UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

Harmonizing Cyberlaws and Regulations:

The experience of the East African Community

UNITED NATIONS

United Nations UNCTAD/DTL/STICT/2012/4/Corr.1

United Nations Conference on Trade and Development

16 August 2013

English only

Harmonizing Cyberlaws and Regulations: The experience of the East African Community

Corrigendum

1. Page 13, paragraphs 6 and 7

For Penal Code Act n°1/95 *read* Penal Code Act n°1/05

2. Page 13, paragraphs 6 and 7

For Press Act n°025/01 *read* Press Act n°1/025

3. Page 13, paragraphs 6 and 7

For Protection of Right of Author and its related Act n°1/06 *read* Protection of Right of Author and its related Act n°1/021

4. Page 30, first paragraph

For Chapter 6 *read* Chapter 9

5. Page 48, note 101

For CAP 15 *read* CAP 215

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

Harmonizing Cyberlaws and Regulations:

The experience of the East African Community

UNITED NATIONS
New York and Geneva, 2012

NOTE

Within the UNCTAD Division on Technology and Logistics, the ICT Analysis Section carries out policy-oriented analytical work on the development implications of information and communication technologies (ICTs). It is responsible for the preparation of the Information Economy Report as well as thematic studies on ICT for Development. The ICT Analysis Section promotes international dialogue on issues related to ICTs for development, and contributes to building developing countries' capacities to measure the information economy and to design and implement relevant policies and legal frameworks.

The following symbols have been used in the tables:

Two dots (..) indicate that data are not available or are not separately reported. Rows in tables have been omitted in those cases where no data are available for any of the elements in the row;

A dash (–) indicates that the item is equal to zero or its value is negligible;

A blank in a table indicates that the item is not applicable, unless otherwise indicated;

A slash (/) between dates representing years, e.g. 1994/95, indicates a financial year;

Use of an en dash (–) between dates representing years, e.g. 1994–1995, signifies the full period involved, including the beginning and end years;

Reference to "dollars" ($) means United States dollars, unless otherwise indicated;

Annual rates of growth or change, unless otherwise stated, refer to annual compound rates;

Details and percentages in tables do not necessarily add up to the totals because of rounding.

UNCTAD/DTL/STICT/2012/4

PREFACE

The development of an enabling framework for e-commerce has the potential to generate significant economic development gains for countries by promoting investor confidence, tapping into business opportunities and responding to the increasing reliance on electronic applications in all sectors (government, commerce, health, education, banking, insurance, etc.). Regional and national commitment towards providing a modern legal framework to interface between the physical and digital space is very important in this context.

This study was conducted as part of the work that the United Nations Conference on Trade and Development (UNCTAD) and the East African Community (EAC) Task Force on Cyberlaws have been carrying out since 2007 to prepare legal frameworks for e-commerce.

In 2009, the EAC became the first region in Africa to adopt a modern and effective regional harmonized framework for cyberlaws. It had been developed to meet the need expressed by Council of Ministers of the East African Community in 2006 to support the regional integration process with regard to e-Government and e-commerce. Two sets of recommendations for cyberlaws were subsequently prepared by the EAC Task Force on Cyberlaws in close cooperation with the EAC secretariat with the support of UNCTAD. Phase I of the Framework – covering electronic transactions, electronic signatures and authentication, cybercrime as well as data protection and privacy – was adopted in 2010 by the EAC Council of Ministers on Transport, Communications and Meteorology. It is currently being implemented at the national level. Phase II of the Framework – covering intellectual property rights, competition, e-taxation and information security – is to be examined by the EAC in 2012.

The present study assesses the status of cyber-legislation in the EAC. Similar analyses have previously been prepared by UNCTAD for Latin America and Central America.[1] The analysis contained in this report provides valuable information also for developing countries outside of the EAC region by documenting progress to date describing the law reform process and identifying best legislative standards to ensure cyberlaw harmonization.

The first part discusses the need for regional harmonization and the challenges faced with regard to the implementation of cyberlaws in the EAC region. The second gives a detailed account of the status of cyberlaws in each country. It is hoped that the work of the EAC Task Force on Cyberlaws and this study offer some useful lessons and tools for other countries and regions engaging in cyberlaw reforms.

The study's principal consultant was Professor Ian Walden. National inputs were provided by the following members of the EAC Task Force: Pierre Ndamama (Burundi), Mercy Wanjau (Kenya), Allan Kabutura (Rwanda), Adam Mambi (The United Republic of Tanzania), Denis Kibirige (Uganda), and Matthew Nduma (EAC Secretariat). The study was prepared by a team from UNCTAD comprising Torbjörn Fredriksson and Cécile Barayre, under the overall guidance of Anne Miroux. Statistical support was provided at various stages by Smita Barbattini and Agnes Collardeau-Angleys. The document was edited by Nancy Biersteker. Destop publishing and the cover were done by Nadège Hadjemian.

Valuable comments and inputs were received from Robert Achieng (EAC Secretariat) and Luca Castellani (UNCITRAL). Special thanks are also given to the members of EAC Force on Cyberlaws who have been actively involved in the preparation of Africa's first regional harmonized framework for cyberlaws.

Financial support from the Government of Finland is gratefully acknowledged.

ABBREVIATIONS

CERT	Computer Emergency Response Team
CIRT	Computer Incidence Response Team
COMESA	Common Market for Eastern and Southern African States
EABC	East African Business Council
EAC	East African Community
EALA	East African Legislative Assembly
EASSy	Eastern Africa Submarine Cable System
ICT	Information and Communication Technologies
IPR	Intellectual Property Rights
ITU	International Telecommunication Union
RURA	Rwanda Utilities and Regulatory Agency
SADC	Southern African Development Community
TCRA	Tanzania Communications Regulatory Authority
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNECA	United Nations Economic Commission for Africa
VAT	Value Added Tax
WIPO	World Intellectual Property Organization

CONTENTS

PART I
REFORMING CYBERLAWS IN THE EAST AFRICAN COMMUNITY

PART I.
REFORMING CYBERLAWS IN THE EAST AFRICAN COMMUNITY

A. The East African Community

The East African Community (EAC)[2] is a regional economic community comprising five states: the Republic of Burundi, the Republic of Kenya, the Republic of Rwanda, the United Republic of Tanzania and the Republic of Uganda (the 'Partner States').

The principal source of EAC law is the Treaty for the Establishment of the East African Community (the "Treaty").[3] According to the Treaty, the main objective of the EAC is to widen and deepen the integration process. Article 5(2) of the Treaty establishes the objectives to be the formation and subsequent evolution of a Customs Union, a Common Market, a Monetary Union and finally a Political Federation, under the overarching aim of equitable development and economic growth amongst the Member countries.

The entry point of the integration process is the Customs Union. It has been progressively implemented since 2004; in January 2010 the EAC became a full-fledged Customs Union. One critical aspect of the implementation has been the establishment of an interconnected ICT solution for a regional customs system.[4]

The EAC Common Market Protocol[5] entered into force in July 2010, providing for the following freedoms and rights to be progressively implemented: free movement of goods, persons, labour, services and capital; as well as a right of establishment and residency. The Community has since then commenced negotiations for the establishment of the East African Monetary Union, which is scheduled to take effect in 2012. The ultimate objective, to establish an East African Political Federation, is targeted for 2016.[6]

The structure of the EAC promotes decision-making through consensus. Each State has the authority to veto details of regulations formed under the Treaty. Once consensus is reached and regulations passed, they are binding on all Partner States. Each State may still, however, achieve regulatory goals through its own individual domestic policies.

The Treaty obliges the Partner States to plan and direct their policies and resources with a view to creating conditions favourable to regional economic development[7] and through their appropriate national institutions to take necessary steps to harmonize all their national laws appertaining to the Community.[8] Harmonization is one of the key concepts espoused by EAC. With particular respect to the integration of laws, Article 126 of the Treaty and Article 47 of the Common Market Protocol both call for the harmonization of national legal frameworks.[9]

It should be emphasized that two different law systems are applied among the participating countries: Kenya, The United Republic of Tanzania, and Uganda follow a common law system, while Burundi and Rwanda both subscribe to a predominantly civil law system.[10] This has led to somewhat divergent legislative practices and procedures between the groups of countries, and may have contributed to slowing down the process of harmonization efforts in the region.

Article 5(2): In pursuance of the provisions of paragraph 1 of this Article, the Partner States undertake to establish among themselves and in accordance with the provisions of this Treaty, a Customs Union, a Common Market, subsequently a Monetary Union and ultimately a Political Federation in order to strengthen and regulate the industrial, commercial, infrastructural, cultural, social, political and other relations of the Partner States to the end that there shall be accelerated, harmonious and balanced development and sustained expansion of economic activities, the benefit of which shall be equitably shared.

Article 47:

Approximation and Harmonization of Policies, Laws and Systems

1. The Partner States undertake to approximate their national laws and to harmonise their policies and systems, for purposes of implementing this Protocol.
2. The Council shall issue directives for purposes of implementing this Article.

Article 126:

Scope of Co-operation

1. In order to promote the achievement of the objectives of the Community as set out in Article 5 of this Treaty, the Partner States shall take steps to harmonise their legal training and certification; and shall encourage the standardisation of the judgements of courts within the Community.
2. For purposes of paragraph 1 of this Article, the Partner States shall through their appropriate national institutions take all necessary steps to:
   (a) establish a common syllabus for the training of lawyers and a common standard to be attained in examinations in order to qualify and to be licensed to practice as an advocate in their respective superior courts;
   (b) harmonise all their national laws appertaining to the Community; and
   (c) revive the publication of the East African Law Reports or publish similar law reports and such law journals as will promote the exchange of legal and judicial knowledge and enhance the approximation and harmonisation of legal learning and the standardisation of judgements of courts within the Community.
3. For purposes of paragraph 1 of this Article, the Partner States may take such other additional steps as the Council may determine.

B. The EAC e-government strategy

Against the background of progressive regional harmonization, the EAC Council of Ministers in 2006 adopted the EAC Regional e-Government Programme. It was an important step towards deepening East African regional integration through the provision of government information and services. The Regional Strategy for e-Government, supported by the United Nations Economic Commission for Africa (UNECA), aimed at improving and enhancing public service delivery through the use of Information and Communication Technologies (ICTs) in public administrations, combined with organizational change and the development of new skills. Improved public service delivery would in turn support regional integration for economic development of the region.

The creation of an enabling legal and regulatory environment was identified as a critical factor for the effective implementation of e-government and e-commerce strategies at national and regional levels. To achieve operational efficiency of such strategies, strong back up support is needed in terms of legislation related to data security, network security, cybercrime, information systems and electronic transactions. Cyberlaws and e-Justice were in turn identified by the EAC as key cross-cutting issues that need to be in place for the successful implementation of e-Government applications and the development of e-commerce in the region. The strategy was incorporated in the overall EAC Development Strategy for the period 2006-2010.

C. ICT developments in the EAC

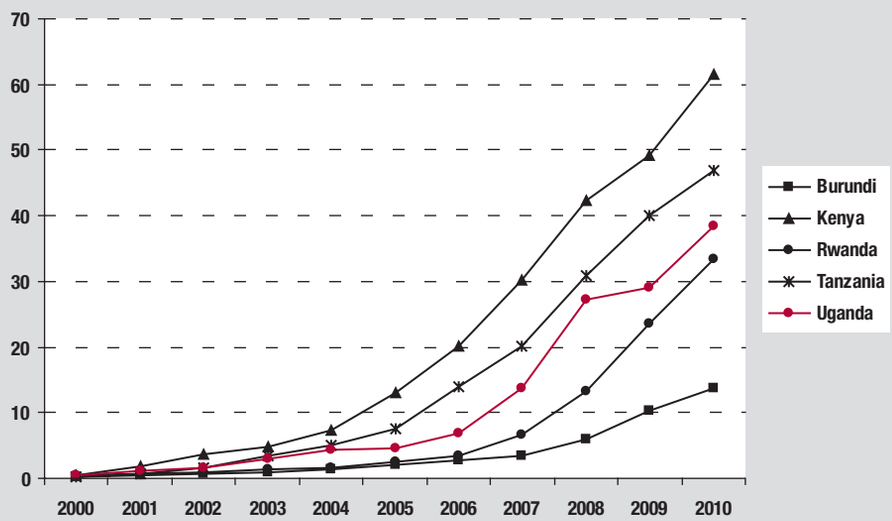
It is beyond the scope of this report to examine all aspects of ICT development within the region. However, two key areas have been particularly important for the economic and regulatory environments: the improved fiber-optic links between the region and the rest of the world and the expansion of mobile telephony and related services, notably mobile money (see Table 1).[11]

In July 2009, the first under-sea fibre optic cable network, SEACOM,[12] reached Kenya, the United Republic of Tanzania, Uganda, Mozambique, and South Africa. It was soon thereafter connected with Rwanda.[13] This marked the beginning of an era of radically faster and cheaper Internet use in East Africa.

In 2010, the second submarine fibre optic cable system, EASSy became operational along the East and South African coasts to service voice, data, video and Internet needs of the region.[14] It links South Africa with Sudan, with landing points in Mozambique, Madagascar, the Comoros, the United Republic of Tanzania, Kenya, Somalia, and the Republic of Djibouti. This made it more economic

to connect the eastern and southern coast of Africa with high-speed global telecommunications network. Average mobile penetration in the EAC had reached 40 subscriptions per 100 inhabitants in 2010, with the highest level noted in Kenya (61) and the lowest in Burundi (14) (figure 1).

Figure 1. Mobile cellular telephone subscriptions in the EAC per 100 inhabitants



Source: UNCTAD, based on ITU World Telecommunication/ICT Indicators, 2011

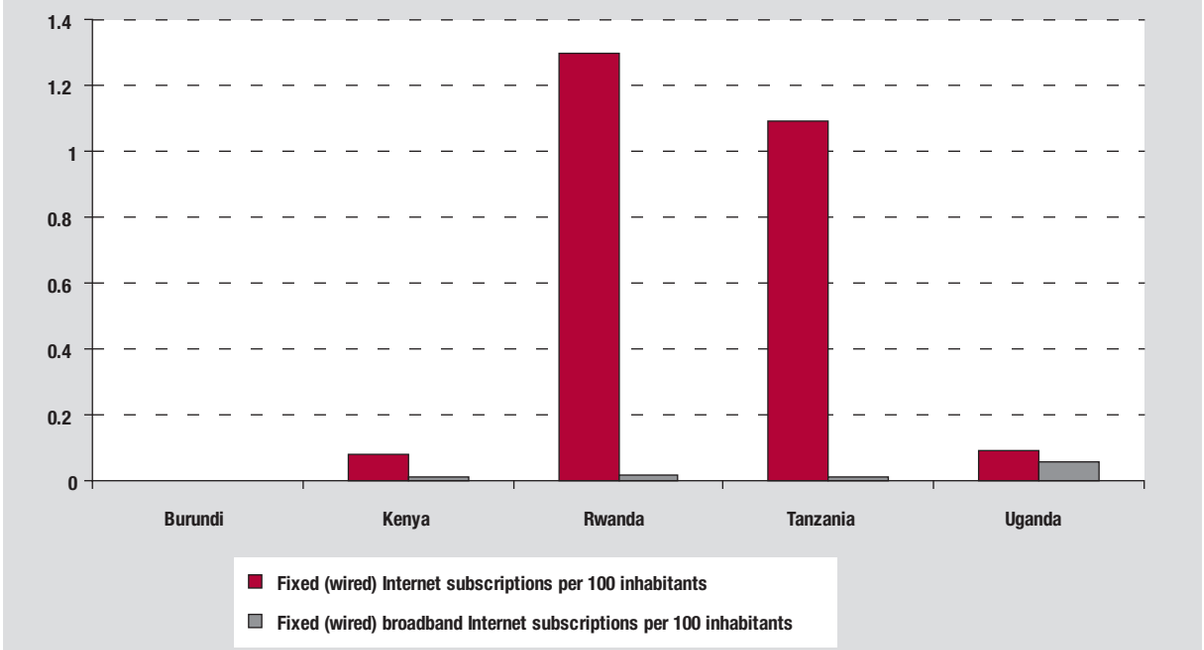
Table 1. Mobile Money snapshot across East Africa (as at 31st August 2011)

Category	Burundi	Kenya	Rwanda	United Republic of Tanzania	Uganda
Population (thousands)[15]	8,413	40,669	10,660	45,012	33,532
Percentage of the population 20 years and above	62.3%	57.7%	57.5%	55.5%	51.7%
Mobile network operators	5	4	2	7	6
Mobile subscriptions[16]	1,076,478	24,960,000	3,730,000	21,203,698	16,015,959
Mobile money platforms	1	4	2	4	3
Mobile money subscriptions	29,000[17]	17,800,000[18]	309,127[19]	9,200,000	2,100,000
Ratio of mobile money subscriptions to mobile subscriptions (%)	2.7	71.3	8.3	43.4	8.1

Source: UNCTAD Mobile Money for Business Development in the East African Community: A Comparative Study of Existing Platforms and Regulations, 2012

While the mobile penetration has significantly increased overtime, the fixed Internet penetration was merely 0.512 in 2010 and the fixed broadband Internet penetration reached only 0.02 (figure 2). In this context, one of the challenges of the EAC will be to leverage existing broadband infrastructure by aggregating demand and scaling up applications in the public sector through for instance e-government, e-business and other e-services.

Figure 2. Fixed (wired) Internet and broadband Internet subscriptions per 100 inhabitants (2010)



Source: UNCTAD, based on ITU World Telecommunication/ICT Indicators, 2011

D. The need for cyberlaw reform

Regional ICT, together with the expected increase in online activities by the private sector as well as public administration, underline the need to develop up-to-date harmonized cyberlaws in the region, reflecting international best practice.

The e-government initiative launched in 2005 identified the creation of an enabling legal and regulatory environment as a critical step for effective implementation of e-Government strategies at national and regional levels.[20] It further emphasized that operational efficiency of any e-Government strategy needs strong back-up support of relevant legislation.

The Regional e-Government Framework Stakeholders Consultative meeting held in Nairobi (28-29 June 2005) identified Cyberlaws and e-Justice, as well as Information Security, as key crosscutting issues for the successful implementation of the e-government applications in East Africa. As a follow-up on the Nairobi recommendations, two workshops were held in Kampala: a "Workshop on Cyberlaws and e-Justice" (25–26 April 2006) and a "Workshop on Information Security", (27–28 April 2006). These identified priority laws that needed to be harmonized, made recommendations and drafted an action programme. The recommendations included, among others:

a) the EAC should ensure necessary coordination intended to harmonize regional and national legal frameworks in order to create an enabling environment for the successful implementation of the e-Government and e-Commerce Programmes in the region, and

b) a Task Force should be constituted from amongst key players and stakeholders in the region to spearhead the implementation of a roadmap towards the creation of a harmonized legal framework for cyberlaws in the EAC.

