the expansion of the Internet for defendants in defamation litigation to interpret the activities of ISPs as "publication". In many countries, ISPs are given statutory exemption from liability for harmful content streamed through their infrastructure.

The law governing ISP should be drafted and worded in a way to ensure the takedown notice and procedure is not abused by rival actors whether public or private. This can be achieved through

(i) Ensuring the take down notice is confirmed to be genuine by an independent body so that competitors in the sector do not misuse the aspect of notice.

(ii) No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;

(iii) Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online; and

(iv) ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown

Kenya should also incorporate into its law a compulsory policy were ISPs, should provide their following minimum information, which must be easily, directly and permanently accessible:

a. the name of the ISP and its geographic address.

b. details of the ISP and its email address. The CJEU in *Bundesverband v Deutsche Internet Versicherung (2008)*[346] confirmed that a company may need to provide other methods of communication beyond its postal and email address. A 'contact us' form without also providing an email address is not sufficient;

c. details of its register, including registration number.

d. if a company, its registration number.

e. the particulars of the relevant supervisory authority if subject to an authorisation scheme;

f. details of any professional body or institution with which the provider is registered, its professional title and Member State where title has been granted and A VAT number, Prices and whether prices are inclusive of tax and delivery costs.

4.2.8 Improve the Online Payment Systems and mobile money

An effective electronic payment system is significant to curb challenges related to fraud, security, consumer protection and privacy. The cross-border aspect of payment services raises issues about the standards and roles applicable to domestic payment systems and their interoperability with foreign systems. It determines the level of consumer protection available for using foreign payment systems. The current laws are either inadequate on this issues or do not address them at all.

Support policies and procedures designed to promote transparency in the regulation of payments systems, including standards, application process, judicial, arbitral, and/or administrative review are required.

[346] AG ECJ Case 298/07 of 2008.

The National Payment Systems Act does not fully address payment regimes nor does it foreclose on the projected developments in digital cash. Stored value systems such as credit cards are becoming interoperable and there is a perceptible shift towards cardless value transfer involving bit currency. This vacuum can be a fertile ground for money laundering and other related crimes such as facilitation of cyber-terrorism.

The banking sector must create a secure payment platform to enable people pay for goods/products online. A proper enforceable legal framework is necessary to give the consumers and businesses the confidence to transact in e –commerce. An effective data protection law must be enacted if consumers are to freely give their credit card details online.

On mobile money, Mobile phones are not only being used for communication, but also for data applications and personal banking services such as m-commerce and m-banking. One of the major barriers to poverty reduction is access to formal financial systems for the poor.

Mobile phone finance systems can be used to receive and send money, save, borrow, repay debt among others. It requires effective laws to be put in place as this will offer an effective way of conducting payments and providing access to finance, particularly in areas where access to physical bank branches, bank agents or even ATM machines is minimal.

Though there is very high growth of agency banking in Kenya[347] which has substantially increased accessibility of money to Kenyans in rural areas, the same cannot act as a substitute to improving mobile money transfer. Though the CBK promulgated the Money Remittance Regulations, 2013, these regulations cannot in any way be said to regulate Mobile phone money transactions. The Regulations only applies to money remittance business by body Corporate.[348] Whereas the definition of the money remittance business may arguendo incorporate mobile phone transaction,[349] the same becomes restricted by the requirement that only body corporates can

[347] Business Daily, website December, 2015.

[348] Regulation 4, The Money Remittance Regulations, 2013

[349] Regulation 2(a) where the Money Remittance Business is defined as means a service for the transmission of money or any representation of monetary value without any payment accounts being created in the name of the payer or the payee, where funds are received from a payer for the sole purpose of transferring a corresponding amount to a payee or to another payment service operator acting on behalf of the payee'

engage in such business. Further, the licensing procedures of money remittance operators is not applicable to those persons who desires to operate a mobile money transaction business. The mobile phone money transaction cannot be said to fall with the provisions of National Payment Systems Act [350] as a payment system.

There is confusion as the agents used by mobile money transfer services are not regulated by any financial institutions regulators but by the telecommunication service providers. It is not clear who bears the burden of liability in case of a mistake. It can be argued that the lack of regulatory framework for Mobile money transfer is because there are two regulatory bodies involved, that is the Financial Regulator and the Telecommunication Regulator. This can be resolved by establishing a Financial Services Authority.[351]

To improve on Mpesa, Kenya needs to

a) Consider Europe's approach, in separating the regulation of payment services from the Regulation of credit institutions.
b) Establish flexible supervision models and standardize laws to give an enabling environment for new innovations.
c) Ensure co-operation of the relevant agencies involved in policy, regulation and supervision to ensure consistency.
d) Enact appropriate laws to increases confidence, level playing ground, collaboration stability and integrity of the financial system.

