The Internet and Regulatory Responses in Ethiopia:

Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media

Kinfe Micheal Yilma [♣] and Halefom Hailu Abraha[♣♣]

Abstract

Whilst Ethiopia has telephone services since 1894 − not long after its invention−, the history of the Internet in Ethiopia is less than two decades old. The prototype Internet with limited accessibility was introduced only in 1997, and broadband Internet was not widely deployed until recently. This slow pace in the proliferation of the Internet has delayed the legislative responses of the country to the brave new worlds of the Internet. Despite a few laws currently in operation namely the cybercrime and telecom fraud offence laws, most areas of the online environment needs the attention of the Ethiopian legislature. Nonetheless, there are few draft cyber laws that are in the pipeline. This article briefly reviews major legislative developments in telecoms, cybercrime, privacy, e-commerce and the new media. It sketches legislative responses of the Ethiopian legislature to the advent of the Internet by outlining major sources of Internet law and their defining features. The article further considers the salient features of the major draft pieces of cyber legislation that await enactment.

Key terms

Internet, information technology, telecommunications, cyber law, Internet law, e-commerce, Ethiopia

DOI http://dx.doi.org/10.4314/mlr.v9i1.4

Acronyms

CA	Certification Authority
DESL	Draft Electronic Signature Law
DETL	Draft Electronic Transactions Law
DoS	Denial of Service Attacks

[♣] Kinfe Micheal Yilma (LLB, Addis Ababa University; LLM, University of Oslo; LLM, Brunel University London). The author was formerly a Lecturer-in-Law at Hawassa University. Currently, he works as an independent consultant and researcher.

[♣♣] Halefom Hailu Abraha (LLB, Mekelle Univeristy; LLM, University of Southampton). The author currently serves as Deputy Director of Legal and Policy Affairs and as a Cyber Law and Policy Researcher at the Ethiopian Information Network Security Agency.

The authors thank Ato Kidus Teshome for his support in the course of writing this article. Comments to the authors may be forwarded to: kinfeyilma@gmail.com.

EBA	Ethiopian Broadcasting Authority
ECX	Ethiopian Commodity Exchange
EICTDA	Ethiopian ICT Development Agency
ETA	Ethiopian Telecommunications Agency
EU	European Union
ICT	Information and Communication Technology
NSA	Information Network Security Agency
IP	Internet Protocol
INSA	Ethiopian Information Network Security Agency
ITU	International Telecommunications Union
MCIT	Ministry of Communication and Information Technology
NISS	National Intelligence and Security Service
PKI	Public Key Infrastructure
RCA	Root Certification Authority
SATRC	South Asian Telecommunications Regulator's Council
TFO	Telecom Fraud Offences Proclamation
TVRO	Television receive-only
UNCITRAL	United Nations Conference on International Trade Law
VoIP	Voice over Internet Protocol

> "The Government strongly supports the use of the Internet, and recognizes the benefits that it gives to our society […]. However, cybercrime poses a number of challenges for Government."[1] Debretsion Gebremichael

> "The sad irony is that Ethiopia's enthusiastic embrace of the computer has made it more vulnerable, as people start dispensing with paper records."[2] Chris Michael

Introduction

Ethiopia was among the few beneficiaries of telecommunication services soon after its invention in the last quarter of the 19th century. The Internet was, however, introduced rather late (in 1997) with limited access. In 2005 the first four thousand kilometres of fibre optic backbone were laid in Addis Ababa.[3] Ethiopia is currently amongst countries with the lowest level of Internet penetration and use. According to World Internet Status data for 2014, for

[1] Debretsion Gebremichael, Cybercrime: Current and Future Trends, *Global-ICT-2012*, 2012, available at <http://bit.ly/1bGaJJK> (Last accessed on 25 September 2015). Dr. Debretsion is the Deputy Prime Minister and Minister of Communication and Information Technology of Ethiopia.

[2] Chris Michael, Computer Viruses' Slow African Expansion, *The Guardian*, 12 August 2009, available at <http://bit.ly/1IrfbZT> (Last accessed on 25 September 2015).

[3] *See* Ethiopian Ministry of Communication and Information Technology, *Communication and Information Technology Statistical Bulletin,* Vol. 1, No. 1, 2014, p. 6; see also Aman Assefa, Information and Communications Technology in Ethiopia: Challenges and Prospects from an A2K Perspective, *in Proceedings of the Gathering of the Access to Knowledge Global Academy*, Yale Law School Information Society Project, August 2009, p. 168.

instance, Ethiopia has had only 1.9% Internet penetration.[4] Similarly, the World Economic Forum rates the number of Internet users in Ethiopia at 1.9%, ranking 139 out of 144 countries.[5] Recent data released by the Ethiopian government claims that the level of Internet penetration has reached 5.5% as of December 31, 2013.[6] Much of the Internet traffic in Ethiopia is said to be downloads of content from overseas websites than uploads of local content which constitutes only 10% of the overall Internet traffic in the country.[7]

This delay in the proliferation of the Internet has partly played a role in delaying legislative measures in the field of Internet law.[8] The first Ethiopian legislation that addresses Internet-related endeavours and/or behaviours came only in 2004,with the adoption of the Ethiopian Criminal Code which penalizes a short list of computer crimes most notably 'computer hacking', 'spreading malware' and 'denial of service (DoS) attacks'.[9] The other –and so far the most

[4] World Internet Stats, *World Internet Usage and Population Statistics 2014*, 2014, available at <http://bit.ly/1z8zSrO> (Last accessed on 25 September 2015).