E. The EAC Task Force on Cyberlaws and reform process

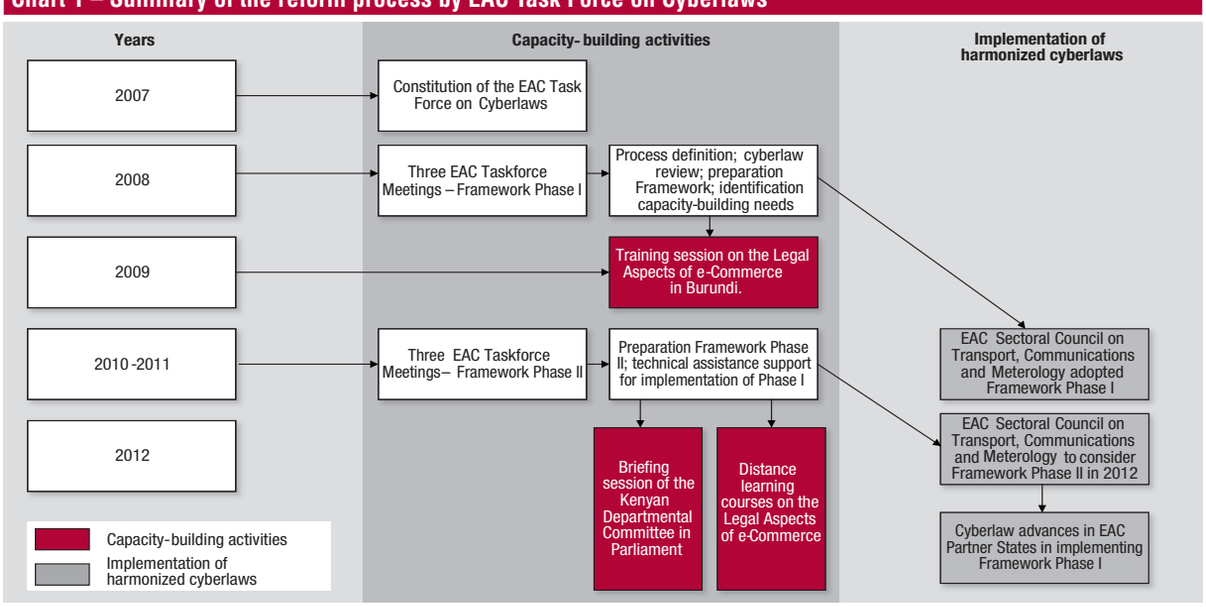
Against this background, the EAC, with the assistance of UNCTAD, established a Task Force on Cyberlaws (the 'Task Force') composed of experts from the Partner States (see chart 1). Since 2007, UNCTAD has been providing a mix of legal advice and training to build awareness on policy and legal issues pertaining to e-commerce. A series of consultative Task Force meetings provided an opportunity for Partner States to discuss and agree on the main principles for cyberlaw harmonization. The commitment of EAC members engaged in the reform process has been instrumental in keeping the momentum. Regional political institutions, such as the East African Legislative Assembly (EALA); stakeholder entities, such as the East African Business Council and the East African Law Society, as well as international bodies, such as UNCITRAL, UNCTAD and UNECA, have been closely associated with the legal drafting and harmonization processes.

In January 2008, the first regional Task Force meeting was held in Arusha (United Republic of Tanzania).[3] At the meeting, attendees discussed a range of issues relating to the need to reform national laws to address the increasing use of the Internet as a medium for electronic commerce and administration. The Task Force noted and recommended that the process of law reform be coordinated at a regional level and harmonized and benchmarked against international best practice. The Task Force also recommended that a comparative review of the existing laws and bills of Partner States be undertaken as a basis for the development of a harmonized regional framework for cyberlaws.

A participatory approach and consultative methodology was adopted in the Task Force proceedings. It became apparent that the region was in dire need to harmonize the on-going national initiatives on cyberlaws, since each country was at a different stage in the development of its domestic cyberlaws. As of September 2008:

- The Republic of Uganda had prepared three bills that had been approved by Cabinet and were awaiting presentation to parliament for debate and enactment: Electronic Transactions Bill; Digital Signatures Bill; and Computer Misuse Bill.
- The Republic of Kenya had a draft Electronic Transactions Bill covering aspects of legal recognition of e-documents and transactions. The bill further provided for institutional arrangements, offences, dispute resolution mechanism and safeguards for privacy and data protection.
- The Republic of Rwanda had a draft bill providing for an omnibus law, covering electronic transactions and signatures, with similarities to the draft bills of Uganda and Kenya.
- The United Republic of Tanzania had no specific cyberlaw, but in 2005 its Law Reform commission

Chart 1 – Summary of the reform process by EAC Task Force on Cyberlaws



Source: UNCTAD

had submitted a report with recommendations on the legal framework for e-commerce and cybercrimes. In 2007, the United Republic of Tanzania had also amended the Evidence Act to recognize electronic evidence.

- Meanwhile, the Republic of Burundi was yet to develop any cyberlaws.

In terms of developing a draft legal framework for EAC Partner States, the Task Force recommended that the process of reform be divided into two phases. In Phase I, cyberlaw reforms would focus on five key topics: electronic transactions, electronic signature and authentication, data protection and privacy, consumer protection and computer crime. Phase II would then address four topics that affected cyberspace activities, but also raised broader issues of concern that were beyond the scope of the Task Force: intellectual property rights, competition, taxation and information security.

In May 2008, a draft legal framework was prepared for consideration and discussion at national consultative meetings. Feedback from these consultations was presented at a meeting of the Task Force, in Kampala, Uganda in June 2008.[22] The delegates then examined and debated the draft in detail and provided further input, and also identified the key principles and issues with respect to each of the five subject areas.[23] The Draft Framework prepared in Phase I was adopted at the 2nd Extraordinary Meeting of the EAC Sectoral Council on Transport, Communications and Meteorology in May 2010 (see Annex I).

The Task Force then embarked on preparation of the draft legal framework on issues earmarked for Phase II. In June 2010, it met in Kigali, Rwanda to examine the relevant issues. As with Phase I, the purpose was to develop a regional framework for adoption and/or adaptation by the Partner States. Further meetings were held in Mombasa, Kenya in March 2011, and Zanzibar, the United Republic of Tanzania in October 2011.[24] Some 17 recommendations in the four areas were debated and eventually adopted by the Task Force on 26 October 2011 (see Annex II). They were designed to harmonize the law reform process between the EAC Partner States, as well as reflect international best practice. At the time of preparing this report, the Phase II Framework had been submitted for approval to the EAC Sectoral Council for Transport and Communication.

In terms of national implementation of the recommendations, the EAC Secretariat is tasked with monitoring progress among the Partner States. In addition, UNCTAD continues to offer support at a national level, by organizing parliamentary briefings to educate and facilitate the adoption of the appropriate legal instruments, and by delivering training programmes for relevant stakeholders including the judiciary and law enforcement agencies. In Kenya, for example, a briefing session was held in March 2011 with the Departmental Committee in Parliament that handles matters touching on the communications sector.[25]

Significant progress was made by each Partner States, although at different paces (Table 2). The Task Force has proved very successful at raising the profile of these important issues, at both a national and regional level. This has resulted in the adoption of existing, but previously stalled, reform measures (e.g. Uganda) and the preparation of new legislative initiatives (e.g. Rwanda).

Table 2: Progress made by EAC countries in the area covered by Framework, Phase I (2008-2012)

	Electronic transactions and signatures		Data protection and privacy		Consumer protection		Computer crime	
	2008	2012	2008	2012	2008	2012	2008	2012
Burundi	None	Draft	None	Draft	None	Draft	None	Draft
Kenya	Draft	Enacted	Draft	Draft	Draft	Draft	Draft	Enacted
Rwanda	Draft	Enacted	Partial	Partial	None	Partial	Draft	Enacted
United Republic of Tanzania	None	None	None	None	None	None	None	None
Uganda	Draft	Enacted	None	None	Draft	Draft	Draft	Enacted

Source: UNCTAD

F. Law reform topics

As noted in the previous section, the work of the Task Force was divided into two phases, each covering different topics of concern. In each case, the Task Force was careful to ensure that the EAC approach reflected best practice, with special attention given to compatibility with leading international public law instruments addressing the respective topics. The following briefly outlines concerns arising in respect of each topic.

Phase I

- **Electronic transactions and signatures -** The adoption of electronic means of doing business can generate legal uncertainties about the validity, enforceability and admissibility of electronic messages and signatures. Such legal uncertainties may originate in primary legislation, secondary regulations, administrative practices and procedures, as well as the attitudes of the judiciary. Law reform can remove or reduce such legal uncertainties, thereby facilitating e-commerce.
- **Cybercrime -** As e-commerce expands, criminal activity inevitably follows. As with electronic transactions, the existing criminal law may not adequately address traditional criminal conduct (e.g. fraud) carried out using ICTs or new forms of criminality (e.g. perpetrated through the use of viruses). As well as reforming the substantive criminal law, to effectively criminalise such conduct, reforms may also be required to national rules governing criminal procedure, especially the adequacy of the investigative powers of law enforcement.
- **Consumer protection -** Consumers can benefit greatly from e-commerce; although the nature of the transaction can differ from a traditional physical environment, particularly knowing with whom the consumers are dealing and the speed with which a transaction can be concluded and payment made. Adequate consumer protection rules that reflect the unique feature of e-commerce can enhance consumer trust and confidence and therefore take-up of e-commerce or mobile commerce.
- **Data protection -** Personal data are sometimes said 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 the grant of rights to use the customer's data for marketing purposes. The need to strengthen the control over the use and abuse of personal data was examined, including the imposition of obligations on those processing such data and the granting of rights to the individual whose data are being processed.

Phase II

As noted above, given the remit of the Task Force, the Phase II covered topics that could only be considered from the limited perspective of some of the implications arising from operating in a cyberspace environment. The EAC has other fora where these topics are examined from a more general perspective. As such, the Task Force was careful not to interfere with, or pre-empt, the work of these other bodies.

- **Intellectual property rights** - Consideration was given to the need to reform existing regimes, especially copyright, in order to maintain the protections of rights-holders, while limiting the potential liabilities of intermediaries. The resolution of disputes arising from the operation of national domain name systems and trademark law was also considered.
- **Competition -** Effective domestic competition laws and regulatory authorities can protect both the competition between market participants and the interests of consumers. Cyberspace can present unique opportunities to facilitate a competitive environment, but can also challenge a regulator's ability to control abuse of competition.
- **Taxation -** E-commerce can challenge existing taxation rules, especially with respect to the consumption of digital products and services. Possible approaches were examined, as well as issues relating to the management and collection of taxation revenues.
- **Information security -** The operation of appropriate information security measures underpins a number of other topics, such as cybercrime and data protection. Laws can be used to promote the implementation and maintenance of good information security practices and procedures.

G. Challenges to reform

A major challenge for any developing country is to successfully take the process of law reform from

initial recognition of an issue, and the preparation of draft measures to their formal adoption by the national political institutions and implementation in a manner that has a real impact on business and administrative attitudes and practices.

Addressing the process of effective law reform often has to involve a number of stakeholders, elements and steps. First, there is the need for explicit political commitment at the highest level of government and the legislature to the law reform process. This generally requires a sustained process of raising awareness, especially among parliamentarians who often have a broad range of issues competing for their attention. Second, a relevant government ministry must claim ownership over the matter and be prepared to devote sufficient internal resources, both to carry out the necessary work as well as liaise and coordinate actively with other relevant stakeholders in the process, particularly, but not exclusively, other ministerial departments and public authorities.

A third element is the need to identify and appoint relevant technical and legal expertise to support the lead ministry, internal to the authority and/or external, whether located nationally or internationally. The work of the expert(s) should then be supported through the establishment of a stakeholder review group, chaired by the lead ministry, including representation from the public and private sectors. Obvious potential candidates include people from the ministry of justice, the national law reform commission and local commercial practitioners. Any draft measures prepared by the experts would then be subjected to a process of scrutiny by the stakeholder review group, which should both substantially improve the quality of the final draft and facilitate awareness and build support for the proposal among the wider community. Finally, the draft measure needs to be steered through the parliamentary process by the lead ministry, ensuring that relevant steps are taken to fully explain the purpose, nature and consequences of the measure to the political representatives.

One of the main issues faced by Partner States is the lack of experience of policy makers and the legal profession in general with legal issues related to e-commerce. The EAC Task Force members reported capacity building needs in this area during the law reform process, and training activities are being supported by UNCTAD.[26] Building capacity among the persons and institutions that will be required to adopt implement, manage or operate in the reformed environment is still a priority. In particular, the regulatory authority, other law enforcement agencies and the judiciary were identified as requiring training to ensure that the reforms are effective.

Envisaging law reform has always been substantially easier than actually achieving it. To address successfully the legal aspects of ICT development requires that states devote as much time and resources to the process of law reform itself as to the various legal topics identified.

The next part of the study examines the current national legal frameworks and law reform initiatives being pursued in each Partner State, reflecting the progress in implementing Phase I and II of the Framework. In each Partner State, the law reform process is a component of national ICT policy and strategy. The relevant laws, draft laws and regulatory institutions are identified.

NOTES

1. See UNCTAD/DTL/STICT/2009/1 and UNCTAD/DTL/STICT/2009/3
2. http://www.eac.int/
3. The Treaty entered in force on 7th of July 2000, and was amended on 14th December 2006 and 20th August 2007. The full text is to be found at http://www.eac.int/treaty/
4. Except for Kenya, EAC countries are using the UNCTAD ASYCUDA system for custom automation.
5. Article 47 provides that Partner states undertake to approximate their national laws and to harmonize their policies and systems, for purposes of implementing the Protocol. http://www.eac.int/advisory-opinions/cat_view/68-eac-common-market.html
6. The timelines were provided by the 13th Ordinary Summit of Heads of State in 2011.
7. Article 8(1)
8. Article 126(2)b
9. The Sub-Committee on the Approximation of Laws in the EAC Context
10. As noted below (2.3), membership of the EAC is shifting Rwanda and Burundi towards a common law approach.
11. See UNCTAD Report, Mobile Money for Business Development in the East African Community: A Comparative Study of Existing Platforms and Regulations, June 2012 (UNCTAD/DTL/STICT/2012/2, available at http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf
12. http://www.seacom.mu/
13. Daily Nation newspaper on the web, 23rd July 2009. The cable covers some 17,000 kilometres.
14. http://www.eassy.org/index-2.html. The cable covers some 10,000 kilometres.
15. United Nations, Department of Economic and Social Affairs, Population Division (2011). World Population Prospects: The 2010 Revision, CD-ROM Edition.
16. In the EAC, mobile subscription numbers are determined on the basis of active SIM cards (make or receive call/SMS) over a 90-day period. Given that many individuals own multiple SIMs, this compounds computing mobile teledensity. Figures for Burundi, Kenya, Uganda and the United Republic of Tanzania obtained from interviews with regulators at the end of March 2011. Mobile money subscriptions reflect customers who have completed both registration and activation procedures for the service, but provide no indication of whether customers have ever made any transaction or how recently.
17. Email interview with Cyrille Nibigira, General Manager, Business Development for Econet Wireless Burundi. Econet Wireless Burundi operates Ecokash, the only mobile money platform in Burundi (June 2011).
18. Central Bank of Kenya (CBK), Governor's speech on the relaunch of Airtel Money Transfer Service (August 2011) www.centralbank.go.ke/downloads/speeches/2011/Governor's%20remarks%20at%20Launch%20of%20Airtel%20Money%20Transfer%20Service.pdf.
19. Rwanda, The New Times (August 2011), www.newtimes.co.rw/index.php?issue=14718&article=44174
20. EAC Development Strategy 2006-2010
21. EAC/TF/2008
22. EAC/TF/2/2008 at 4
23. Ibid, at 5
24. See 'EAC Develop Cyber Laws', Press Release, 25 October 2011, available at http://www.eac.int/about-eac/eacnews/834-eac-develops-cyber-laws.html
25. http://www.unctad.org/Templates/meeting.asp?intItemID=2068&lang=1&m=21395 (Accessed on November 25, 2011).
26. UNCTAD organized training workshops in Kenya (2006), Burundi (2009); a briefing of Parliamentarians in Kenya was organized in 2011. Delivery of the TrainForTrade distance-learning version of the training course on the Legal Aspects of E-commerce for Rwanda and Kenya was organized in May 2012 and other capacity-building activities are planned in 2012 and 2013.

PART II
REPORTS ON THE LEGAL FRAMEWORKS IN THE PARTNER STATES

A. BURUNDI IN BRIEF

Economy	2010
GDP current prices, million $	1'400.0
GDP per capita	167
Real GDP growth %	3.9
GNI, million $	1'401.7
GNI per capita	170

Trade	
Merchandise Exports, million $	100.5
Merchandise Exports, % of exports of Merch. and Services	55.8
Main merchandise exports, million $	
Coffee and coffee substitutes	55.5
Tea and mate	12.8
Gold, non-monetary (excluding gold ores and concentrates)	8.8

Services Exports, million $	79.5
Services Exports, % of exports of Merch. and Services	44.2
Main services exports, million $	
Government services not indicated elsewhere	72.2
Tourism	1.8

Demography	
Population, millions	8.4
% of youth population (below age 20)	49.3
Life expectancy at birth (years)	50.9
Adult literacy (age 15+) as %	66.6
Youth literacy (age 15-24) as %	76.6

Labor and finance	
Labor in Agriculture, as %	89.2
FDI inflows, million $	14.1
Remittances, million $	28.2

ICT	2000	2005	2010	Growth Rate (00-10)*
Fixed (wired) Internet subscriptions per 100 inhabitants	0.02	..	0.06	11.61
Fixed telephone lines per 100 inhabitants	0.31	0.43	0.39	2.32
Mobile cellular telephone subscriptions per 100 inhabitants	0.26	2.11	13.72	48.68
Percentage of fixed telephone lines in urban areas	87	..	..	..
Percentage of fixed telephone lines which are residential	63	..	..	..
Percentage of individuals using the Internet	0.08	0.54	2.1	38.65

Sources: UNCTAD (UNCTADstat database) World Bank (WDI database), UNDESA (Population Division), UNESCO (UIS database), FAO (FAOSTAT database)

1. Introduction: ICT policy and legal framework in Burundi

The Government of Burundi has adopted a National ICT Development Plan for the period 2011-2015. Elaborated by the Executive Secretariat for ICT (SETIC), it is a revision and update of a previous strategy (2006-2010). It was designed to make it more compliant with the 2005 World Summit on the Information Society (WSIS) commitments.[27] The adopted plan is articulated through ten pillars, one of which is concerned with ensuring an appropriate legal and regulatory environment.

Facilitating the development of a dynamic information society is one of the main objectives of the establishment of the Communications Infrastructure Project (CIP) for Burundi, which falls under the national policy on ICTs and the National Information and Communication Infrastructure Plan (NICI).

The efforts of the CIP are concentrated on identifying those elements that result in a reduction in the cost of connectivity; an extension of national coverage in telecommunication networks; and the sustainability of national and international broadband infrastructure. However, the establishment of the necessary communication infrastructure is not an end in itself. The Government's objective is to enable Burundi to benefit from a real technological leap to boost economic growth for the development of activities in a secure legal environment using ICTs. The current legal and regulatory framework does not provide a secure environment for the creation of a climate of confidence without which e-commerce will not take off.

In this regard, the Government has drafted a single legislative instrument ('draft Bill') to create a framework within which the information society can evolve and grow in Burundi. The reforms to be engaged in the area are in line with the ICT National Policy and the National Strategic Plan on ICT and fall within its second strategic pillar.

Currently, the existing framework focuses mainly on telecommunications infrastructure development and services. Since 1997, when the current telecommunications law was enacted,[28] the Burundi telecommunications sector has seen significant development rendered possible by its liberalization. However the level of growth does not compare well with other Partner States. In part, this is due to lower purchasing power. It may also reflect the fact that the framework does not fully reflect international best practice in terms of openness and transparency, predictability, neutrality and objectivity, which may have had a negative impact on foreign investment in the sector.

In terms of the non-telecommunications legal framework, it currently comprises the following pieces of primary legislation, some of which address cyberlaw concerns:

- Central Bank Act n°1/34 of December 2008;
- Competition Act n°1/06 of March 2010;
- Customs Code Act n°1/02 of January 2007;
- Industrial Property Act n°1/13 of July 2009;
- Penal Code Act n°1/95 of 22 April 2009;
- Press Act n°025/01 of November 2003;
- Private and Public Companies Act n°1/09 of May 2011;
- Protection of Right of Author and its related Act n°1/06 of December 2005;
- Trade Code Act n°1/07 of April 2010;
- Value Added Taxation Act n°1/02 of February 2009.