A strict law to control mobile phone use is necessary as mobile phones can be altered to transmit false identifying information. The cost of mobile phones and mobile telephony service has dropped leading to more "disposable phones," Strict and effective enforcement of the regulation and registration of Sim Card can increase the ability of law enforcement agencies to gather evidence linking a perpetrator to the communication. Severe and deterrent penalties need to be imposed.

[350] Section 2 of the Act No 39 of 2011
[351] Barnabas Andiva, '*Mobile Financial Services & Regulations in Kenya*. 2015

4.2.9 Strict regulation of electronic signatures

Secure, reliable and interoperable identification and authentication measures are necessary for the further development of cross-border e-commerce. Kenyan can make its use more effective if regulations are put in place;

i. for merchants, to have a way to verify the identity of the customer.

ii. to increase trust in electronic commerce.

iii. e-identification schemes based on real IDs verified by the government or its agency to help reduce cybercrime and fraud.

The use and legal validity of the digital signature remain unregulated in Kenya. This mode of banking necessitates, and demands, the replacement of personal relationship management with man-to-machine interaction hence the need for clarity and regulation.

The use of digital signatures within the electronic banking environment assumes the character of message authentication which allows each party to verify that data received electronically is genuine and has not been altered. Authentication is in closed environment within a bank and regulated by the bank. The law and regulations in Kenya should address the issue whether the Personal Identification Number is an electronic signature within the remit of the law.

The use, validity and the evidentiary value of electronic signatures in Kenya and its legal validity, however, remains untested. This is indeed a legal vacuum, and particularly within the banking environment, because the customer's signature is his mandate to the bank. Further, cheques and hand written signatures go hand in hand and are regulated by legislative enactments.

4.2.10 Harmonisation

The world needs some level of harmonisation of the law governing cross border e commerce to avoid the situation in the European Union, where enterprises have to operate with 28 different sets

of national rules for conducing cross-border trade. The players are faced with a situation to first identify the provisions of the applicable laws of particular countries, and assume the costs associated with translation, legal advice and adaptation of contracts. This adds costs, complexity and legal uncertainty.

4.2.11 Review of tax laws and Attribution

Tax administration rules should be re-examined to ensure that online businesses and the revenue authorities have adequate and technically secure means to collect, remit and audit the taxes in an online environment. Monitoring transactions in an e-commerce environment coupled with the absence or unavailability of auditable records can render tax administration considerably more complex. These require revenue authorities to redesign enforcement strategies by ensuring proper policies, legislation, effective regulations and internal administration processes and policies which are more efficient and grow with the technology as it grows.

There should be cooperation of stakeholders to regulate the industry and more particularly the ISPs who can be used to bill their clients on behalf of the KRA through a withholding tax. Similarly, banking institutions could withhold value added tax, if need be, on financial transfers for electronic transactions carried out online.

States should reform national tax rules and adopt international best practice, such as that of the OECD, concerning the concept of 'permanent establishment' to clearly indicate when an online business meets the applicable criteria.

Government should ensure companies develop best practices and internal mechanisms to check anonymity on the internet which remains a big challenge. There is need for more legal rules in addition to Section 83L of Cap 411A, so as to achieve effective enforcement of the law through and development of both managerial and technical measures.

4.2.12 Need to amend Section 267 of the Penal Code Cap 63 laws of Kenya

Section 267 of the Kenyan Penal Code defines what can be stolen as "Every inanimate thing, which is the property of any person, and which is movable". It is my proposal that this section should be amended and expanded to include information and to create a new offence of information theft.

4.2.13 Establishment of an Independent, Effective, Fair and Transparent Oversight Body

There should be separate regulatory frameworks for the various communication sectors by different government agencies to be statutorily recognized, independent and fully funded as well as a specialized independent Authority to deal with e commerce and related issues.

Government regulations have to be moderate and balanced to allow the free development of Internet services hence the need for a specialised independent body that should be empowered with the resources and capacity to monitor the market trends.

The national regulator is critical in providing regulatory certainty, ensuring non-discriminatory treatment of market participants both domestic and foreign, and in preventing anti-competitive behavior.

CONCLUSION

This research set out to analyse the current national and international e-commerce laws and policies that apply in Kenya; Critically examine the legal and regulatory framework governing e commerce in Kenya, its effectiveness and challenges and identify and come up with recommendations on the legal, regulatory framework to ensure faster growth of e commerce and build confidence in the consumers. These three objectives were precisely set out in chapter one.