These laws constitute the backbone of commercial activities in general, but without emphasis on e-commerce. Some of the reforms recently adopted in Burundi already take into account ICTs as outlined below:

- The Press Act n°025/01 of 27 November 2003 refers explicitly to the concept of information published on the Internet. The text also mentions news on web agencies subject to prior declaration to the National Council of Communication and the public prosecutor who requires information on their identity, including where the site is hosted;
- Industrial Property Act n°1/13 of July 2009, and the Protection of Right of Author and its related Act n°1/06 of December 2005 both include the protection of software and other electronic or digital formats;
- Penal Code Act n°1/95 of 22 April, 2009 contains some articles on cybercrime, including provisions related to computer-related forgery (article 473), computer-related fraud (article 474), unauthorized access devices (article 475) and system interference (article 476);
- The Telecommunications Act n°1/11 of 4 September 1997 includes the following provisions that reference ICT-related offences:

1. Article 10 prohibits the unauthorized interception of communications not intended for use by the general public and the unauthorized disclosure, content publication or use of any communications not intended for use by the general public. Article 24 grants the regulator the ability to authorize such conduct.
2. Article 23 requires network and service providers to ensure confidentiality, data protection and secrecy.

2. Status of cyberlaws

Since the meeting of the EAC Task Force on 28-30 March 2011, the draft Bill on electronic transactions was produced under the supervision of the SETIC. The draft Bill was prepared in consultation with relevant stakeholders and has taken into consideration the work already carried out in the region.

The Bill does not intend to respond exhaustively to all the legal and regulatory issues raised by the Task Force Recommendations. It provides for mechanisms of self-regulation of electronic exchanges that can lead consumer representatives, active Internet companies and the Government to agree on the establishment of alternative procedures for dispute resolution.

The draft Bill has been examined by the Ministry of Justice to check its compliance with existing laws. The Council of Ministers is scheduled to discuss this during the course of 2012. The next stage will be the sensitization of the members of the Parliament – the members of the National Assembly and those of the Senate – to raise their awareness and understanding of the issues before adopting the Bill. After the adoption by the Parliament, the Bill will return to the Executive for enactment.

The Bill enacts the basic principles applicable to electronic communications, including the following aspects:

2.1 eContracting and administration, e-signatures and evidentiary issues

Chapter 1 of Title II states that any agreements, writing and signature may be made and stored in electronic format. The electronic format writings must be qualified as original and have the same probative force as that of traditional paper writings and documents. This recognition, which is not explicit in the current legislation, should have a significant impact on the development of electronic trade.

The recognition of the right to form valid electronic contracts is also essential. Chapter 2 of Title II provides that a contract shall not be denied legal effect merely because it is concluded by means of a data message. The rules governing the formation of these contracts must be specified to ensure the security of electronic exchanges.

2.2 Data protection and privacy

Chapter III (Articles 37 to 39) deals with online data collecting, prospecting and advertising electronically.

The draft Bill provides for specific provisions to guide online collection of personal information of the users (e.g. names and addresses) by imposing obligations to inform users of the purpose of the collection and the means made available to the user to access, modify and/or delete these data.

2.3 Consumer protection

The first chapter of the Bill (Articles 25 and 26) sets out the principles, the applicable law and the liability of the parties. Chapter II (Articles 27 to 36) deals with the rights and obligations of the contractors in e-commerce.

Buying goods or services online and remotely requires the adoption of a set of provisions to complete the existing law on consumption. The Act provides, in particular, strengthened obligations for communicating the identity of the buyer, the information about the purpose and the terms of the sale, and the time of performance. A right of withdrawal of seven days is also expected to allow the consumer to cancel the transaction online in certain specified circumstances.

2.4 Copyright

Regarding intellectual property law, Burundi is planning to amend the 2005 Law because it does not address digital issues.

2.5 Cybercrime and cybersecurity

Chapter VII (Articles 60 to 72) is devoted to administrative sanctions and to the criminal provisions.

As stated above, Act n°1/95 of 22nd April 2009 relating to the review of the criminal code deals with cybercrime in detail. The draft Bill completes the 2009 Act by providing for offences on the violation rules provided for in this Act on the protection of personal data, illegal content, tax offences, non-compliance with the provisions applicable to electronic signature certification, cryptology and taxation. The first chapter (Articles 60 and 61) provides for administrative sanctions, while the second (Articles 62 to 72) sets out criminal provisions.

An accompanying draft decree on data conservation gives details about the type and scope of the information to be stored by the communication service providers, including for the purpose of future usage in police or judicial investigations. The decree details what data are to be retained and the applicable conditions and time period for retention.

The draft Bill includes a large number of provisions about the legal conditions necessary for the security of the digital economy. Chapter 1 (Articles 55 and 56) introduces terms for the usage, transfer, import and export of cryptographic products.

In Chapter II (Articles 57 to 59), the issue of accreditation of certification service providers and their liability is addressed. It mandates a regime applicable to cryptology and certifications, making sure those providers establish and implement rules in conformity with international best practice and standards.

In addition, a draft decree on cryptography describes the procedures to be followed in cases of declaration or authorization exemption. A draft decree on electronic signatures deals with the accreditation of certification service providers. The characteristics and components of certificates, including provider identity, information needed for signature recognition, and identification code are delineated. The text also deals with issues concerning guarantees, integrity and security services, and sets the conditions for certificate revocation. The text describes the accreditation procedure issued by the Ministry of ICT.

2.6 Content control

Title III (Articles 16 to 24) is related to the protection of users and the liability of intermediary providers and content publishers.

Article 16 of the draft Bill sets out the principle of electronic communication freedom and its limits. For Internet and the broadcasting radio and press, the freedom of communication is limited by certain principles (including prohibition of interference with the person, or to maintain the public order). Chapter II (Articles 17 to 22) of the Act defines the responsibility of technical providers, who deliver communications or provide Internet access, and the content publishers. In this sense, the law adopts the fundamental principle of exempting technical intermediary service providers from liability and the obligation to monitor content, except where there is a need to prevent the proliferation of, or access to, content about which they have been notified as constituting an obvious violation of Burundi law.

The draft Bill also requires Internet access providers to store the needed data for the identification of illegal content publishers. Chapter III (Articles 23 and 24) of the draft Bill also provides specific obligations applicable to online content publishers to allow users to identify them and eventually exercise a right of reply.

2.7 Internet and mobile payment systems

In order to complete the draft Bill, the Central Bank of Burundi has prepared three studies with the objective of producing legal and regulatory instruments on three specific aspects:

- Legal Framework for 'Système Brut de Paiement en Temps Réel au BURUNDI'
- Legal Framework for 'MONETIQUE in Burundi'
- Legal Framework for 'MOBILE BANKING in Burundi'.

2.8 eTaxation

Chapter IV (Articles 40 to 44) of the Bill handles the issues of taxation of electronic transactions and customs fees. This chapter is itself subdivided into two sections. The first (Articles 40 to 43) concerns the Value Added Tax (VAT) regime, while the second (Article 44) is devoted to custom fees. The provisions will clarify the conditions for establishing VAT and customs for electronic contracts and/or services provided electronically via the Internet.

In addition, an accompanying draft decree is meant to clarify the object and the scope of Articles 40 and

42 of the draft Bill dealing with VAT on electronic services and products. A list of the potential deliverable services is also given. The issues of the declaration procedures, the identity of the person in charge, as well as the collection of the VAT are fixed by this decree.

3. Regulatory authorities

Two regulatory authorities are in place in Burundi, one for the Telecommunications sector, the Agence de Régulation et de Contrôle des Télécommunications (ARCT) and one in charge of media regulation, the Conseil National de la Communication (CNC). These two institutions are implementation authorities and are not responsible for regulatory reforms.

Reform is the responsibility of the Ministry in charge of ICT in general and, in particular, by the SETIC whose mission among others is the promotion of the National ICT Policy and the implementation of the National Information and Communication Infrastructures Plan (NICI Plan).

The ARCT is in charge of the telecommunications sector. Its mission includes among others, the settling of disputes between users or subscribers and the operators on the one hand and between the associated services providers on the other. ARCT deals with spectrum management, tariffs and interconnection control. It also delivers concessions and licenses for the establishment and management of radio networks.

The regulatory authorities are not independent of the Government, but the draft Bill is proposing greater independence for the ARCT, in order to create an enabling business environment for the ICT sector.

B. KENYA IN BRIEF

Economy	2010
GDP current prices, million $	32'151.9
GDP per capita	794
Real GDP growth %	5.0
GNI, million $	31'810.2
GNI per capita	790

Trade	
Merchandise Exports, million $	5'150.7
Merchandise Exports, % of exports of Merch. and Services	58.4
Main merchandise exports million $	
Tea and mate	900.4
Natural gums, resine & horticulture	609.4
Vegetables	277.2
Services Exports, million $	3'675.5
Services Exports, % of exports of Merch. and Services	41.6
Main services exports, million $	
Transport	1'562.6
Tourism	799.9

Demography	
Population, millions	40.7
% of youth population (below age 20)	52.9
Life expectancy at birth (years)	54.9
Adult literacy (age 15+) as %	87
Youth literacy (age 15-24) as %	92.7

Labor and finance	
Labor in Agriculture, as %	70.6
FDI inflows, million $	133.0
Remittances, million $	1'777.0

ICT	2000	2005	2010	Growth Rate (00-10)
Fixed (wired) Internet subscriptions per 100 inhabitants	0.13	0.22	0.08	-4.74
Fixed (wired) broadband Internet subscriptions per 100 inhabitants	..	0.02	0.01	..
Fixed telephone lines per 100 inhabitants	0.93	0.81	1.14	2.06
Mobile cellular telephone subscriptions per 100 inhabitants	0.41	12.95	61.63	65.08
Percentage of fixed telephone lines in urban areas	95.2	95	..	..
Percentage of fixed telephone lines which are residential	43	..	..	..
Percentage of households with a computer	0.5	3.4	7.95	..
Percentage of households with Internet access at home	..	1.2	4.04	..
Percentage of individuals using the Internet	0.32	3.1	20.98	51.94
Percentage of the population covered by a mobile cellular network	..	62	..	..

Sources: UNCTAD (UNCTADstat database) World Bank (WDI database), UNDESA (Population Division), UNESCO (UIS database), FAO (FAOSTAT database)

1. Introduction: ICT policy and legal framework in Kenya

The ICT sector in Kenya has experienced unprecedented growth in the last decade and the role played by ICTs in the generation of socio-economic development has been noted. This trend has been aided by market liberalization and augmented by convergence, new technologies and resultant innovations. In order to embrace the opportunity, the Government of Kenya has recognized and integrated the ICT platform in the achievement of development goals under the Vision 2030. The ICT platform is recognized in public policy as a tool to improve the livelihood of Kenyans and is backed with a commitment to ensuring the availability of accessible, efficient, reliable and affordable services:

"The achievement of e-Government is one of the main priorities of the Government towards realization of national development goals and objectives for wealth and employment creation. Effective and operational e-Government will facilitate better and efficient delivery of information and services to the citizens, promote productivity among public servants, encourage participation of citizens in Government and empower all Kenyans."

~ H.E. Hon. Mwai Kibaki, President of Kenya[29]

2. Status of cyberlaws

There has been concerted activity for the development of cyberlaws in Kenya for almost a decade now. Its genesis was the Postal and Telecommunications Sector Policy Statement that was issued in January 1997 and is credited as the anchor policy that paved the way for robust growth in the ICT sector in Kenya. The policy recognized that *'if the sector [was] to fulfill its mission as a catalyst for growth…. then fundamental structural reforms [had to] be initiated.'*[30] It captured the policy objective for the sector as *'the ability to ensure availability of efficient, reliable and affordable communications services throughout Kenya'*.[31]

Premised on this policy, an e-Government Strategy was issued in 2004.[32] The strategy recognized that e-government is a fundamental element in the modernization of government. It sought to provide a common framework and direction across the public sector and to enhance collaboration within and among public sector organizations, between government and the citizens that it serves in the implementation of government policies. Thereafter, the National ICT Policy was revised, raising the policy bar and expectations placed on ICTs as a driver for socio-economic development. Kenya has been trying to re-position itself in order to benefit from business process outsourcing and other IT-enabled service opportunities.[33] It had also encountered a revolution in mobile applications, the most successful of which is a mobile money service called M-Pesa[34] by Safaricom,[35] the largest mobile network operator in Kenya.[36]

Initiatives for the development of domestic cyberlaw legislation were reinforced locally as the need to upgrade the domestic regulatory framework to be in line with global best practice had been recognized. The need for a legislative framework that addressed issues of certainty and public trust around transactions conducted with various forms of ICTs was urgent.

Kenya now has a cyberlaw framework articulated under the Kenya Information and Communication Act (KICA), Chapter 411A of the Laws of Kenya, which was passed in January 2009.[37]

This passage prompted concerted efforts to sensitize key stakeholders – such as the parliamentary committee responsible for ICTs – in order to seek support for its implementation and anticipated further developments within the regulatory framework.

The Kenya Communications (Electronic Transactions) Regulations were passed in 2010 to amplify and complement the normative principles captured in the primary legislation. There is a wider supporting framework for electronic transactions to be found in areas of licensing, consumer protection, and dispute resolution among others.

The mandate for administration of this piece of legislation rests with the national ICT regulator, the Communications Commission of Kenya (the 'Commission').[38] In addition to cyberlaws, the Commission also regulates the telecommunications, radio communications, postal and broadcasting subsectors.

2.1 e-Contracting and administration, e-signatures, evidentiary issues

Part VI.A of KICA deals with electronic transactions and is inspired by UNCITRAL texts. The scope

and content of this part relied significantly on a comparative analysis of the Commonwealth Model Law on Electronic Transactions (2002).[39] The UNCITRAL Model Laws on Electronic Commerce (1996) and Electronic Signatures (2001),[40] the United Nations Convention on the Use of Electronic Communications in International Contracts (2005)[41] and the SADC Model Law on Electronic Transactions and Data Protection were also inspired by UNCITRAL texts.[42]

Recognition of electronic transactions

This portion of the cyberlaw seeks to capture best practice in terms of the recognition and conduct of electronic transaction in Kenya.

Section 83C of the KICA officially recognizes electronic transactions in Kenya and spells out in detail the functions of the Commission in relation to this area of its mandate.

Functions of the Commission in relation to electronic transactions

- facilitate electronic transactions by ensuring the use of reliable electronic records;
- facilitate electronic commerce and eliminate barriers to electronic commerce such as

those resulting from uncertainties over writing and signature requirements;

- promote public confidence in the integrity and reliability of electronic records and electronic transactions;
- foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium;
- promote and facilitate efficient delivery of public sector services by means of reliable

electronic records; and

- develop sound frameworks to minimize the incidence of forged electronic records and fraud in electronic commerce and other electronic transactions.

The recognition of electronic transactions was fundamental because it meant that information would no longer be denied legal effect, validity or enforceability solely on the ground that it was in the form of an electronic version.

The law however provides exemption of this rule under S.83B for the creation or execution of a will, negotiable instruments and documents of title.

In April 2011, the Central Bank of Kenya announced that in collaboration with commercial banks, a cheque truncation project had been adopted.[43] The essence of this project is to replace the physical movement of cheques with electronic information.

Requirement for a license

S.83D(1) introduces the requirement of a license issued under the Act in order to operate an electronic certification system or to update a repository or administer a sub-domain in the Kenya country top level domain (.ke). It further introduces a penalty of a fine not exceeding three hundred thousand shillings or imprisonment for a term not exceeding three years, or both. Section 83E and F go into more detail on the particulars of the required licenses for a structured framework that would be necessary for enhancing trust and confidence in the use of ICTs.

Issues of validity

The execution of a range of legal acts, pertinent issues of form, contract formation and record keeping as well as evidential requirements need to be articulated in the law. This would help clarify issues particularly where uncertainties exist on whether electronic versions are acceptable, or where the previous norm and practise expressly excluded electronic versions.

Section 83G allows for legal recognition of electronic records. Section 83I further elaborates that, where information is supposed to be kept in its original form, the electronic version thereof meets this requirement if there exists reliable assurance as to the integrity of that information.

Criteria for assessing integrity and reliability of information[44]

- Whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
- The purpose for which the information was generated; and
- All other relevant circumstances

The commitment towards adoption of the e-platform by government is reflected in Section 83S by recognizing the use of electronic records and electronic signatures in government and by its agencies.

The law further provides for the publication of any rule, regulation, order, notification or other matter to be published in the electronic gazette.[45] It also provides for the Minister to prescribe the manner and format in which such electronic records shall be created, filed or used, as well as the manner or method of payment of any fee or charge for filing.[46]

The government of Kenya has adopted e-government in recognition that it is a fundamental element in the modernization of government.[47] This is being deployed through four (as listed below) primary delivery models: the relationship between government and citizens (G2C), electronic interactions between government agencies and private businesses (G2B), relationship between governmental organizations (G2G), and the relationship between government and its employees (G2E).[48]

It is therefore now possible to conduct a series of transactions on-line as advertised on the e-government portal:

Do It Online

- o Apply for Public Service Jobs
- o Track status of ID & Passport
- o Exam Results and Candidate Selection
- o Submit Tax Returns Online
- o Customs Services Online
- o Report Corruption Online
- o HELB Loan Repayment Status
- o Business Licensing e-Registry

Source: http://www.e-government.go.ke/

Formation and validity of contracts

Section 83J provides that where an electronic message is used in the formation of a contract, the contract shall not be denied validity or enforceability solely on the ground that an electronic message was used for the purpose of contract formation. The same treatment would apply with regard to a declaration of intent or other statement between the originator and addressee of an electronic message.[49]

This means that where the law requires information to be in writing, the requirement of the law is fulfilled if the information is contained in an electronic version that is accessible and intelligible so as to be useable for subsequent reference.

Legal recognition of electronic signatures

To fulfill the requirement for authentication or signature of any document, the law provides that the requirement will have been met if such information is authenticated by means of an advanced electronic signature affixed in the prescribed manner.[50]

The Minister of ICT has the power to prescribe regulations on type, manner and format of signature as well as control of the processes that would facilitate the identification of the person affixing the signature to ensure adequate integrity.

In order for an advanced electronic signature to be considered adequate for purposes of satisfying the legal requirement, it must meet a certain criteria.

Legal requirement for an electronic signature[51]

- Generated through a signature creation device
- Signature creation data were, within the context in which used, linked to the signatory and to no other person
- Signature creation data were, at the time of signing, under the control of the signatory and of no other person
- Any alteration to the electronic signature made after the time of signing is detectable
- Where the purpose of the signature is to provide assurance of the integrity of that information, any alteration made to that information after the time of signing, is detectable

There is also growing confidence in the conduct of businesses online and the acceptability of credit cards and other on-line financial transactions. E-transactions legislation has enhanced the ease of doing business and expanded the opportunity for delivery of critical services such as education and health to the people of Kenya.

2.2 Data protection and privacy

Increasing reliance on the e-platform for transactions would seem to require a complementary regulatory framework dealing with the protection of users' privacy and the security of information generated

and stored about them. It would govern the manner and purpose of collection of personal information, access to records, storage and security of personal information. Legislation covering this area is yet to be passed. A Data Protection Bill 2009 has been drafted, but is currently only applicable to personal information held by public authorities. This is an area of vulnerability, for which rules need to be established.

2.3 Consumer protection

The Kenya Information and Communications (Consumer Protection) Regulations, 2010[52] articulate a framework to uphold consumer rights and entitlements in the ICT sector. This framework will be complemented by the proposed Consumer Protection Bill, 2011 that seeks to provide for a consolidated regulatory platform for consumer protection for all goods and services consumed in Kenya.[53] The Bill lists as its objects, the protection of the consumer and prevention of unfair trade practices in consumer transactions.

Part IV of the proposed law articulates rights and obligations related to specific consumer agreements, and goes on to recognize Internet agreements. This recognizes that while conventional transactions were entered into in the physical space, increasingly the novelty of agreements in the digital space continues to pose consumer protection challenges in Kenya.

The memorandum of objects and reasons notes that it is a particular source of concern that no law currently exists to specifically regulate consumer agreements[54] entered into online and that the proposed legislation aims to extend protection to consumers doing business via the Internet.[55] The Bill awaits its second reading in Parliament.

2.4 Copyright

Intellectual Property Rights (IPRs) pose a particular challenge because of the ease with which they can be infringed upon by others. While adoption of ICTs has given global visibility to literary works, for example, it has also left them vulnerable to the challenge of infringement.

In order to establish an enforcement framework for on-line IPRs in copyright in Kenya, the Copyright Act, Cap130 recognizes a computer program that is computer generated to be within the scope of a literary, dramatic, musical or artistic work.[56] The law also provides for the definition of 'copy' within a scope that recognizes works in the digital format.[57]

In articulating offences under the Act, the law makes it an offence in certain circumstances, for a person to sell, let, hire, distribute or possess a copy of a work at a time when copyright or the right of a performer is subsisting.[58]

The Industrial Property Act, Cap 3 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. While it does not specifically cite electronic formats, this would be an item for interpretation as to whether it falls within the broad scope of 'other graphic representation'. [59]

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, this may be the next frontier for development of cyberlaws in Kenya.

2.5 Cybercrime and cybersecurity

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

The regulatory framework captures a series of offences in order to ensure compliance with the law. Given the notoriety of cybercrime, these crime categories already are in need of enhancement in order to capture the emerging incidents' mischief. The schedule below provides the list of crimes and attendant penalties.

In early 2011, a Computer Incidence Response Team (CIRT) was established within the Commission as part of efforts towards safeguarding the Kenyan cyberspace and upholding its integrity through early detection of incidences meriting response and investigations. A lot still needs to be done by way of acquisition of the technical skills and equipment for the CIRT as well as building technical capacity and strengthening cooperation with other CIRTs globally.[60]

Cyber-related crimes		
Section	**Offence**	**Penalty (Kenya shillings)**
83U	Unauthorized access to computer data	200,000 or imprisonment for a term not exceeding 2 years or both
83V	Access with intent to commit offences	200,000 or imprisonment for a term not exceeding 2 years or both
83W(2)	Unauthorized access to and interception of computer service	500,000 or imprisonment for a term not exceeding 3 years or both
83W(3)	Unauthorized access to and interception of computer service where the operation of the computer system is impaired, or data contained in the computer system is suppressed or modified	200,000 or imprisonment for a term not exceeding 2 years or both
83X	Unauthorized modification of computer material	500,000 or imprisonment for a term not exceeding 3 years or both
83X(2)	Unauthorized modification of computer material where the operation of the computer system, access to any programme or data contained in the computer system is suppressed or modified or otherwise impaired	200,000 or imprisonment for a term not exceeding 2 years or both
83Y	Damaging or denying access to computer system	200,000 or imprisonment for a term not exceeding 2 years or both
83Z	Unauthorized disclosure of password	200,000 or imprisonment for a term not exceeding 2 years or both
84A	Unlawful possession of devices and data	200,000 or imprisonment for a term not exceeding 2 years or both
84B	Electronic fraud	200,000 or imprisonment for a term not exceeding 3 years or both
84C	Tampering with computer source documents	300,000 or imprisonment for a term not exceeding 3 years or both
84D	Publishing of obscene information in electronic form	200,000 or imprisonment for a term not exceeding 2 years or both
84E	Publication for fraudulent purpose	1,000,000 or imprisonment for a term not exceeding 5 years or both
84F	Unauthorized access to protected systems	1,000,000 or imprisonment for a term not exceeding 5 years or both

2.6 Child online protection

Improper use of ICTs can expose vulnerable population groups such as children to harmful content with undesirable outcomes. The Sexual Offences Act makes it an offence for any person to knowingly display, show, expose or exhibit obscene images, words or sounds by means of print, audio-visual or any other media to a child with intention of encouraging or enabling a child to engage in sexual acts.[61]

The Kenya Information and Communications (Consumer Protection) Regulations, 2010 also recognize the need to protect children from undesirable content and require licensees to establish mechanisms that enable parents and legal guardians to block access to harmful content by children.[62] The law further makes it an offence for any person to promote, glamorize or market alcohol and tobacco products or other harmful substances that are directed at children.[63]

With 43 percent of its population under age 15 and access to ICTs increasing steadily, the need to protect children on-line cannot be emphasized enough. In order to ensure the safety of children as they interact with the Internet, the Commission has put in significant efforts towards education for awareness and empowerment.[64]

2.7 Internet and mobile payments

In the past two decades or so, Kenya has undergone significant reforms and consequent modernization in its payment systems.[65] The Central Bank of Kenya has been involved in facilitating the smooth operation of payments, clearing and settlements systems.[66]

The proliferation of computer applications and communications technology in the financial services sector has resulted in enhanced paper-based payments that have correspondingly evolved into electronic forms.[67] The Electronic Fund Transfer systems (EFTs) are one such example.[68]

The licensing of mobile operators in the last decade has significantly redefined payment platforms and repositioned the handset as the frontier for innovations for m-payments. This began with Safaricom, with M-Pesa in 2007. Airtel Kenya (formerly Zain)[69] followed with Airtel Money and Essar telecom[70] with YuCash in 2009 and finally Orange Kenya (Telkom Kenya)[71] with Iko Pesa in 2010.[72]

The majority of the Kenyan population was unbanked and the m-money platform was quickly taken up by a large user base, the bulk of which belongs to M-Pesa.

This robust market segment has grown largely out of creative regulatory forbearance as there is no defined regulatory framework. There are however on-going discussions on how to formalise m-payments within the regulatory framework.[73]

2.8 eTaxation

As has been the case in the financial services sector, tax collection methods have been affected by ICTs. In recognition of this and in order to lend clarity on emerging trends, the Income Tax Act, Cap 470 introduced an amendment that allowed the Commissioner to prescribe income tax formalities or procedures to be carried out by use of information technology.[74]

In order to uphold the integrity of the e-taxation platform the law makes it an offence for a person to have unauthorized access to, or improper use of, a computerized tax system[75] and outlaws interference with a computerized tax system.[76]

3. Push for legal reform

Arising out of the high uptake of ICTs in Kenya, some unintended outcomes have come to the fore, leading to public outcry and the need for legal reform. Currently, the use of mobiles to commit crimes and the destruction of ICT infrastructure are a cause for a lot of concern. The efforts being undertaken to deal with this in the legislative framework are discussed below.

4. SIM card registration

The mobile phone in particular has been used to exploit the dark side of ICTs.[77] Due to the high mobile penetration in Kenya, it has recently become a major tool of crime. In order to obtain a mobile SIM card, no registration has been required and one can literally buy a SIM card on the street.

This situation is posing an enforcement challenge leading to proposals for legal reform. The Finance Bill, 2011 proposes to compel the registration of subscribers to telecommunication services by making an amendment to the KICA in order to curb the menace.[78]

The bill is awaiting its third reading in Parliament.

5. Damage to ICT infrastructure

Another challenge that has emerged is the damage to ICT infrastructure caused either by activities of economic sabotage or theft, such that ICT networks are rendered unreliable or unusable until they are repaired by operators. This has been perceived as a significant threat to the information economy, with the increased deployment of ICT infrastructure such as fibre optic networks.

To mitigate this negative trend, legal revisions have been introduced through the Energy and Communications Law (Amendment) Bill 2011 to have the damage to ICT infrastructure recognized as an economic crime.[79] In this regard, the proposal is to increase the penalty to a fine of not less than five million shillings or to imprisonment for a term of not

Proposal made in the Energy and Communications Law (Amendment) Bill, 2011

Section 32 of the Kenya Information and Communications Act, 1998 is deleted and replaced with the following new section—

Tampering with telecommunication apparatus.

32. A person who, willfully, with intent to—

(a) prevent, obstruct or delay transmission of any message; or

(b) interfere with the management or operation of a telecommunication apparatus; or

(c) unlawfully intercept or acquaint himself or herself with the contents of any message; or

(d) commits mischief, vandalises, damages, removes, tampers with, touches or in any way whatsoever interferes with any telecommunication apparatus or telecommunication line, post or other thing whatsoever, being part of or used in or about any licensed telecommunication system or in the use thereof, commits an offence and shall be liable on conviction to a fine of not less than five million shillings or to imprisonment for a term of not less than ten years or, both.

32A. A person who severs any telecommunications apparatus or other works under the control of a licensee, with intent to steal, commits an offence and is liable on conviction to a fine of not less than five million shillings or to imprisonment for a term of not less than ten years or both.

less than ten years, or both. This bill is awaiting its second reading in Parliament.

Complementary proposals to amend the Scrap Metal Act have been made to require licensing of scrap metal dealers and introduce a tighter operations regime as dealers have been found to contribute to the vandalism of infrastructure to satisfy dealer supply demands.[80]

C. RWANDA IN BRIEF

Economy	2010
GDP current prices, million $	5'644.8
GDP per capita	531
Real GDP growth %	6.5
GNI, million $	5'537.0
GNI per capita	520

Trade	
Merchandise Exports, million $	297.3
Merchandise Exports, % of exports of Merch. and Services	44.4
Main merchandise exports, million $	
Tea and mate	102.6
Ores and concentrates of base metals, not elsewhere specified	65.3
Coffee and coffee substitutes	47.5

Services Exports, million $	372.6
Services Exports, % of exports of Merch. and Services	55.6
Main services exports, million $	
Transport (2000-2009)	54
Tourism (2000-2009)	174

Demography	
Population, millions	10.7
% of youth population (below age 20)	52.5
Life expectancy at birth (years)	50.6
Adult literacy (age 15+) as %	70.7
Youth literacy (age 15-24) as %	77.2

Labor and finance	
Labor in Agriculture, as %	89.4
FDI inflows, million $	42.3
Remittances, million $	91.8

ICT	2000	2005	2010	Growth Rate (00-10)
Fixed (wired) Internet subscriptions per 100 inhabitants	0.01	0.03	1.43	64.26
Fixed (wired) broadband Internet subscriptions per 100 inhabitants	..	0.01	0.02	..
Fixed telephone lines per 100 inhabitants	0.22	0.26	0.37	5.34
Mobile cellular telephone subscriptions per 100 inhabitants	0.48	2.42	33.4	52.84
Percentage of households with a computer	..	0.2	0.48	..
Percentage of households with a fixed line telephone	1.1	0.8	..	..
Percentage of households with a mobile cellular telephone	..	4.6	..	..
Percentage of households with a radio	35.1	45.8	..	..
Percentage of households with a TV	2.4	2.3	..	..
Percentage of households with electricity	..	4.8	..	..
Percentage of households with Internet access at home	..	0.07	0.13	..
Percentage of individuals using the Internet	0.06	0.56	7.7	62.49
Percentage of the population covered by a mobile cellular network	..	75	..	..

Sources: UNCTAD (UNCTADstat database) World Bank (WDI database), UNDESA (Population Division), UNESCO (UIS database), FAO (FAOSTAT database)

1. Introduction: ICT policy and legal framework in Rwanda

Since 1998, the Government of Rwanda has identified ICTs as a key factor for accelerating socio-economic development and the transition to a knowledge-based economy. It has integrated ICT development in the Vision 2020 and Poverty Reduction Strategy and is investing significantly to develop and deploy ICT infrastructure as well as to train Rwandans in ICTs.

The ICT strategy implementation through the National Information and Communication Infrastructure (NICI) Plans involves the participation of all stakeholders including the implementation steering committee, the project implementers, Rwanda Development Board (RDB), as well as a strong monitoring and evaluation component. The implementation of ICT in Rwanda is driven by the following institutions:

- The Ministry responsible for ICT, which develops ICT policies and ensures sector coordination, as well provides political oversight.
- The Rwanda Development Board (RDB-IT) coordinates and implements national ICT initiatives and programmes in Rwanda.
- Rwanda Utilities Regulatory Agency (RURA), an independent regulatory agency regulates public utilities, including ICT.
- ICT units within Ministries, public service organizations and in districts

As part of the NICI plans implementation strategy, in 2007 the Government initiated the development of a national ICT Bill (the 'Bill'), through a stakeholder consultative process, involving the private sector as well as civil society.

The Bill covers five broad chapters: ICT legislative framework, electronic transactions, information society, broadcasting and postal services. Since its introduction, the Bill has undergone different validation stages. It was endorsed by Cabinet in 2010, and is undergoing review in the National Parliament, where it is expected to be enacted into law in the near future. The Bill will help address existing legal gaps in Rwandan law, as well as repeal some of the existing laws currently governing the ICT sector. However, existing legislation, particularly a 2010 Act, means that Rwanda already has relevant rules in place for many aspects of e-commerce.

2. Status of cyberlaws

The country has historically had a civil law system, but has begun to move towards a common law system in line with harmonization requirements after admission into the East African Community and the Commonwealth.[81] Today, law reforms are initiated at various levels including national institutions, ministries, the Parliament as well as civil society groups. However a proposal has been put forth to set up a national law reform commission that will be in charge of all matters related to law reform.

2.1 eContracting and administration, e-signatures and evidentiary issues

In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic messages according to the Bill. Where an electronic message is used in the formation of a contract, that contract shall be valid regardless of the use of electronic means for that purpose.

In accordance with the Bill, where the law requires a signature of a person, that requirement is met in relation to a data message if:

I. a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

II. that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

In the Bill, Article 18(a) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

An electronic signature is considered to be reliable for the purpose of satisfying the requirements referred in Article 18(a) if:

I. The signature creation data are, within the context in which they are used, linked to the signatory and to no other person

II. The signature creation data were, at the time of signing, under the control of the signatory and of no other person

III. Any alteration to the electronic signature, made after the time of signing, is detectable

Rwanda has in the recent past enacted legislation that admits electronic evidence in national courts of law. Prior to the enactment of this law, electronic evidence was rejected in court proceedings. In accordance to the Law n°18/2010 of 12 May 2010, relating to electronic messages, electronic signatures and electronic transactions ('2010 Act'), Article 6 states:

"In any legal proceedings, the evidential value of an electronic message shall not be denied:

1. on the sole ground that it is an electronic message;
2. on the ground that it is not in its original form, if it is the best evidence that the person adducing it could reasonably obtain.

In assessing the evidential weight of an electronic message, regard shall be placed on the reliability of the manner in which the electronic message was generated, stored or communicated, as well as the reliability of the possibility of its alteration".

2.2 Data protection and privacy

Currently, data protection and privacy provisions are only present in the Telecommunications Law[82] at Chapter XVI. It provides that voice and data communications are confidential and should only be intercepted if authorized. Such authorization can arise if either the user has given explicit consent; if authorized by a court or if required to provide evidence of commercial transactions or business communications. Finally, public telecommunications operators are required to take technical and organizational measures to ensure the security of services and networks.

Reference to 'data privacy protection' is also made in the 2010 Act, in respect to electronic signature certification authorities (Art. 23(3)(f)), although no such rules are currently applicable.

The Bill contains various references to data protection and privacy, in respect of the provision of electronic communication services (Chapter III, Part 11); the provision of domain names and as part of the consumer protection provisions. However, no comprehensive regime is currently proposed.

2.3 Consumer protection

As Rwanda moves progressively towards increased liberalization, certain undesirable business practices have started to emerge which act as a hindrance to development and economic growth. Until recently, the absence of a competition and consumer protection laws has created opportunities for some sectors of the business community to engage in unfair business practices, such as price fixing, speculative hoarding and collusive tendering.

To address such concerns, a competition and consumer protection law has been passed by the National Parliament and is undergoing a promulgation process. For its enforcement, the law also stipulated the establishment of a national Inspectorate and Competition authority, which is yet to be set up.

According to existing law, in the 2010 Act, Chapter 8, Article 57 on Complaints to Consumer Affairs Committee states that: "A consumer may lodge a complaint with the Regulatory Authority in respect of any non-compliance with the provisions of this Law by any supplier".

In Rwanda, dispute resolution has benefited from the establishment of a Commercial High Court. The Bill has also been crafted to address certain consumer protection issues in relation to the provision of utility services, as found in its Information Society Chapter, Section Four; Articles 209-213.

Rwanda Utilities and Regulatory Agency (RURA)[83] does the following in handling a complaint:

1. Once a complaint is received, RURA forwards a copy of the complaint to the utility providing the service, which must respond to RURA within five days.
2. The above act is done with care by RURA and it can use other means to get to the service provider where, in the opinion of RURA, the complainant can suffer possible negative consequences should the concerned utility be directly told the real source of the complaint.
3. RURA thereafter conducts a preliminary inquiry into the complaint. If the complaint in question can be resolved by mediation, it may invite officials of the concerned utility company

and the complainant for a resolution of the complaint.

4. If the parties fail to reach an agreement, RURA will then conduct a formal hearing where both parties will be given the opportunity to state their case before a panel of at least three persons representing RURA.
5. A person appearing before RURA's panel may conduct his own case or be represented by legal counsel or other expert.
6. At the conclusion of the formal hearing, the three-person panel will submit a full report on the decision of the panel with recommendations to RURA's Director General.

Any person or authority dissatisfied with the decision of RURA may go to court for the redress of the matter.

According to the Bill, different measures have been adopted to provide a clear level of protection for consumers in a cyberspace environment when using communication services in accordance to the following principles:

- The provisions of the law shall not be derogated to the detriment of the consumers.
- Where users are not consumers, the provisions shall only apply to the relevant parts of any agreement and only if the contrary has not been agreed.
- Except as provided by the law, a subscriber or other user of an electronic and/or communications network or service shall not be denied a service provided by a licensed operator, or have the service discontinued.

According to the Bill, a licensee shall:

- Make available all electronic communications network and services as may reasonably be provided to any person wishing to subscribe to the network or services;
- Ensure that all rates, charges, practices and classifications are just and reasonable;
- Provide efficient services and comply with the standards for quality as imposed by the Regulatory Authority;
- Notify the Regulatory Authority and publish by notice in the media when the services are to be interrupted for the installation, repair or changing of equipment;
- Establish an efficient mechanism for receiving complaints and repairing failures in the electronic communications network or services;
- Comply with the provisions of this Law and related regulations, directives and the terms and conditions of the license;
- Comply with the terms and conditions of the General Code established by the Regulatory Authority

For communication services, in accordance with the Bill, the powers granted to the Regulatory Authority in Consumer Protection shall ensure the following to protect consumers:

- To supervise compliance with this law and provisions issued under it for the protection and promotion of general interest of the consumers and users of all ICTs and more particularly their economic interest.
- To draft enforceable general codes for the use of, or adaptation by, all licensed networks and services operators. This General Code shall be the basis for all the different Consumer Protection Code or Code of Practice that are used by licensed operators.
- To ensure compliance in the event of the violation of the directives provided for in the general code.

2.4 Copyright

The Rwandan Law n°31/2009 (26 October 2009) enacting intellectual property rights includes extensive provisions on enforcement and provides a range of powers for the judiciary and special tribunals, the police and customs authorities to address IP enforcement. The law also seeks to provide safeguards for third parties in line with the Trade-Related Aspects of Intellectual Property (TRIPS) principles.[84] The promulgation of the new policy and law also coincided with the inauguration of the Commercial Court branch of the High Court of Rwanda under whose jurisdiction IP issues fall. These are particularly important developments for Rwanda. The reason is that, while there are increasing complaints regarding counterfeiting, there is very limited technical and human capacity to address claims of infringement within the police and the customs department.