The analysis of the legal framework on e commerce has shown that e-commerce is of international importance considering that the United Nations has developed models laws upon

which the various state parties can align their municipal laws with. Further, it has been established that the current law in Kenya as it regards electronic evidence is very convoluted and strict making it very hard for such evidence to be admitted during litigation.

It has also been shown that the legislative development has not kept pace with technological development which has led to slow growth of legislations dealing with e commerce.

The research has further shown how various e-commerce disputes have been addressed by courts in various jurisdictions. The issues can adequately be addressed through good e-commerce legislation. It has also been shown that effective enforcement of Cyber laws requires a multipronged approach. No one strategy by itself is self sufficient or mutually exclusive to create effective enforcement results. Kenya has to devise a well integrated action plan.

The need to create awareness on e commerce amongst general public and impart continuous training to the law enforcement personnel and forensic experts has also been shown. General educational system has to emphasis orientation to internet technology in order to build trust and confidence. This will also raise awareness, acceptance and usage of e-commerce in Kenya by its citizens.

The issue of consumer protection especially in e transactions has also been highlighted. There is need for Kenya and other developing countries should recognise in law and join various regional mechanisms for online consumer complaints and enforcement to facilitate cross-border e-commerce

The problems having been identified, various recommendations have been proposed as outlined above.

REFERENCES

Abby W, Kenya's cyber law being developed, The Standard Newspaper (online edition), published on Sun, Aug 5th, 2007 accessed 05/04/2013.

Almeida G. A, Avila A, Boncanoska V, (March 2007), Promoting e-Commerce in Developing Countries Internet Governance and Policy - Discussion Papers Diplo.

Amelia B.H, *Searching for security in the law of electronic commerce.* Nova Law Review 23.2 (1999):

Austin, TX (ZPRYME News), 04/09/08 http://zpryme.com/news-room/kenya, the regional effort of harmonizing laws on cybercrime zprymehtml.html accessed on 15/11/12.

Bakar M, A Cyber Law Policies and Challenges, Butterworth's Asia, Kuala Lumpur, (1999)

Barney J, Firm resources and sustained competitive advantage, Journal of management 1991 vol 17 no1, Texas, A&M University

Bell R. S.K. and Ray .N ,*European Union Electronic Communication law* (Oxford University press 2004)

Brady M, and Trus S, challenges in electronic commerce
http://www.itl.nist.gov/div897/staff/brady/ec/nist-ec.html accessed on 5th November 2012.

Business news 26th October 2009,http://www.standardmedia.co.ke page No 1 accessed 27/11/12.

Butt F.S, Aijaz H.T, Karlsson T.J, Barriers in the Development of Electronic Commerce: A Study of Pakistani Environment Master thesis, Business Administration Authors: June 2009.

CCK website, Quarterly Sector Statistics Report Second Quarter of the financial year 2012/13 (Oct-Dec 2012) p 8.

David Souter. D and Makau M. K, Internet Governance in Kenya – An Assessment for the Internet Society, September 2012.

Dickie J ,*Producers and Consumers in EU E-Commerce Law* (Oxford: Hart 2005) .

Distance Selling Directives

Dr. Kenneth W, Rebecca M N. and Eunice A (2012), factors affecting adoption of Electronic Commerce by Small Medium Enterprises in Kenya.

Draft EAC Legal Framework for Cyber laws, November 2008.

Edwards .L. and Waelde C, *Law and the internet* (2009), Hart publishing, Oxford and Portland oxford.

E-shopping is Kenya ready for-business MNTE News Africa at http://www.itnewsafrica.com/2007/06/ accessed on 15/11/12.

Framework for Cyber Laws Phase II, October 2011.

Gichuki E.N (2007),challenges on electronic commerce on tax; Towards a sustainable tax policy on e-commerce for sustainable development in Kenya.

Goel R, *E-commerce* (New age international publishers limited 2007, reprint 2009).

Grace J.K (2005), taxation of e-commerce, the challenges posed by the concept of permanent establishments.

Grundmann. S, The Structure of European Contract Law, 2001
Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001).

Http://www.kachwanya.com/e-commerce-industry-in-kenya-the-missing-link/accessed 15/11/12.

Http://www.standardmedia.co.ke/articleID=2000069710&story_title=Kenya-ICT-Board-to-release-funds-for-digital-villages.

Http://www.bizcommunity.com/Article/111/16/39933.html The Information and Communication Permanent Secretary as at 14th September 2009 Dr. Bitange Ndemo accessed on 27/11/12.