Within industry, while counterfeiting is cited as a problem, it does not appear to be an extreme. To date, there have been very few cases relating to IP infringement. Since the creation of the Commercial High Court in May 2008, no IP cases have been brought before them. The situation may soon change, however, especially with the new IP law. During the interviews for a needs assessment exercise, the low level of IP cases previously was attributed to the level of damages payable for infringement and lack of awareness. In criminal cases, the lack of testing and detection ability has meant that it is difficult to surmount the requirements of proof in court. Beyond the national concerns, another key concern was the impact of Rwanda's entry into the EAC. Anecdotal evidence suggests that the country is facing increasingly complex cases and that Rwandan exporters have to deal with issues of infringement, particularly with respect to trademarks in other EAC countries.

Another aspect of copyright law in Rwanda has been its focus on the treatment of copyright in libraries, educational and teaching institutions, use by visually impaired and other disabled people, computer programmes, and technological protection measures (TPMs), as well as issues touching on folklore and public domain. For these purposes, libraries, educational institutions, including specialized institutions such as schools for the blind, and the general public have been sensitized to the permissible uses of copyrighted works to encourage and support education, including cultural education, and entrepreneurship.

In terms of software protection, the IP Law provides that the reproduction of a single copy is permitted for use with a computer for the purpose and extent for which the programme has been obtained, for archival purposes and for the replacement of the lawfully owned copy. This exception for reproduction also applies for adaptation of computer programmes in a similar manner. Temporary reproduction is also permitted where it is made in the process of a digital transmission of the work or an act of making a digitally stored work perceptible, or such use is caused by an authorized person or person making use of the personal use exception and where temporary reproduction is an accessory to transmission or making perceptible the protected work.

The IP Law prohibits circumventing Technological Protection Mechanisms (TPMs), or to produce, import, distribute, sell, rent, advertise for sale or rental, or possess devices, products, components or services for commercial purposes that are promoted, advertised or marketed for the purpose of circumventing TPMs. These provisions will have to be enforced in a balanced manner taking into account the policy objectives related to access to technology, technological learning and skills upgrading and access to IP-based essential products.

2.5 Domain name management

In accordance with the Bill, the regulatory authority RURA may, upon application in the prescribed manner and subject to such conditions as it may deem necessary, grant licences under any prescribed regulation-authorizing persons, whether of a specified class or any particular person, to administer a sub-domain in the country code Top-Level Domain.

Express provision is made for potential disputes, empowering the Authority to establish an alternative dispute resolution scheme in respect of the .rw domain name space:

a) The regulations shall be made with due regard to existing international practices.

b) The regulations may prescribe:

- the procedures for resolution of certain types of disputes determined in the regulations and which relate to a domain name registration;
- the role which the Authority must fulfil in administering the dispute resolution procedure;
- the appointment, role and function of dispute resolution adjudicators;
- the procedure and rules which must be followed in adjudicating disputes;
- the measures to prevent unlawful actions or activities with respect to domain names;
- the manner, costs of and time within which a determination must be made;
- the implementation of determinations made based on the dispute resolution procedure;
- the limitation of liability of registrars and registries for implementing a determination; and
- the enforcement and publication of determinations.

2.6 Cybercrime and cybersecurity

According to the 2010 Act, various forms of conduct threatening the integrity, confidentiality and availability of computers and the data they process are criminalized. In Chapter 6, the following conduct gives rise to an offence: 'unauthorised access to and interception of computer service' (Article 60); 'unauthorised modification of computer data' (Article 61); 'damaging or denying access to computer system' (Article 62); 'unlawful possession of computer system, devices and data' (Article 63) and 'unauthorised disclosure of password' (Article 64).

Cybersecurity is at the core of a knowledge-based society and as such is considered a national priority. It ensures trustworthy management of all deployed ICT assets that support all facets of Rwanda's ICT goals. To fully realize ICT benefits, there must be full confidence that all information and communication is secure and can be recovered.

The scope of the cybersecurity in the Rwandan policy context is three-fold. First is to increase the level of cybersecurity awareness and protect key ICT assets against attacks. Second is to build local capabilities to respond to attacks as well as foster international cooperation on cybersecurity. Third is to create a legal and regulatory environment to mitigate cyber vulnerabilities.

Rwanda's ICT infrastructure demands that every Rwandan participate in safeguarding it. Cyberattacks can come in the form of virus-infested hardware or casual access to malicious sites, which could cause serious harm to the country's critical infrastructure. Therefore, to fully safeguard ICT infrastructure assets, it is recognized that all Rwandans need to be made aware about ICT security, which requires due diligence.

Current Policy interventions on cybersecurity in Rwanda include the following:

- ***Build cybersecurity capabilities:*** Building appropriate cybersecurity capabilities is critical to ensuring that Rwanda possesses adequate and relevant capacity to counter any attacks. While the ICT infrastructure is protected by in-built state-of-the-art security technology and solutions, it is extremely important that Rwanda builds national capacity to safeguard its ICT assets, as in-built protection is not sufficient and sustainable.
- ***Protect Rwanda's infrastructure and systems from cyberattacks:*** Rwanda built state-of-the-art ICT infrastructure during NICI II. However, the threats of cyberattacks against the country are of grave concern and pose real and credible threats to ICT assets. Therefore, it is imperative that there is adequate planning to ensure that mechanisms are in place to counter or mitigate future threats.
- ***Foster national and international cooperation to handle cybercrimes and threats:*** Cyberattacks are increasingly global in nature and, as such, it is no longer feasible or appropriate to simply handle them at a national level. Therefore, global cooperation and collaboration to safeguard interdependent infrastructure and mitigate the effects of cyberattacks are increasingly necessary.

2.7 Content control

The government of Rwanda does not dictate content in broadcasting and other transmission forms; instead plurality of content is encouraged. The Media High Council was established in 2002[85] and encourages and promotes the development of local content as well as monitoring both technical and non-technical content, including media over the Internet.[86]

With the Government mindful of its responsibility to foster the development of the local culture and entertainment industry and help local artists, the regulators, where applicable, enter into dialogue with the content providers for the promotion and development of local content. The local and sub-regional content in all fields, including culture, is starting to develop the resilience for the tough competitive environment of the modern digitalized world. The Government recognizes the importance of providing significant opportunities for the development of local content of national value and culture. The Broadcasting Content Policy recognizes the primacy of parental guidance and supervision in the use of the Internet by children. The Government ensures easy availability of software and hardware tools to assist parents in the supervision of their children.

The 2010 Act, at Chapter III, provides immunity from liability for communication service providers and intermediaries for third-party content either made accessible through the service (Articles 8 and 10), where the provider does not have control

over the content; where the content is cached on an 'automatic, intermediate and temporary' basis (Article 11); where the content is stored, but the intermediary is unaware of such content and takes it down expeditiously upon notice (Article 12) or where it provides information location tools, but is unaware of such content, receives no financial benefit directly attributable to the infringing material and takes it down within a reasonable time upon notification (Article 13).

2.8 Internet and mobile payment systems

Some of the relevant financial legislation that influence the operations of Mobile Money system within Rwanda include:

- Law no. 55 (enacted November 2007)[87] governs the mandate of the National Bank of Rwanda (BNR), the Central Bank that oversees the financial sector in Rwanda;
- Law no. 7 (enacted April 2008)[88] defines the organization of the banking sector and explicitly prohibits any entity engaging in banking activities without prior licensing by BNR;
- Law no. 40 (enacted August 2008)[89] regulates the activities of microfinance institutions within Rwanda;
- The AML/CFT Law no. 47 (enacted 2008)[90] provides for the establishment of a Financial Investigation Unit (FIU), to which the BNR, banks and other financial institutions report suspicious transactions;
- Regulation no. 03 (enacted April 2011)[91] stipulates pecuniary sanctions for licensed banks that violate regulations, instructions and decisions of the BNR;
- Regulation no. 04 (enacted April 2011)[92] defines a minimum set of requirements that banks in Rwanda need to meet to ensure effective business continuity practices and other regulations with the potential to influence the conduct of Mobile Money operations within Rwanda.

The new law under the auspices of the Ministry of Trade and Industry will repeal an older regulation that is currently used to enforce competition policy across different sectors, Law no. 41/63 (enacted February 1950). It will also provide coherent consumer protection mechanisms that span different sectors as opposed to the sector-led efforts under the auspices of different regulators.

D. THE UNITED REPUBLIC OF TANZANIA IN BRIEF

Economy	2010
GDP current prices, million $	18'372.2
GDP per capita	550
Real GDP growth %	5.2
GNI, million $	16'552.8
GNI per capita	500

Trade	
Merchandise Exports, million $	2'164.0
Merchandise Exports, % of exports of Merch. and Services	62.3
Main merchandise exports, million $	
Coffee and coffee substitutes	407.4
Fish, fresh (live or dead), chilled or frozen	153.8
Tobacco, unmanufactured; tobacco refuse	115.3
Services Exports, million $	1'310.1
Services Exports, % of exports of Merch. and Services	37.7
Main services exports, million $	
Tourism	729.9
Government services not indicated elsewhere	326.5

Demography	
Population, millions	33.5
% of youth population (below age 20)	59.2
Life expectancy at birth (years)	53.4
Adult literacy (age 15+) as %	71.4
Youth literacy (age 15-24) as %	84.1

Labor and finance	
Labor in Agriculture, as %	74.8
FDI inflows, million $	847.6
Remittances, million $	914.5

ICT	2000	2005	2010	Growth Rate (00-10)
Fixed (wired) Internet subscriptions per 100 inhabitants	0.03	0.24	1.09	43.23
Fixed (wired) broadband Internet subscriptions per 100 inhabitants	..	0	0.01	..
Fixed telephone lines per 100 inhabitants	0.51	0.4	0.39	-2.65
Mobile cellular telephone subscriptions per 100 inhabitants	0.32	7.63	46.8	64.63
Percentage of fixed telephone lines in urban areas	49	..	..	..
Percentage of fixed telephone lines which are residential	60	64	..	..
Percentage of households with a computer	..	2.1	2.62	..
Percentage of households with a radio	47.5	58.4	..	..
Percentage of households with a TV	2.8	6.1	..	..
Percentage of households with electricity	8.6	11.4	..	..
Percentage of households with Internet access at home	..	0.45	0.74	..
Percentage of individuals using the Internet	0.12	4.3	11	57.12
Percentage of the population covered by a mobile cellular network	..	45	..	..

Sources: UNCTAD (UNCTADstat database) World Bank (WDI database), UNDESA (Population Division), UNESCO (UIS database), FAO (FAOSTAT database)

1. Introduction: ICT policy and legal framework in the United Republic of Tanzania

The ICT Policy in the United Republic of Tanzania ('Tanzania') highlights the increasingly rapid development of ICT applications over the world, boosting the economies of some countries while changing the society's behaviour.[93] The United Republic of Tanzania Development Vision 2025 articulated ten main focus areas in harnessing ICT, which include strategic ICT leadership; ICT infrastructure; ICT Industry; Human Capital; Legal and Regulatory Framework; Productive Sectors; Service Sectors; Public Service; Local Content; and Universal Access.[94]

The Government adopted a National ICT Policy in 2003. It reflects national goals, objectives and aspirations as expressed in Vision 2025, setting out digital opportunities that the United Republic of Tanzania can exploit towards meeting the Vision 2025

The National ICT Policy's broad objectives are to:[95]

1. Provide a national framework that will enable ICT to contribute to achieving national development goals.
2. Establish an enabling legal framework, aligned with the United Republic of Tanzania's constitutional provisions, legislative and regulatory environment, and consistent with regional and global best practice.
3. Ensure that the United Republic of Tanzania does not become a haven of cybercrime.
4. Transform the United Republic of Tanzania into a knowledge-based society through the application of ICT.

2. Status of cyberlaws

No specific legal framework exists in the United Republic of Tanzania that addresses challenges and other issues brought by ICTs. Most existing laws were designed to facilitate paper-based transactions that are not attuned to technological changes with legal rules that require the use of documents, written notices and manuscript signatures. Most laws that deal with contracts provide for certain legal requirements that might only apply in the physical world environment. For instance, where contracts are concerned, there are usually three different types of formalities that may be required: writing, signature and some kind of third party authentication or involvement such as notarial execution. Most written contracts contain a standard clause that states that no amendments to the contract will be valid or binding unless reduced to writing and signed by both parties, which makes the use of those formalities mandatory.

The process of formulating cyberlaws in the United Republic of Tanzania goes back 2003 when the national ICT Policy was adopted. In 2006 the Law Reform Commission made a study of existing laws to identify gaps that needed reforms to take on-board issues related to ICTs.[96] The reforms were also influenced by some cybercrime cases. The process was driven largely by the need to make the law responsive to the changing needs of society. Following the Commission Report in 2007, The Evidence Act was amended. In 2009, the Tanzanian Communications Regulatory Authority (TCRA) initiated legal reforms to facilitate electronic communications that resulted into the enactment of The Electronic and Postal Communications Act (EPOCA) in 2010.

2.1 e-contracting and administration, e-signatures and evidentiary issues

The United Republic of Tanzania has a number of laws that regulate contracts and other related agreements. These laws, such the Law of Contract Act[97] and the Sale of Goods Act,[98] have no provisions for the use of electronic contracts and other related electronic transactions. Like other countries, laws in the United Republic of Tanzania were developed over a long period during which physical actors and physical media were the only, or at least the primary, mechanisms by which transaction with legal consequences could be effected.[99] The basic Commercial laws and Civil laws in the United Republic of Tanzania are derived from 19th century, mainly paper-based, methods of transactions. The laws and regulations were designed to facilitate paper-based transactions that are not in line with the current advanced technological changes, with legal rules that require the use of documents, written notices and manuscript signatures. Most laws, such as civil laws and contract laws that regulate transactions, require an agreement to be evidenced in writing and signed by the person who is to be bound by it. The general position of Common Law

is that where the communication is made by post, the contract goes into effect on the date the letter of acceptance is posted. That is, when an offer made by one party is accepted unconditionally by the other. This rule is equally found in the United Republic of Tanzania under the principal law, which governs most contracts.[100]

Most laws that deal with contracts provide for certain legal requirements that might only apply in the physical environment. These requirements were made purposely for authenticating and evidencing the transactions between the parties in the physical world. Like other Common law countries there are also considerable numbers of traditional statutory rules and principles in the United Republic of Tanzania about particular types of contract, requiring them to be made or evidenced in a particular way. Requirements not in line with electronic contracts and communications under e-commerce can be briefly categorized as follows:

1. The contract must be under seal. This is a legal requirement for a valid contract (ref. relevant provision(s)).
2. The contract must be in writing.
3. The contract must be evidenced in writing and signed before the witness.

The legal concepts of writing and signatures under the current laws do not involve data message. It is difficult for both parties entering into contract to use other parties to witness their transactions in cyberspace.

The development of e-commerce and e-government, specifically the communication of legally significant information in the form of data, are likely to be hindered by obstacles or uncertainty about the legal effect or validity of using such data messages. The current legislation governing transactions and communications including storage of information is inadequate and outdated, as it does not reflect or contemplate the use of e-commerce and the implementation of e-government.

The United Republic of Tanzania has not signed nor ratified the United Nations Convention on the Use of Electronic Communications in International Contracts, 2005, which addresses e-contracts and other related e-transactions at the cross-border level.

An electronic signature, which is generated using ICTs, is a new area that is not regulated by any law in the United Republic of Tanzania. A number of statutes require the use of handwritten or manuscript signatures and writing for legal validity of certain transactions and authentication of e-documents. These statutes include the Law of Contract Act, the Sale of Goods Act (CAP 214), the Civil Procedure Act, the Law of Evidence Act (CAP 6, 1967) and other laws. Authentication by signature is a bigger problem in this era of digital technology. In most jurisdictions like in the United Republic of Tanzania the requirement of signature is only met if a physical signature is affixed to a paper document. The so-called electronic signatures do not satisfy these legal requirements unless specific provision for electronic authentication has been made.

The laws in the United Republic of Tanzania cover neither on-line transactions nor digital signatures. Most laws still maintain the manuscript signatures as a means of authentication of documents and identifying parties, creating a discriminatory approach to e-signatures and data messages or alternatives to paper-based methods under e-commerce. A good example is the Bills of Exchange Act of the United Republic of Tanzania[101] whereby a signature is essential to liability. The definition of signature under the law does not include electronic signature.

The regional EAC Cyberlaw Framework adopted in 2011 makes it even more urgent for the country to prepare and adopt an effective legal framework for e-signatures in order to enable and facilitate the use of electronic signatures and provide equal treatment to users of paper-based documentation and users of computer-based information.

The main law that regulates evidence in the United Republic of Tanzania is the Law of Evidence Act, which was enacted before the development of digital technology. Most laws related to business, civil matters and evidence were made to suit the physical world through the use of paper-based methods, and advocate for the mandatory requirement of original evidence or the computer-derived evidence in certain circumstances. Section 76 of the Evidence Act was amended by this legislation by adding after the word "Bankers books" to include: "*data message or kept on information systems including, but not limited to, computers and storage devices, magnetic tape, microfilm, video or computer display screen or any other form of mechanical or electronic data retrieval mechanism*"

(emphasis added)[102]. The new amendment law has further brought fundamental changes as far as the legal status and admissibility of electronic records are concerned. This can be observed under the additional section of the new Act to the Evidence Act whereby electronic records or data messages are given legal status and can be admissible as evidence before the court.

Arguably, one could say that the Written Laws (Miscellaneous Amendments) Act, 2007 has not really resolved the problem of legal certainty and admissibility of electronic evidence.

This law only applies to electronic evidence from banking transactions and admissibility of such evidence under criminal proceedings. The provision of the new law reads as follows: so-called "best evidence rule" that qualify for admissibility in the court in case of dispute settlements and court procedures.[103] The 'best evidence' rule gives evidential preference to original documents that can be admissible in the court of laws.

Under the Evidence Act[104] the best evidence rule excluded the admissibility of secondary evidence unless corroborated by the primary evidence. However in 2007 the Government of the United Republic of Tanzania passed the Written Laws (Miscellaneous Amendments) Act, which amends the Evidence Act, 1967.[105] This law seems to allow the admissibility of:

40A In any criminal proceeding:

a) Information retrieved from computer systems, networks or services

b) Records obtained through surveillance of means of preservation of information including facsimile machine, electronic transmission and communications facilities

c) Audio or video recording of acts or behaviours or conversation of persons charged shall be admissible in evidence[106]

It might be difficult to apply such evidence where the only available evidence to be applied in cases related to civil and other related cases or proceedings is e-evidence. The question of proof of the integrity of the electronic records or e-evidence has also not been considered. Before the amendment of the Evidence Act, the Judiciary tested the admissibility of electronic evidence, in the landmark case of *Trust Bank Ltd. v. Le-marsh Enterprises Ltd., Joseph Mbui Magari, Lawrence Macharia,*[107] which seem to beneficially erode the best evidence rule admitting computer printout and other related e-evidence under The Evidence Act (CAP 6 R.E 2002).

The key issue before the court was whether electronic evidence from a computer printout was admissible before the court under the Evidence Act, 1967. Reading from the provision of the Evidence Act, 1967, the court noted that the electronic evidence was not admissible. However the court, under Hon. Justice Nsekela as he then was, consulted various common law cases and statutes and departed from the best evidence rule under the Evidence Act by accepting electronic evidence as admissible in the Courts in the United Republic of Tanzania. This decision of the High Court has never been challenged and influenced the amendment of the Evidence Act in 2007.

Other Laws were amended to accommodate electronic evidence including the Customs Duties Act, The Excise Management & Tariff Act, 1954 Cap 147 and The Airport Service Charge Act, Cap 365.

2.2 Data protection and privacy

Data protection and privacy are among the key areas under cybersecurity raising concerns and challenges. The threats that the use of data processing techniques pose to the freedoms of individuals whose personal data are subject to automated processing may give rise to more legal concerns about the misuse of information. As part of cybersecurity, legislation on data protection and privacy needs to be in line with legislation on cybercrimes. In the United Republic of Tanzania there is no legal framework to regulate and protect individual data and government information that are stored and flow electronically. The lack of legal framework on data protection and e-security makes the free flow of personal data and confidential information unsafe. Hacking and unauthorized interference with computer systems can cause great concern about cybersecurity. E-banking also raises legal issues regarding the questions of privacy and security.

Creating a legal framework to address issues related to cybersecurity, privacy and trust will improve the e-security and privacy of individuals, enterprises, governments and the entire cyberspace, which

will therefore encourage people to accept and rely on such technologies. The security risk might cause banks and other related financial institutions to lose gain and hope of e-banking if the legal issues and problems are not properly addressed through policies and effective legal framework. The Electronic and Postal Communications Act (EPOCA), 2010 provides for data protection for electronic communication. This law has addressed some of the issues related to cybersecurity such as cybercrimes, data protection, e-privacy and children's protection online. Some of the offences relating to electronic communications, offences and penalties relating to SIM cards are dealt with under sections 125-137. Furthermore, Section 124 (3) stipulates an offence for unauthorized access or use of computer system.

The law allows regulation of Computer Emergency Response Teams (CERTs) and other issues to be developed (Section 124).

However, the law is not exhaustive: it considers issues arising from communications only, while key elements of cybercrimes and principles of data protection are not adequately addressed. In the absence of specific laws to address cybercrimes, data protection and privacy there is no highly assured security against fraud, theft and other related cyber-offences, given the lack of legal framework that regulates this area.

2.3 Consumer protection

Consumer protection in the United Republic of Tanzania is addressed and regulated by various off-line laws. The laws governing consumers, such as the Fair Competition Act, 2003, primarily protect consumers who are in most cases involved in an off-line business only and hardly apply to the on-line business transactions, such as distance contracts. Consumers are not confident of the security and identity of the sender or recipient, especially when using credit cards details on the Internet, because of the fear that they might be intercepted and fraudulently misused. While the development of e-commerce has been generally viewed as beneficial to consumers since it offers wider choices and more competitive prices, there are also concerns about the vulnerability of consumers to unscrupulous traders operating at a distance, often from a foreign jurisdiction.[108]

No law protects consumers against risks involved in selling and buying goods and services on-line due to the fact that these laws were passed when the online or distance contracts did not exist in the United Republic of Tanzania. The United Republic of Tanzania, and the East African Community in general, need to enact consumer protection laws that will specifically regulate distance selling and will equally apply to contracts entered into via the Internet.

2.4 Copyright

One area in e-commerce that might cause many problems is trading on-line in goods and services involving intellectual property rights (IPRs).[109] The impact of digital technology can also be observed in intellectual property rights specifically copyright, trademarks and domain names. While technology has facilitated access to and infringement of copyrighted works on-line, the introduction of Internet domain names has threatened trademarks owners, creating illegal activities known as cyber-squatting. Copyright became most important area of intellectual property that protects software such as computer programmes, database and other related forms of electronic information. Most things seen on a computer display (generated by software) are protected by copyright, trademark and related rights. The growth of the Internet has had major implications for the treatment and protection of copyright materials and other related intellectual property rights that are published electronically. Technological developments have made copyright material easier to access and reproduce, and more difficult to protect.

Most intellectual property laws have not been reviewed and reformed to cope with technological developments. More specifically copyright law such as Copyright and Neighbouring Rights Act faces challenges in keeping pace with changes in technology. The Copyright and Neighbouring Act of the United Republic of Tanzania, which came into operation in 1999, seemed to be passed soon after the enactment of the US Digital Millennium Copyright Act (DMCA), which was passed in 1998. One would expect Copyright law to take into account some of the provisions of the US DMCA, which had the main goal of updating US copyright laws with an eye toward making them more relevant and flexible given the ever-changing

digital information climate.

Works that are eligible for copyrights in the United Republic of Tanzania are provided under Sections 5 to 23 of the Copyright and Neighbouring Rights Act.[110] While literal and non-literal copying of computer programme might amount to copyright infringement in other jurisdictions, the Copyright and Neighbouring Act seems to be silent on this form of electronic infringement. The current legal framework might not be useful in the fight against online piracy of IP rights. The United Republic of Tanzania has neither signed nor ratified the Berne Convention or the WIPO Copyright Treaty (1996) and the WIPO Performances and Phonograms Treaty (1996).

2.5 Domain name management

The development of technology with the evolution of e-commerce related to the sale of goods and services online has brought a new dimension of trade and service mark law and practice, where traders or companies have opted to use "e-trademarks" – namely domain names. Domain names have been successfully used as the best way for business companies to identify themselves and establish their presence in cyberspace. Most countries such as the United Republic of Tanzania lack an adequate legal framework to safeguard aggrieved parties where individuals register company names as their domain names for extortion purposes. The current legal framework (Trade Marks Act and Merchandise Marks Act) that protects trademarks and service marks and other related matters do not address the rise and use of domain names. It is difficult to enforce these laws in the area of domain names because they deal with tangible products and the registration of domain names is in the hands of the private sector. The problem seems to be as hot as counterfeit and pirating, whereby cybersquatters register known domain names as country codes by the United Republic of Tanzania Network Information Centre (tzNIC). The dispute resolution of domain names is conducted by the tzNIC. Policy and Rules for Uniform Domain Name Dispute Resolution have been developed and are implemented by tzNIC, supported by the TCRA.

Any person or entity may initiate an administrative proceeding by submitting a complaint to tzNIC in accordance with the Policy, and these Rules to the Policy Advisory Committee (PAC)(a). The tzNIC PAC shall review the complaint for administrative compliance with the Policy and these Rules and, if in compliance, shall forward the complaint to the Respondent in the manner prescribed by the Rules within three (3) calendar days following receipt of the fees to be paid by the Complainant. The Panel shall determine the admissibility, relevance, materiality and weight of the evidence. Furthermore, the PAC shall decide on a request by a Party to consolidate multiple domain name disputes in accordance with the Policy and Rules. In all cases, the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case. Additionally, a Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable. In the case of a three-member Panel, the Panel's decision shall be made by a majority. In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.[111]

2.6 Cybercrime and cybersecurity

The revolution in ICTs has changed fundamentally the way information is processed and stored. Furthermore, the development and use of ICTs have facilitated the commission of traditional crimes resulting into electronic crimes while introducing new types of cyber offences. Like any other country, the United Republic of Tanzania might face the same e-challenges in combating cybercrimes and other related e-crimes. Technical and legal challenges are posed by the development of digital technology and Internet.

Most crimes in the United Republic of Tanzania are regulated by laws such as the Criminal Procedure Act Cap 20 [R.E.2002](Procedural law). Other relevant laws include substantive laws, such as the Penal Code (Cap 16 [R.E.2002]), the Extradition Act (Cap 368 [R.E.2002]) and other related laws. However, most of these laws are outdated and do not take into account the development of technology that is always changing very rapidly. The new harmful conducts facilitated by the development of ICTs, such as denial-of-service attacks, are not addressed

by the criminal laws in the United Republic of Tanzania, which can hinder the development of e-commerce. There is a great likelihood for culprits to evade their criminal responsibility under the current provisions of laws. In 2010, the Electronic and Postal Communications Act (EPOCA) was enacted. Although this law provides for a few cybercrime offences and electronic content regulation, it is not useful in fighting cybercrimes.

The Police Department has introduced a cybercrime unit which up until 2010 investigated and prosecuted more than 270 cybercrimes cases.[112]

Like all African countries, the United Republic of Tanzania is not a signatory to the Council of Europe Convention on Cybercrime, 2001.

2.7 Content control

The question of controlling and regulating content has been a great debate and of concern in the United Republic of Tanzania due to the development of digital technology. The key concern is how to protect children online from harmful content such as pornography and other adverse, problematic materials. No specific law regulates online content. However there are some legal provisions found under the Regulations such as the Broadcasting (Content) Regulations 2005.[113] The Electronic and Postal Communication Act[114] provides some provisions on content regulation and control. For instance section 104, which provides for the Code of conduct for content services licensees states that:

104 (1) The code of conduct contemplated in this section shall prohibit the provision of content which is indecent, obscene, false, menacing or otherwise offensive in character.

The law under section 104 (2) further provides that without derogating from the generality of subsection 1(b), the code of conduct shall be designed to achieve the following objectives:

(a) the protection of children;

(b) the exclusion of material likely to encourage or incite the commission of crime, from content provided by content service licensees.

E. UGANDA IN BRIEF

Economy	2010
GDP current prices, million $	18'372.2
GDP per capita	550
Real GDP growth %	5.2
GNI, million $	16'552.8
GNI per capita	500

Trade	
Merchandise Exports, million $	2'164.0
Merchandise Exports, % of exports of Merch. and Services	62.3
Main merchandise exports	
Coffee and coffee substitutes	407.4
Fish, fresh (live or dead), chilled or frozen	153.8
Tobacco, unmanufactured; tobacco refuse	115.3

Services Exports, million $	1'310.1
Services Exports, % of exports of Merch. and Services	37.7
Main services exports	
Tourism	729.9
Government services not indicated elsewhere	326.5

Demography	
Population, millions	33.5
% of youth population (below age 20)	59.2
Life expectancy at birth (years)	53.4
Adult literacy (age 15+) as %	71.4
Youth literacy (age 15-24) as %	84.1

ICT	2000	2005	2010	Growth Rate (00-10)
Fixed (wired) Internet subscriptions per 100 inhabitants	0.02	0.03	0.09	16.23
Fixed (wired) broadband Internet subscriptions per 100 inhabitants	..	0	0.06	..
Fixed telephone lines per 100 inhabitants	0.25	0.31	0.98	14.64
Mobile cellular telephone subscriptions per 100 inhabitants	0.52	4.63	38.38	53.75
Percentage of fixed telephone lines in urban areas	..	92	..	..
Percentage of fixed telephone lines which are residential	35	..	..	..
Percentage of households with a computer	..	0.8	2.12	..
Percentage of households with a fixed line telephone	..	0.5	..	..
Percentage of households with a mobile cellular telephone	..	10.1	..	..
Percentage of households with a radio	..	59.8	..	..
Percentage of households with a TV	..	6	..	..
Percentage of households with electricity	..	8.9	..	..
Percentage of households with Internet access at home	..	0.08	0.37	..
Percentage of individuals using the Internet	0.16	1.74	12.5	54.62
Percentage of the population covered by a mobile cellular network	16.05	70	..	..

Sources: UNCTAD (UNCTADstat database) World Bank (WDI database), UNDESA (Population Division), UNESCO (UIS database), FAO (FAOSTAT database)

1. Introduction: ICT policy and legal framework in Uganda

In 2003, the Government of Uganda established an ICT Policy to provide a framework for the systematic development of the ICT sector in Uganda. The ICT Policy focuses on three major areas namely[115] :

(a) ICT as a resource for development;

(b) Mechanisms for accessing information and

(c) ICT as an industry, including e-business, software development and manufacturing.

The Policy also earmarks e-commerce and ICT-based services among the eight priority areas for export development, particularly through the Smart Strategic Partnership programme between the Government of Uganda, private investors and development partners.

The ICT policy was issued in the wake of other policies like trade liberalization, financial sector reform, privatization of public enterprises and programmes on alleviation of poverty, which had underpinned the economic growth of the country. Due to the significant leaps in the growth of ICT infrastructure and services since 1996, the ICT Policy was seen as a means of strategically harnessing the opportunities and potential provided by ICT. Indeed the sector is looked at as a great opportunity for attracting investment in the country.[116]

The ICT sector is spearheaded by the Ministry of Information and Communications Technology, which is responsible for setting the policies to guide the sector and to oversee the sector on behalf of the Government, the Uganda Communications Commission, the independent regulatory body, and the National Information Technology Authority.[117]

While the Uganda Communications Act and the Electronic Media Act have been in place since 1996,[118] the two laws regulate the telecommunications and broadcasting subsectors without much emphasis on the cyberworld. A new Bill, the Uganda Communications Regulatory Authority Bill was introduced in March 2012 to provide for convergence of the broadcasting and telecommunications subsectors.

With the advent of communications technology in Uganda and due to the steady growth in the infrastructure and services provided over the electronic or ICT platform, there was a need to reform the existing legal regime to cater to the advances in technology that were taking place globally and within the country, and to provide a conducive legal regime for the implementation of the ICT Policy.

2. Status of cyberlaws

The process of formulating cyberlaws in Uganda was initiated in 2003 when a national taskforce led by the Uganda Law Reform Commission was set up to undertake the exercise.[119]

The formulation and development of cyberlaws was part of a wider reform of the commercial justice system in Uganda that started in 2000.[120] The process was undertaken largely to make the law responsive to the changing needs of society.

In establishing the national taskforce, the Government of Uganda recognized that developments in ICT have dramatically changed the way information is collected, stored, processed, disseminated and used, thus making it the most powerful tool for doing business, and for modernization and development.[121]

The process of formulating and developing laws relating to ICT was protracted since it involved reviewing the existing legal regime in order to design a legal framework that promotes and supports the ICT policy, while at the same time being cognizant of major cross cutting issues like privacy, security and intellectual property rights and not unduly restricting public access to information. Since ICT was also a relatively new and developing area, it was critical that as many interested parties or stakeholders were consulted on the nature and suitability of the proposed legal framework.[122]

This process was further complicated by the complexity of the subject matter of the proposed legislation. At every stage of the consultative or law making process, it was necessary that the concept of transmission of information over the electronic medium was explained as simply as possible before any consultation could take place. In most cases, the consultative sessions became sessions on creating awareness about the use of computers and related technology rather than sessions on collecting views and ideas on how best to regulate ICT use.

In addition, when the process of developing a regulatory framework began in 2000, it was

promoted by a section in the Ministry of Works, Transport and Communications until the Ministry of ICT was created in 2006 to specifically spearhead and promote the use of ICT in the country.

So, although the process for reforming the law and formulating a cyberlegal framework started in 2003, the laws were not enacted by Parliament until the beginning of 2011.

In 2004, after initial consultations, the Uganda Law Reform Commission proposed three Bills to address the issues related to ICT in Uganda.[123] The Electronic Transactions Bill, the Electronic Signatures Bill and the Computer Misuse Bill. These Bills were subjected to further scrutiny and consultation between 2004 and 2011, when they were eventually passed.

The Electronic Transactions Act, 2011, the Electronic Signatures Act, 2011 and the Computer Misuse Act, 2011 now form the backbone of the legal framework for e-commerce, electronic transactions and computer- or ICT-related communication in Uganda. The three laws became effective on 15th April 2011.[124]

The Electronic Transactions Act, 2011 provides for the use, validity, security, facilitation and regulation of electronic communications and transactions and encourages the use of e-Government services. The objective of the Act is to remove the legal and operational barriers to electronic transactions by facilitating the use of electronic communications and applying existing legislation to electronic communications.

The Act in effect gives a functional equivalent of electronic communications or transactions to the traditional paper-based communications or transactions. Whatever can be done in the traditional physical paper environment can now be done electronically.[125]

The Electronic Signatures Act, 2011 provides for the regulation and use of electronic signatures, determination of minimum requirements for functional equivalence of electronic signatures, modernization and harmonization of the laws relating to computer generated evidence and amendments of the current laws to provide for admissibility and evidential weight of electronic communications.

The Computer Misuse Act, 2011 provides for the safety and security of electronic transactions and information systems, the prevention of unlawful access, abuse or misuse of information systems including computers and for securing the conduct of electronic transactions in a trustworthy electronic environment.

The Electronic Transactions Act, the Electronic Signatures Act and the Computer Misuse Act reflect international best practice in the field of electronic commerce and electronic signatures since they are largely based on UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures and also take into account the provisions of the United Nations Convention on the Use of Electronic Communications in International Contracts.

2.1 eContracting and administration, e-signatures and evidentiary issues

Electronic transactions including contracts are now given legal validity by the Electronic Transactions Act, 2011. Section 14(1) provides that a contract shall not be denied legal effect merely because it is concluded by means of a data message.[126]

Indeed whereas section 3 of the Contract Act[127] and section 5 of the Sale of Goods Act[128] require that certain contracts are not enforceable unless they are in writing and signed, section 5(3) of the Electronic Transactions Act, 2011 now provides that this requirement is met if the document or information is in electronic form.

In addition, section 14(1), section 5(1) provides that information shall not be denied legal effect or validity or enforcement solely on the ground that it is in the form of a data message. It follows that once the general principles of contract are established, a person or court relying on this section cannot disregard information (in the form of a data message) when determining whether a contractual relationship exists between the parties.

According to the Act, a contract may be entered into by performing any act required by law to form a contract.[129] The acts referred to here are the offer, acceptance and the related requirements for a contract to be concluded. Section 5(2) of the Act provides that information incorporated into a contract that is not in the public domain is regarded as incorporated in a data message if it is referred to in a way that a reasonable person would notice the reference to the incorporation in the contract.

A necessary safeguard in this regard is where there is an error in sending a data message between the contracting parties. Section 13(4) provides that the relationship between the parties does not amount to a contract where the parties are using an automated system and the computer makes a material error that is conveyed to the other party and an opportunity is offered to the other party to rectify the error. However, the Act does not define what a 'material' error is, so this will need to be determined by a court, in the specific circumstances, for the purposes of invoking the protection under section 13(4).[130]

Time and place have been compressed by the borderless environment characterized by the nature of the Internet and other ICT services; thus it is necessary to determine with certainty the time and place with respect to conclusion of an e-contract or a contract concluded in electronic form. In this regard, section 14(2) of the Act provides that a contract by means of a data message is concluded at the time when and the place where the acceptance of the offer is received by the person making the offer.

In 2007, before the Electronic Transactions Act was enacted, the Commercial Division of the High Court of Uganda was called upon to determine a contractual dispute by examining electronic messages sent via email as a basis for establishing a contractual relationship between parties. *In Hansa & Lloyds Ltd, Emmanuel Onyango v Aya Investments Ltd, Mohammad Hamid*[131] the dispute related to whether there was a contract between the parties, since there was no signed contract in the traditional paper-based environment sense. The Court relied on the emails exchanged between the parties to determine that there was a "course of dealings" and therefore a contract between the parties. In this case the court did not have to verify the integrity of the electronic messages since the emails were not disputed.

The Electronic Transactions Act 2011 therefore gives legal certainty in respect of the validity, legal effect and enforceability of information in electronic form with respect to relations between parties, especially establishing contractual relationships.

Many of the laws in Uganda were enacted to suit a paper-based environment. Indeed most of them require documents or information to be "written", "filed", "delivered", "signed" or "registered".[132] With respect to correspondence and communication within the public service and Government, until 2010, the law did not recognize electronic communication.[133]

The Electronic Transactions Act, 2011 promotes the use of e-government services. To this end the Act provides that a public body may accept, register, file or issue a document in electronic form.[134] This departure from the traditional paper-based correspondence, communication and delivery of public services is now recognized by new Government Standing Orders. Indeed it is now possible to communicate by email, Internet, video and teleconferencing.[135]

As in other electronic communications, a major concern is whether the information can be kept confidential or secret, especially where this is required by law.[136] A public body may take comfort in section 23 of the Electronic Transactions Act, 2011 which allows each public body to specify the manner and format in which a data message shall be filed, created or retained, the type of electronic signature required, the criteria to be met by an authentication provider, the appropriate control process and the procedure to ensure integrity, security and confidentiality of a data message or payment. It is therefore necessary for each public body to adopt a system of transmitting and receiving electronic messages in a manner that suits the specific requirements of the public body.

A signature is useful in confirming or endorsing the intent of the person signing a document, identifying that person and authenticating and confirming the integrity of the document signed.[137] In the faceless and impersonal environment of technology, it is critical to ascertain that a data message is initiated by a particular person or computer, that the message (especially the content of the message) has not been changed or tampered with during the process of transmission and is therefore authentic and reliable. An electronic signature is therefore a useful tool in ascertaining the integrity of the electronic communication.