Humphrey J, Mansell R, Paré D, Schmitz .H (March 2003), the reality with e-commerce with developing counties.

Jeffrey R. B. and Judith Y. Gliniecki J.Y, *International Electronic Commerce and Administrative Law: The need for harmonized national reforms.* Harv. JL & Tech. 6 (1992):

Information Society, *Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD

Karake. Z, Qasim. L, Cyber law and cyber security yin developing and emerging economies, Edward Elgan publishing 2010.

Kerros T. R, E-Commerce in Saudi Arabia: Driving the evolution, adaption and growth of e-commerce in the retail industry Orloff 2012

Kinyanjui M. N and McCormick D, E-commerce in the garment industry in Kenya usage, obstacles and Policies, Institute for Development Studies University of Nairobi, 2002

Laudon K.C and Traver C.G, E- *commerce 2011*(7th edition Pearson education ltd).

Leung1 L. C., Chu1 S, Hui Y. V, and Cheung1. W. The Evolution of E-commerce Websites a Conceptual Framework and Analysis Center of Cyber Logistics, Business Administration, Chinese U. of Hong Kong.

Magutu P.O , Lelei J.K, Nanjira A.O African Journal of Business & Management (AJBUMA) AIBUMA Publishing http://www.aibuma.org/journal/index.htm Vol. 1 (2010), accessed on 15/1/12.

Molla B R, , Heeks, A.R. and Hinson, R. (2011). Advancing E-commerce Beyond Readiness in a Developing Economy: Experiences of Ghanaian Firms, Journal of Electronic Commerce in Organizations.

Mullenex D and Mouren A.S, M-Payment in Africa: Great Means to Great Ends, December 2012 Regulatory Communications.

Mumo M, "Trade via Internet yet to pick up despite cables", Daily Nation (online edition), Posted Tuesday, January 15 2013 at 02:00, accessed 9/4/2013.

Murungi M M, cyber law in Kenya Kluwer law and business.

Muthoki Mumo, "Trade via Internet yet to pick up despite cables", Daily Nation (online edition), Posted Tuesday, January 15 2013 at 02:00, accessed 9/4/2013.

Nasi M.A (2004), Legal issues involved in e- commerce.

Netcom Information Systems Ltd, Internet Market Analysis Study Final Report: Communications Commission of Kenya, May 2007

OECD 2009, OECD Conference on Empowering E-consumers Strengthening Consumer Protection in the internet Economy Background Report Washington D.C., 8-10 December 2009.

OECD Report, Measuring the information economy 2002, Annex 4, the OECD definitions Guidelines for the interpretation of the definitions of electronic commerce.

OECD 1997 Report on information, computing and communication policy, measuring electronic commerce.

OECD, 1998. E-commerce: impacts and policy challenges by Jonathan Coppel.

Prasad Bingi P, Mir. A& Khamalah J (2000): The Challenges Facing Global E-Commerce, Information Systems Management, 17:4, 1-9 < http;//dx.doi.org/10.1201/1078.

Professor Michael Geist, Current issues of e-commerce law, University of Ottawa, Faculty of law.

Rayport J.F and Jaworski B.J, *Introduction to e-commerce* (2nd edition MC Graw Hill 2003).

Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce, Guidelines

Reed .C, Internet Law: Text and Materials, 2nd edition, Cambridge University Press, 2004

Robin .M (2003) Electronic commerce: conceptual pitfalls and practical realities. Prometheus, 21 (4), available at: http://eprints.lse.ac.uk/3534/ LSE Research Online: May 2008 accessed on 15/11/2012**.**

Ronald H.C (1937), 'The Nature of the Firm', Economica, 4, New Series, November .

Smedinghoff T. J. The Legal Challenges of Implementing Electronic Transactions 2008.

Tassabehlyl R, applying e-commerce in business 2005, Sage Publishers ltd.

The Communications Commission of Kenya Strategic Plan for the period 2008 – 2013

Posner R.A, Theories of Economic Regulation, Nber working paper series, May 1974, UN Convention on the Use of Electronic Communications in International Contracts.

Vanhoose D.D, E-Commerce Economics 2nd edition, Taylor and Francis, 2011.

Vanhoose D. D, E-commerce economics, Routledge 2011.

Vision 2030, Republic of Kenya, 2007 Government Press.

Wang Y and Shi X towards a Theoretical Framework of E-Business Value Creation: The Dynamic Capabilities Perspective.

Watson R T, Berthon P, Leyland F. Pitt, and. Zinkhan G. M, Electronic commerce; the strategic perspective (2008).

Zittrain J.L, Internet Law Series: Jurisdiction (Foundation Press, New York, 2005).