The Electronic Signatures Act, 2011 provides for the use of electronic signatures in Uganda. The Act defines an electronic signature as data in electronic form, affixed to a data message or logically associated with it, which may be used to identify

the signatory or indicate the signatory's approval of the information contained in the data message[138].

The Act also provides specifically for the use of 'advanced electronic signature' and 'digital signature' as forms of electronic signature and for the use of third-party certification systems, such as a Public Key Infrastructure (PKI), for securing information conveyed over the Internet.

Although, according to the Act, digital signatures and PKI are supposed to be certified by a controller before they are made available by a service provider, the Act does not appoint a controller or certification authority and leaves this to the Minister of ICT to do at a later stage. While this is prudent and gives power to the Minister to satisfy himself or herself that the technological infrastructure is in place before appointing a controller or certification authority, it means that whereas the Act commenced on 15th April, 2011, electronic signatures are [or the electronic signature component is] not fully operational until the Minister has exercised the powers under the Act. The Ministry of ICT has developed draft regulations on which they are consulting various institutions before the Minister can sign them into law. [139]

A major challenge for public bodies like the Uganda Revenue Authority,[140] which are receiving and issuing information in electronic form, is that the information is not backed up by electronic signatures as required by law since there is no authority appointed to authenticate or certify them. These public bodies are therefore accepting electronic information but are asking for the hard copies of the information to back up the information submitted electronically.

The rules regarding admissibility and weight of evidence in Uganda are contained in the Evidence Act[141], which was borrowed from India and modified to suit the circumstances of Uganda. The rules categorize evidence into primary and secondary evidence and require in all cases that a person produce the best evidence available in support of their case.[142]

Section 8 of the Electronic Transactions Act, 2011 provides in respect to evidence that the rules of evidence as specified in the Evidence Act, should not be applied in a manner that denies admissibility of evidence merely because it is in electronic form, especially where it is the best evidence available.[143]

The key issues associated with electronic evidence are relevance and authenticity of the evidence. While these issues have been well articulated in some jurisdictions,[144] in Uganda authenticity of electronic transactions has not been determined by the courts.

Although the matter of admissibility is now settled by section 8, the issue of authenticity still lingers. Indeed in the cases where electronic records have been admitted in court, no proper test has been applied to the records, rather, the electronic records have just been attached as exhibits. In *Uganda vs Kato Kajubi,*[145] and *Uganda vs Dr Aggrey Kiyingi*, [146] for instance, computer printouts of mobile telephone numbers and messages were admitted to establish communication between persons accused of murder. Regarding a recording of a telephone conversation, the Judge observed that, "one cannot be certain about the authenticity of the telephone conversation".[147] Interestingly, three of the largest mobile telephone providers who were called as witnesses in this case confirmed that their systems did not have the capacity to listen to the telephone conversations and also alluded to the shortfalls in the printouts about telephone conversations.[148]

With regard to the evidential value attached to electronic records, section 8 (4) of the Electronic Transactions Act requires a court to take into account the reliability of the manner in which the electronic record was generated, stored or communicated.

2.2 Data protection and privacy

Data protection is the cornerstone of electronic transactions, since because of the borderless nature of the Internet, there is movement of data across international boundaries.

Regulations against the access or disclosure of data and the requirements to guarantee its security and privacy are necessary in establishing public confidence in using technologies that transmit data. The Computer Misuse Act, 2011[149] criminalizes unauthorized access to information. The Act guarantees the privacy only as far as it limits a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material from disclosing it to another person.[150]

The Regulation of Interception of Communications Act, 2010 and the Anti-Terrorism Act, 2002,[151]

on the other hand, make it lawful for security agencies to intercept and monitor emails and other communications in the course of transmission.

Due to the increasing use of the Internet and electronic communication in Uganda, and especially considering that the existing legislation on privacy,[152] in communication is rooted in telecommunications, there is dire need for legislation to be developed to address the issues of data protection.

Whereas the laws on data protection are not adequate, there are proposals for legislation to be proposed in this area in the future.[153]

2.3 Consumer protection

As a concept, consumer protection is linked to the idea of "consumer rights" (that consumers have various rights as consumers). Some of the generally accepted basic rights of consumers include:

1. Right to safety, which includes the right to protection from hazardous or dangerous goods or services.
2. Right to information, which includes making available to consumers information required in order for consumers to be able to weigh alternatives, and protection from false and misleading claims in advertising and labelling of products and services.
3. Right to choose: availability of competing goods and services that offer alternatives in terms of price, quality, service.[154]

Due to a lack of a general consumer protection law in Uganda, the provisions on the rights of consumers are scattered in more than one enactment.[155] In 2012, the Ministry of Trade revived the proposals for a Bill to enact a general law on consumer protection.

In the absence of a general consumer protection law, sections 24 to 28 of the Electronic Transactions Act, 2011 offer some protection to consumers involved in e-transactions. The Act requires that a person offering goods or services electronically must provide certain basic information to the consumers, including the name and legal status of the person, address and membership or accreditation to any self-regulatory body, a description of the goods or services, the time within which the goods or services shall be delivered or performed.

It also requires that an opportunity should be provided to a consumer to withdraw from the electronic transaction before it is concluded and requires a person offering services electronically to use a secure and technologically accepted payment system.

Most importantly, section 28 of the Act makes it unlawful for an electronic medium to contain a provision that purports to exclude the rights of consumers as provided for under the Act.

2.4 Copyright

The Copyright and Neighbouring Rights Act, 2006 acknowledges that literary, scientific and artistic works may be reproduced electronically, and therefore extends copyright protection to computer programmes and electronic data banks.[156] However, due to the borderless nature of Internet and other ICT services, it remains to be seen how an owner of a copyright can take advantage of section 43 of the Copyright Act, which allows an owner of the copyright to register the work that is the subject of protection as a means of providing information on ownership that information may be useful in resolving copyright infringement issues.

The Copyright and Neighbouring Rights Act, 2006 still requires that, for copyright to subsist in a work, the literary, scientific or artistic work must be reduced into material form.[157] The Act does not specify what 'material form' is, although this is easy to comprehend in a paper-based environment, it is not quite clear in an electronic environment given the intangible nature of data.

Due to the uncertainty in law of the issues relating to intellectual property, copyright, trademarks, and patents have been earmarked as areas that require further study.[158]

2.5 Domain name management

Internet domain names have assumed greater significance in the recent times with Internet increasingly being used as an effective medium for commerce, education, governance and communication. Domain names are seen in some circles as a form of commercial or digital property. Yet there is no legal or regulatory framework specifically providing for the acquisition or use of domain names in Uganda. At the dawn of the Internet in Uganda, the country did not have the necessary capacity to administer domain names including the country code Top Level Domain. ug.

The domain names relating to Uganda were administered by an American company before the administration was transferred to Computer Frontiers International,159 a private limited liability company based in Uganda. The Ministry of ICT is now in the process of establishing a policy for the regulation and management of domain names, including the resolution of conflicts and disputes.[160]

2.6 Cybercrime and cybersecurity

In developing a legal framework for electronic transactions and communications, one of the critical considerations was whether crimes in the cyberworld could be addressed through the existing body of criminal law or would require technology specific legislation. While developments in ICT come with new crimes, the technology also provides a different platform for the commission of existing crimes. Although some of the old crimes, like fraud, terrorism, money laundering, murder and theft committed with the aid of electronic mechanisms could still be prosecuted under the Penal Code, the code could not adequately address crimes that were specific to ICT like hacking and theft of computer programmes or software. In addition, the prosecution of traditional crimes committed with the aid of ICT also posed evidential difficulties to the prosecuting authorities.

In 2007, considering the nature of transactions involving money, before allowing the use of electronic payments systems, the Public Finance and Accountability Regulations were amended to provide specific penal provisions to cater to the transfer of money electronically. Offences like unauthorized access, modification and interception of computer programmes relating to payment systems were created to address some of the dangers in the cyberworld.[161] The Computer Misuse Act, 2011 now reinforces these and other offences relating to the cyberworld.[162]

The core of the computer misuse offences are contained in sections 12 to 27, which include offences relating to unauthorized access, access with intent to commit or facilitate the commission of a further offence, unauthorized modification of computer material, unauthorized use or interception of computer service, unauthorized disclosure of information, electronic fraud, cyber-harassment and cyberstalking.

Computer based pornography is one of the most significant forms of computer crime. The exploitation of children for sexual gratification through the use of technology is singled out and specifically highlighted by the law. The Computer Misuse Act, 2011 makes it an offence to produce, distribute, possess or transmit material that depicts a child engaged in sexually suggestive or explicit conduct.[163]

A major challenge is the capacity of the police to detect, investigate and assist the prosecution office in enforcing the provisions of the Computer Misuse Act, 2011. In addition the judicial officers are key to implementing the penal provisions and therefore their ability to understand electronic transactions is key to successfully supporting the development and use of electronic transactions in Uganda.

In the area of Community Emergency Response Teams (CERT), the Ministry of ICT at the beginning of 2011, partnered with the Uganda Communications Commission and the National Information Technology Authority of Uganda (NITA-U) to carry out an initial study to assess the need and make recommendations on the areas and responsiveness of the institutions to cyber-threats and issues related to cybersecurity. A critical area for the study is the required infrastructure to support the CERT. A multi-institutional taskforce with members from the Uganda Police Force and the Uganda Communications Commission; NITA-U has now been put in place to spearhead this effort.

2.7 Content control

In general terms, the existing legal regime does not provide for monitoring and controlling the information transmitted over the electronic medium. Indeed sections 29 and 32 of the Electronic Transactions Act, 2011 state that a provider of ICT services is not obliged to monitor the data transmitted through their service and exempts them from any liability in respect of third party material transmitted through the service they provide.

However, the Act does not protect service providers in respect of material transmitted or posted on their service where they are notified about infringing material or where they are under an obligation by contract, licence or law to remove,

block or deny access to specified material. In the case of infringing material, a service provider is only liable where he or she has actual knowledge that the material is infringing or is notified about the infringement and does not remove the material or link to the material within a reasonable time.

NOTES

27. The Tunis Commitment: http://www.itu.int/wsis/docs2/tunis/off/7.doc
28. Telecommunications Act No 1/011, 4 September 1997
29. Statement was made at the launch of the Kenya e-government Portal.
30. Postal and Telecommunications Sector Policy Statement, January 1997 at Page iii
31. Ibid at page 2
32. http://www.cio.co.ke/view-all-main-stories/3022-new-e-government-strategy-to-transform-public-service.html
    A new strategy covering 2011 – 2013 was opened to stakeholder consultation in March, 2011.
33. http://www.cio.co.ke/view-all-main-stories/3022-new-e-government-strategy-to-transform-public-service.html
34. M-Pesa is an SMS-based system that enables users to deposit, send and withdraw funds using their mobile phone. Customers do not need to have a bank account and can transact at any of the country's over 11,000 agents. Registrations and deposits are free and most other transactions are priced based on a tiered structure to allow even the poorest users to be able to use the system at a reasonable cost.
35. www.safaricom.co.ke
36. See UNCTAD Report, Mobile Money for Business Development in the East African Community: A Comparative Study of Existing Platforms and Regulations, June 2012 (UNCTAD/DTL/STICT/2012/2, available at http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf
37. The full text of the Act and Regulations can be found at: http://www.kenyalaw.org/kenyalaw/klr_app/frames.php
38. http://www.cck.go.ke/
39. http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7B1072058F-7B90-4A11-A5DF-E33AACEF4000%7D_E-commerce.pdf (Accessed on November 20, 2011)
40. http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf
    (Accessed on November 20, 2011)
41. http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf
    (Accessed on November 20, 2011)
42. SADC/ICM/1/2004/6.4.1
43. Article titled 'Electronic cheques to help Banks extend working hours' available at http://www.standardmedia.co.ke/InsidePage.php?id=2000034557&cid=14, May 2011
44. S. 83I(3) (a) and (b)
45. S. 83T
46. S. 83S(2)
47. http://www.e-government.go.ke/index.php?option=com_content&view=article&id=89&Itemid=94
48. Ibid.
49. S. 83K
50. s. 83P
51. S. 83O (3)(a)-(e)

52. S. 3(1) and (2) of the Regulations provide for the rights and obligations of customers of ICT licensees
53. http://www.kenyalaw.org/klr/index.php?id=98
The text of the Bill is available at number 51 Bill Tracker, 2011.
54. "Internet agreement" means a consumer agreement formed by text-based Internet communications.
55. Consumer Protection Bill at Memorandum of Objects and Reasons, Part IV
56. S.2(1)(g) of the Act
57. According to S.2(1) of the Act a "copy" means a reproduction of work in any manner or form and includes any sound or visual recording of a work and any permanent or transient storage of a work in any medium, by computer technology or any other electronic means.
58. S.38(1) of the Act
59. Section 90(1) of the Act
60. http://internationalcybercenter.org/workshops/cirtkenya2011 (Accessed on November 23, 2011). Reference to National CIRT Capacity Building Workshop, held on 21-22 November 2011, Nairobi, Kenya under the theme: 'Actualizing National CIRTs'.
61. S. 16. (1)(a) of the Act.
62. S.9(1) of the Regulations.
63. S.9(2) of the Regulations.
64. http://www.cck.go.ke/consumers/Internet_services/downloads/children_and_Internet_usefull.pdf (Accessed on November 18, 2011). See Fact Sheet on Child Safety and Internet Use.
65. http://www.centralbank.go.ke/downloads/nps/psk.pdf: 'Payment system in Kenya', September 2003.
66. S. 4A(1)(d) of the Central Bank of Kenya Act, CAP 491.
67. http://www.centralbank.go.ke/downloads/nps/psk.pdf (Accessed on November 18, 2011).
68. EFTs are used for transferring value between Banks on behalf of customers. Within Kenya's inter-bank exchange agreement, the EFT system is used as a facility for processing payments electronically via the Automated Nairobi Clearing House between the Kenya Bankers Association member banks. Value is given on a same day basis while finality and irrevocability of the payment is guaranteed.
69. Airtel Kenya website, africa.airtel.com/kenya
70. Essar website, www.yu.co.ke
71. Orange Kenya website, www.orange.co.ke
72. See UNCTAD Report, Mobile Money for Business Development in the East African Community: A Comparative Study of Existing Platforms and Regulations, June 2012 (UNCTAD/DTL/STICT/2012/2, available at http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf
73. http://www.ifc.org/ifcext/gfm.nsf/AttachmentsByTitle/Tool6.7.CaseStudy-M-PESAKenya+/$FILE/Tool+6.7.+Case+Study+-+M-PESA+Kenya+.pdf at page 9 (Accessed on November 18, 2011)
74. S. 127A (1) of the Act
75. S. 127D of the Act
76. S. 127E of the Act
77. See also: Women and cybercrime in Kenya: the dark side of ICTS. Available at www.nbo.icann.org/.../report-women-cybercrime-kenya-kictanet-11mar10
78. http://www.kenyalaw.org/klr/index.php?id=98 The Finance Bill is listed as n° 12.
79. http://www.kenyalaw.org/klr/index.php?id=98 The Energy and Communications Law (Amendment) Bill 2011 is listed as No. 28.
80. Ibid.
81. July 2007 and November 2009 respectively
82. Law N° 44/2001 of 30 November 2001

83. http://www.rura.gov.rw/index.php?option=com_content&view=article&id=145&Itemid=197
84. WTO Agreement on 'Trade-Related Aspects of Intellectual Property', 33 I.L.M. 81 (1994)
85. Press law n°18/2002 of 11/05/2002, article 73
86. See http://www.mhc.gov.rw/general-information/home.html
87. www.bnr.rw/docs/publicnotices/Law%2055-2007.pdf
88. www.bnr.rw/docs/publicnotices/LAWN0072008%20.pdf
89. www.bnr.rw/docs/publicnotices/Microfinance_Regulation.pdf
90. www.bnr.rw/docs/publicnotices/LawNo472008.pdf
91. www.bnr.rw/docs/publicnotices/Regulation%20No%2003%20%202011%20on%20pecuniary%20sanctions%20applicable%20%20to%20banks.pdf
92. www.bnr.rw/docs/publicnotices/Regulation%20No%20%2004%202011%20on%20Business%20Continuity%20%20Management.pdf
93. See ICT Policy, 2003 at page 10-11
94. Ibid at page 5
95. Ibid at page 14-15
96. See the Commission Report at www.ltct.go.tz
97. The law of Contract Act CAP 345 [RE.2292]
98. Cap 214 [R.E. 2002]
99. Reed C. Internet Law; Text and Materials 2000 at page 148.
100. Section 4 of The Law of Contract Act CAP 345 [RE.2292], which provides as to when communication of offer, acceptance and revocation is complete
101. See CAP 15 RE 2002
102. Section 35 of the Written Laws (Miscellaneous Amendments) Act, 2007
103. See Evidence Act, Civil Procedure Act, Contract Laws etc.
104. CAP 6, [RE. 2002]
105. Ibid.
106. Ibid section 33
107. The High Court of United Republic of Tanzania (Commercial Division) at Dar es Salaam Commercial case n°.4 of 2000 (Unreported)
108. See UNCTAD on The Legal Aspects of E-Commerce 2006. See also A. Mambi, a Source Book on Cyber Law and Information and Communication Technologies Law, 2010.
109. Turban E. on E-Commerce at page 139
110. [Cap 218 R.E. 2002]
111. See Rules for Uniform Domain Name Dispute Resolution
112. See www.policeforce.go.tz
113. See Regulation 18-21
114. Act No. 3 of 2010
115. Uganda National Information and Communications Technology Policy, October, 2003, 1
116. Uganda Investment Authority is promoting the opportunities that are available to investors within the sector. Uganda Communications Commission ICT Sector Brief, 2009
117. Established by the National Information Technology Authority Uganda Act, 2009, Act n°4 of 2009 to provide ICT services to the Government and to promote standards and use of ICT

118. Chapter 104 and 106 of the Laws of Uganda, Revised Edition (2000)
119. The Task Force was composed of members from various government departments and agencies including ministries of justice, trade and industry, water, lands and environment, finance, works and communication - now Ministry of Information, Communication and Technology, Uganda communications commission, Uganda Law Society, Uganda Investment Authority, National Bureau of standards, Bank of Uganda, Makerere University and the Uganda Insurance Commission.
120. The key findings were that Uganda's commercial justice system had fared badly because commercial life was encumbered and this had caused inadequacy in Government or service delivery and led to slow development of the private sector. In response, the Government of Uganda developed a four year detailed strategy for the reform of the commercial justice system. The essential elements for reform were the commercial courts, the commercial registries, the legal profession, the commercial regulatory environment and commercial laws.
121. Government of Uganda, Ministry of Works, Housing and Communications; *National Information and Communication Technology Policy, October 2003*.
122. The Government requires that any proposal for legislation is subject to the widest consultative process possible before it is submitted to the Executive for approval. Section Q of the *Uganda Government Standing Orders, February, 2010*
123. Uganda Law Reform Commission: A Study Report on Electronic Transactions Law, ULRC Publication No. 10 of 2004.
124. By virtue of section 1 of the Act the Minister responsible for ICT was given power to appoint a date when the Act would become effective as law. The Minister appointed 15th April, 2011.
125. Section 5 of the Act. However section 3 of the Act provides that a will, codicil, power of attorney, negotiable instruments (e.g. cheques) and documents creating or transferring interest in property cannot be made electronically.
126. Section 2 of the Act defines a data message as electronic representation of information generated, sent, received or stored by computer means.
127. Chapter 73 of the Laws of Uganda Revised Edition (2000), which is being replaced by the Contract Act, 2011 which is yet to come into force.
128. Chapter 82 of the Laws of Uganda, Revised Edition (2000)
129. Section 13 of the Electronic Transactions Act, 2011
130. However, this provision corresponds to the UN Electronic Communications Convention (2005), at article 14, and the Explanatory Note to the Convention illustrates the point (paragraphs. 224-250), which may guide any court's interpretation.
131. HCT—CC-CS -857-2007, UG CommC 20, http://www.ulii.org/ug/cases/UGCommC/2010 accessed on 02/06/2011
132. Uganda Law Reform Commission: A Study Report On Electronic Transactions Law, Law COM PUB n°10 of 2004) Kampala, Uganda, 2004
133. Chapter 1R of the Uganda Government Standing Orders, 1991 Vol. II (Government Printer Kampala, Uganda 1991)
134. Section 22
135. Section P-a of the Uganda Government Standing Orders, 2010. (Uganda Printing and Publishing Corporation Kampala, 2010)
136. Laws like the Official Secrets Act, Chapter 302 of the laws of Uganda
137. Uganda Law Reform Commission: A Study Report On Electronic Transactions Law, ULRC Publication No.1 of 2004 at 24

138. Section 2
139. The draft regulations include The Electronic Transactions Regulations, 2011, The National Information Technology Authority Uganda (arbitration or disputes) Regulations, 2012, The National Information Technology Authority Uganda (Accreditation of professionals and training institutions) Regulations, 2012, The National Information Technology Authority Uganda (National data bank management and data protection) Regulations, 2012 and The Electronic Signatures Regulations, 2012.
140. www.ura.go.ug accessed on 02/06/2011
141. Chapter 6 of the Laws of Uganda Revised Edition (2000)
142. Section 61 and 62 of the Evidence Act
143. This section is repeated in the Computer Misuse Act, 2011, as section 29.
144. United Republic of Tanzania, in Trust Bank Ltd v Le-Marsh Enterprises Ltd, Commercial Court Case No. 4 /2000. And in the U.S in Lorraine vs Markel America Insurance Co, 2007 WL 1300739 (D.Md May 4, 2007)
145. HCT – 06- CRSCO 16/2009 www.ulii.org> Databases accessed on 15/06/2011
146. HCT - Crim Case No. 0030/2006 www.ulii.org databases accessed on 14/06/2011
147. Per Justice Ruby Aweri Opio in Uganda vs Dr Aggrey Kiying and others
148. MTN, Celtel and UTL (Mango) appeared as prosecution witnesses.
149. Sections 12, 13 and 18
150. This provision is reiterated in section 81 of the Electronic Signatures Act, 2011.
151. Act No. 14 of 2002
152. The Uganda posts and telecommunications Act provides for secrecy of telephone communications and telegrams. It permits interception and disclosure only in the case of public emergency, public safety or tranquility under the direction of the minister responsible for internal security
153 Recommendation 24 of the Uganda Law Reform Commission: A Study Report on Electronic Transactions Law, ULRC Publication No 10 of 2004 at 87. www.ulrc.go.ug/reps&pubs accessed on 10/06/2011
154. U.N Guidelines on Consumer Protection, 1985
155. Some provisions on consumer protection can be found in the Sale of Goods Act, Chapter 82 of the Laws of Uganda
156. Section 2 and 5 of the Act
157. Section 4
158. Recommendation of Uganda Law Reform Commission, ULRC Publication n°.10 of 2004 www.ulrc.go.ug/reps&pubs accessed on 10/06/2011.
159. Randy Bush managed the domain names of some African countries including the United Republic of Tanzania before they were transferred to persons or institutions located within these countries.
160. The Ministry of ICT has now submitted a draft policy to Cabinet for approval, which provides for the establishment of a National Information Centre to take over the administration of domain names. Interview with Dr. David Turahi, Director ICT, Ministry of ICT, Kampala, 4th June, 2011
161. Regulations 74A to 74E of the Public Finance and Accountability (Amendment) Regulations, S.I n° 35 of 2007
162. Sections 3 to 9
163. Section 23 of the Act

ANNEXES

ANNEX I: RECOMMENDATIONS, FRAMEWORK PHASE I

E-Transactions

1. The Task Force recommends that any electronic transaction law be generally applicable to all civil and administrative law matters.
2. The Task Force recommends that private entities be given the freedom to depart from the provisions of the electronic transactions law by agreement, in specified circumstances.
3. The Task Force recommends that a comprehensive set of statutory definitions be incorporated into the electronic transactions legislation.
4. Provisions should be drafted recognising the validity of electronic communications as meeting the requirement for a 'writing', 'signature' or 'original' and all areas where the law requires a person to file paper documents with public bodies, including licensing and certification. Such validity may be subject to certain conditions being met and exemptions may be made for certain specified legal acts. The Task Force recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).
5. The Task Force recommends that these issues of contract law be expressly addressed in the electronic transactions law and recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).
6. The Task Force recommends that the electronic transaction law facilitates electronic record-keeping and permits the admission of electronic records as evidence before a judicial, administrative or dispute resolution body, subject to certain conditions.
7. The Task recommends that regional standards be developed, reflecting international standards, to assist judicial, administrative or dispute resolution bodies to evaluate the evidential value of electronic records.
8. The Task Force recommends that the electronic transactions law addresses the issue of when and where an electronic communication is sent and received, and recommends the wording used in the United Nations Convention on the Use of Electronic Communications in International Contracts (2005).
9. The Task Force recommends that specific provisions be made in any electronic transaction law stating that public authorities should accept electronic modes of communication.
10. The Task Force recommends that Partner States give consideration to the adoption of rules to protect communication intermediaries from liability for third-party content, subject to certain conditions.
11. In order for the EAC to keep abreast and take advantage of emerging opportunities in cyberspace, the Task Force recommends that:
    - Partner States should endeavour to research and implement institutional reforms to provide for policy formulation, implementation, regulations and private sector participation.
    - Consideration is given to institutional reforms at the EAC Secretarial level to carry forward emerging challenges in legal frameworks with respect to cyberlaw issues.

E-signatures and authentication

12. The Task Force recommends that Partner States give consideration to granting delegated authority to a specified government ministry or department to adopt relevant secondary regulations concerning digital signatures and the provision of certification services..

13. The Task Force makes the following additional recommendations in respect of electronic signatures:
    - That Partner States provide for a statutory definition for 'signatures' and 'electronic signatures'.
    - That Partner States should support the principle of technology neutrality and promote interoperability in respect of 'electronic signatures' technologies.
    - That Partner States should identify and recognise international standards in relation to the use and operation of electronic signatures.
    - That Partner States should consider the need for an institutional framework to support the provision of certification and related services at both a national and regional level.

Computer crime

14. The Task Force recommends that Partner States should undertake reform of their criminal laws to specifically provide for cybercrimes.
15. The Task Force recommends that the impact of ICTs on criminal conduct be given due consideration whenever a Partner State engages in a review or examination of its criminal code in the course of a reform initiative.
16. The Task Force recommends the following:
    - That Partner States undertake reform of substantive and procedural criminal laws to address the phenomenon of computer crime.
    - That the EAC Secretariat considers the possible role of the Court of Justice in addressing the multi-jurisdictional nature of computer crime and the adoption of common criminal procedures within the EAC.
    - That Partner States give due consideration to the wording and provisions of the Council of Europe Convention on Cybercrime (2001).
    - That the EAC Secretariat and the Partner States examine the possibility of acceding to the Council of Europe Convention on Cybercrime (2001).

Consumer protection

17. The Task Force recommends the following:
    - That the EAC Secretariat and Partner States give due consideration to consumer protection issues in cyberspace within a broader consumer protection framework, at both a national and regional level.
    - That reforms should encompass information requirements, cancellation rights, payment fraud and performance obligations.
    - That the EAC Secretariat and Partner States initiate programmes to raise consumer awareness about the benefits and risks of transacting in cyberspace, including such things as labelling schemes.
    - That the EAC Secretariat and Partner States give further consideration to the regional and national implications of electronic money or digital cash and the need to develop an appropriate regulatory framework.

Data protection and privacy

18. The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet; (b) that legislation providing for access to official information is appropriately taken into account; (c) the institutional implications of such reforms and (d) to take into account fully international best practice in the area.

ANNEX II: RECOMMENDATIONS, DRAFT FRAMEWORK PHASE II

Intellectual Property Rights

1. Without prejudice to any mode of licensing, Partner States should reform national copyright and related rights laws to ensure that the regime reflects the use of digital technologies, taking into account the WIPO Copyright Treaty (1996) and other relevant international instruments under which Partner States have obligations.

2. Further to Recommendation 11 in Phase I, Partner States should adopt rules to exclude liability for copyright infringement, where such copying is temporary or incidental and arises from the actions of an intermediary in course of transmission or from a lawful use of the work.

3. Partner States should ensure that national law appropriately balances the needs of rights-holders and rights of users in a digital environment. Partner States or the Council should also review the draft EAC Anti-Counterfeit Bill, taking into account the Anti-Counterfeiting Trade Agreement.

4. National domain name bodies, trade mark offices and other relevant bodies of the Partner States should be encouraged to co-operate in the establishment of dispute settlement mechanisms, which are fair, fast and affordable, to address claims between trade mark owners and domain name holders.

Competition

5. Rwanda and Uganda should enact domestic general competition laws and establish competition authorities, while Burundi should establish a domestic competition authority. Partner States should ensure that such authorities have the capacity and ability to take into account some of the unique features of economic activity in a cyberspace environment.

6. Taking into account R.5 above:

    6.1 The EAC Council should operationalise a regional competition authority in accordance with the EAC Competition Law 2006;

    6.2 Partner State competition authorities should be given specific training in considering the unique features of economic activity in a cyberspace environment;

    6.3 Institutional arrangements between national and regional competition authorities should facilitate an exchange of experience and the sharing of information and best practices to coordinate enforcement;

    6.4 Competition authorities should actively engage in the work of organisations such as the African Competition Forum, International Competition Network, OECD, UNCTAD and the WTO.

7. Further to the recommendations made in Phase I, Partner States should implement reforms in national consumer protection laws, as an important component of an effective competition law regime.

8. Partner States should give specific consideration to proactive measures that may facilitate consumer access to the Internet, through product and service innovation, availability, improved quality of service, and affordable prices.

Taxation

9. Partner 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.

10. Partner States should review related laws governing the deemed location of a business to ensure that they are consistent with the applicable taxation regime.
11. The EAC Task Force on Tax Harmonization should consider the need for reform of the tax regime to reflect the increasing consumption of intangible digital products and services.
12. The rules and procedures governing tax administration 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 collection of consumption taxes in an online environment.

Information Security

13. Partner States should further harmonise national ICT policies in respect of information security measures.
14. Partner States should consider mandating compliance with regional or international security standards (e.g. ISO 27001), including in specified circumstances (e.g. payment applications) or by specified entities (e.g. Internet service providers).
15. Partner States should require national centres of expertise for responding to emerging cyber-threats to co-operate with similar centres at a regional and international level.
16. Partner States should consider adopting security breach notification laws, regulations or rules, applicable to those providing services over the Internet.
17. Partner States should consider measures to raise awareness about good information security practices.

ANNEX III: OTHER AFRICAN CYBERLAW REFORM INITIATIVES

In various regional economic communities in Africa, other initiatives have been made to develop harmonized policy and legal frameworks for e-commerce. Of the five Partner states of the EAC, Burundi, Kenya, Rwanda and Uganda are also members of the Common Market for Eastern and Southern African States (COMESA).[164] The United Republic of Tanzania is a member of the Southern African Development Community (SADC).[165] Burundi also belongs to the Economic Community for Central African States (CEEAC).[166] Rwanda has recently joined the Commonwealth, joining Kenya, Uganda and the United Republic of Tanzania.[167]

In November 2002, the Commonwealth Law Ministers adopted a series of model laws to assist the Member States on 'Computer and Computer-related Crimes', on 'Electronic Transactions', 'Privacy' and 'Evidence'.

SADC and the USAID have funded Dot-Gov Southern African Development Community ICT and Policy Regulatory Support (SIPRS) project to develop the SADC Model E-Commerce Law, to harmonize the legal framework for e-commerce.[168] The draft framework was first considered at a SADC workshop held in Johannesburg, South Africa, on 24th November 2003.[169] The SADC Model Law addresses two key issues, electronic commerce and data protection. It was based on existing legislation in the region and the UNCITRAL Model Law on Electronic Commerce. The Model Law has been adopted by SADC and is in the process of being updated for implementation in the SADC region.[170]

COMESA has developed regional initiatives mainly related to policy harmonization in ICT.[171] The Southern African Transport and Telecommunications Commission (SATCC) formulated the Model Regulatory Framework for Telecommunications in 1998.[172] In 2002, COMESA adopted a Model ICT Policy that draws heavily from the SADC Protocols, and is currently preparing a model law.[173] In 2003, COMESA established the Association of Regulators of ICT in Central and Eastern Africa (ARICEA).[174] There is now essentially little difference in the ICT policy models and regulatory guidelines of SADC and COMESA.[175]

In 2006, the Economic Community of West African States (ECOWAS) published a legal framework for electronic commerce.[176]

In 2007, the Council of Ministers of COMESA adopted an ICT Strategy whose pillars include: development of an institutional framework; legal and regulatory framework; common ICT infrastructure, eg. COMTEL and EASSy cable projects; and priority e-government services such as e-parliament and e-customs.

In October 2011, the African Union,[177] in conjunction with the UN Economic Commission for Africa, issued a draft Convention 'on the establishment of a credible legal framework for cybersecurity in Africa'. The Convention contains sections on electronic commerce, protection of personal data, cybercrime and cybersecurity. Although ambitious in scope and coverage, the need to obtain the agreement of all 54 Member States may mean that, if the draft proceeds towards adoption, the proposal will need to be substantially narrowed down, especially to reflect the laws already adopted within Africa.

ANNEX IV: EAC TASK FORCE MEMBERS ON CYBERLAWS (as of October 2011)

BURUNDI

Mr Gabriel Bihumugani, Conseiller Juridique, 2ème Vice Présidence de la République du Burundi
Mme. Claudette Mukankuranga, Conseiller Juridique, Ministère à la Présidence chargé des Affaires de la Communauté Est Africaine
Mr. Pierre Ndamama, Technical Manager, ICT Executive Secretariat
Mrs. Delphine Nimbeshaho, Advisor in Legal and Administrative Matters, Second - Vice Presidency
Mr. Alexis Sinarinzi, Conseiller Juridique, Agence de Régulations et de Controles de Télécommunications

KENYA

Ms. Charity Kimani, Legal Officer, Ministry of Information and Communications
Mr. James Kivuva, Ministry of East African Community
Mr. Alex Mbuvi, State Counsel, State Law Office
Mr. Stephen Mwaura Nduati, Head, National Payment System, Central Bank of Kenya
Mr. John Sergon, ICT Director, Directorate of e-Government
Ms. Mercy Kiiru Wanjau, Principle Legal Officer, Communications Commission of Kenya

RWANDA

Mrs. Joy Kabushubi, Legal Officer, Rwanda Utilities Regulatory Agency
Mr. Allan Kabutura, Head, IT Strategy and Policy; IT Consultant, Rwanda Development Board
Mr. Seth Kwizera, Intellectual Property Expert, Ministry of Trade and Industry
Mr. R. Charles Mugisha, Rwanda Development Board
Mr. Sam Toyota, Director Information Systems and Technology, Rwanda Revenue Authority

TANZANIA

Mr. John Daffa, Principal Legal Officer, Tanzania Communications Regulatory Authority
Ms. Maureen Fondo, Legal Officer, Ministry of Industry and Trade, Copyright Society of Tanzania
Mr. Saidi M. Kalunde, State Attorney, Attorney General's Chambers, Division of Public Prosecutions
Mr. Adam J. Mambi, Deputy Executive Secretary, The Law Reform Commission of Tanzania
Ms. Halima Masudi, ICT Engineer, Ministry of Communications, Science and Technology
Ms. Esuvat Mollel, Legal Officer, Ministry of East African Cooperation
Mr. George B. Sije, NPS –Legal Counsel, Bank of Tanzania
Ms. Joyce Sojo, Legal Counsel, Tanzania Revenue Authority

UGANDA

Ms. Stella Alibateese, Director of Legal and Regulatory Services, National Information Technology Authority
Mr. Denis Kibirige, Senior State Attorney, Ministry of Justice and Constitutional Affairs
Ms. Rosemary Kisembo, Manager Software Engineering, Uganda Revenue Authority
Ms. Mary Kamuli Kuteesa, Supervisor Litigation, Uganda Revenue Authority
Mr. George Lwevoola, Ministry of East African Community Affairs
Ms. Juliet Nassuna, Ministry of Justice and Constitutional Affairs
Mr. Kenneth Rutaremwa, Legal Officer, Uganda Law Reform Commission
Mr. David Turahi, Director of Information Technology and Information Management Services, Ministry of Information and Communication Technology

EAST AFRICAN COMMUNITY

Mr. Robert Achieng, Senior Engineer - Communications, EAC Secretariat
Mr. Mathews Nduma, Principal Legal Officer, EAC Secretariat

EAST AFRICAN LEGISLATIVE ASSEMBLY

Mr.Enock Musiime, Research Officer, EALA

EAST AFRICAN LAW SOCIETY

Mr. Leonard Obura Aloo, Advocate, Mwaura & Wachira Advocates

EAST AFRICAN BUSINESS COUNCIL

Mr. Adrian Njau, Trade Economist, EABC

LIST OF SELECTED PUBLICATIONS IN THE AREA OF ICT AND LEGAL ISSUES

UNCTAD (2012). Mobile Money for Business Development in the East African Community: A Comparative Study of Existing Platforms and Regulations. UNCTAD/ UNCTAD/DTL/STICT/2012/2

UNCTAD (2009). Study on prospects for harmonizing cyberlegislation in Latin America. UNCTAD/DTL/STICT/2009/1 (available in Spanish)

UNCTAD (2009). Study on prospects for harmonizing cyberlegislation in Central America and the Caribbean. UNCTAD/DTL/STICT/2009/3 (available in Spanish)

UNCTAD. Information Economy Report 2007-2008: Harmonizing cyber legislation at the regional level: the case of the ASEAN

UNCTAD. Information Economy Report 2006: Laws and contracts in an e-commerce environment

UNCTAD. Information Economy Report 2005: Addressing the Phenomenon of Cybercrime

UNCTAD. Electronic Commerce and Development Report 2004: Protecting Privacy Rights in an Online World

UNCTAD. Electronic Commerce and Development Report 2003: Domain Name System and Issues for Developing Countries

UNCTAD. Electronic Commerce and Development Report 2002: Online Dispute Resolution

UNCTAD. Electronic Commerce and Development Report 2001: Overview of Selected Legal and Regulatory Developments in E-commerce

NOTES

164. COMESA is a Regional Economic Block comprising of 49 southern, Central, Eastern and Northern Africa Countries. It was established on 5th November 1993 and it replaced the former preferential Trade Area (PTA).
165. SADC is an economic block comprising of 14 southern, Central and East African Countries and was established on 17th August 1992. See http://www.sadc.int
166. ECCA, as the name connotes, is comprised of Central African States
167. http://www.thecommonwealth.org
168. E/ECA/CODIST/1/15
169. SADC/ICM/1/2004/6.4.1
170. For more information on the ITU/HIPSSA Project, see http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/
171. According to Shuller Habeenzu, in a paper titled "Zambia Trade and Investment Enhancement Project (ZAMTIE)" October 2003, to be found on www.zamtie.org, SADC has been at the forefront of regional ICT initiatives in Africa such as the Africa Information Society Initiative (AISI) and Connection Africa to improve connectivity and the use of ICTs, pg. 4
172. Pursuant thereto, the member countries have established autonomous regulatory authorities and have operating policies in place.
173. Shuller Habeenzu, Supra at pg. 6
174. http://www.tra.gov.eg/presentations/AfricaFifth07/Flyer.pdf
175. Shuller Habeenzu, Supra at pg. 6
176. Funded by the UNECA
177. www.au.int