[5] *See* Klaus Schwab, Editor (2014), *The Global Competitiveness Report 2014-2015*, Full Data Edition, The World Economic Forum, p. 509.

[6] See Ethiopian Ministry of Communication and Information Technology, *Communication and Information Technology Statistical Bulletin, supra* note 3, p. 7. In a very recent interview, Dr. Debretsion revealed that the number of Internet users in the country has reached over seven million, which accordingly would put the level of Internet penetration about 7 %. *See* Dawit Kebede, The Success Story of Ethiopia's ICT: Interview with Dr. Debretsion, *Awramba Times*, 3 May 2015, webcast available at <http://bit.ly/1EZt8JA> (Last accessed on 25 September 2015).

[7] See Jemal Abdu, Think Tank Research Calls for Telecom Reform, *Addis Fortune*, Vol. 15 , No. 766, 5 January 2015, available at <http://bit.ly/1vUl4V2c> (Last accessed on 25 September 2015).

[8] Internet law – also called cyberspace law, computer law or cyber law – is a new field of law that studies the legal aspects of human experience in the virtual world often referred to as 'cyberspace'. See Brayan Garner , Editor (2004), *Black's Law Dictionary*, St. Paul Minn, 8th Ed, p. 1168; *see* also Victor Mayer-Schonberger (2003), The Shape of Governance: Analysing the World of Internet Regulation, *Virginia Journal of International Law*, Vol. 43, p. 606; see also Chris Marsden, Internet Law, *Oxford Bibliographies*, 26 June 2012, available at <http://bit.ly/1FqT7gO> (Last accessed on 25 September 2015).

[9] *See* Arts 706 -709, Ethiopian Criminal Code, *Federal Negarit Gazeta*, Proclamation No. 414/2004. Note that dozens of cybercrimes have been committed in Ethiopia since the enactment of the Code, but there currently are only few reported court cases where cybercrime rules of the Code were applied. See, for instance, Fasika Tadesse, Yonas Kassahun Receives Two-Year Jail Sentence for Cyber Crimes Against Akiko Seyoum, *Addis Fortune*, Vol. 15, No. 757, 2 November 2014, available at <http://bit.ly/1bEUb5C>. *See* also Fasika Tadesse, Akiko Sees a Cyber-Crime Guilty Ruling against Accuser for 42m Br**,** *Addis Fortune*, Vol. 15, No. 756, 26 October 2014, available at <http://bit.ly/1GuZAcf>; Lucy Kassa, Diaspora Investor Set Free in a Higher Court

recent– cyber legislation in Ethiopia is the Telecom Fraud Offense law that deals with frauds committed through the use of telecom networks and services.[10] Contrary to what its title might suggest, the telecom fraud offense legislation regulates a broad range of matters in connection with telecoms. This is precisely because the term 'telecom' normally includes Internet services under the Ethiopian telecommunication legal regime.[11] In addition to these legal instruments, a number of other Ethiopian laws could potentially be construed to cover activities and behaviours in the context of the Internet as the following discussions illustrate. Moreover, there are ranges of cyber-related legislation drafted a few years ago and currently under consideration before the relevant government authorities.[12]

This article reviews major legislative developments in the field of Internet law in Ethiopia. It sketches legislative responses of the Ethiopian legislature to the advent of the Internet by outlining major sources of Internet law and their defining features. In so doing, it reviews legal instruments governing (or set to be governing) cybercrime, electronic commerce, telecoms, electronic privacy and the new media. The critical comments made in this article are meant to constructively inform ongoing debates on the draft laws. The draft laws are also expected to pay due attention to internet governance in Ethiopia, an issue which is beyond the scope of this article. The issue of internet governance is briefly

Reversal of A Two-Year Sentence, *Addis Fortune*, Vol. 15, No. 767, 11 January 2015, available at <http://bit.ly/1Fmkedi> (Last accessed on 25 September 2015).

[10] *See* Telecom Fraud Offence Proclamation, *Federal Negarit Gazeta,* Proclamation No. 761/2012. Note that just between December 2013 and March 2014, over 17 telecom fraudsters have been convicted under the telecom fraud offense law. See, for instance, Bezawit Zegeye, Phone Company Fraudsters Found Guilty, *The Reporter,* 8 February 2014, available at <http://bit.ly/1GkhZaM> (Last accessed on 25 September 2015).

[11] *Id.*, Art 2(1); see also Art 2(4), A Proclamation to Provide for the Amendment of Telecommunications Proclamation No. 49/1996, *Federal Negarit Gazeta*, Proclamation No. 281/2002. As the reader will easily note, this article includes 'telecoms' within the general discussions of Internet law in Ethiopia. See, for instance section 2 below. Also to be noted is that for the purposes of this study, the discussions within the rubric of the Internet embraces various hitherto disparate digitized services precisely because technological convergences, as shall be seen in section 1 below, have resulted in the convergence of these digitized services such as telephony into the Internet. Therefore, all references to the Internet equally apply to telecommunications and other forms of communications enabled by the Internet.

[12] *See*, for instance, Draft Ethiopian Data Protection Act, Version 1.1, 7 May 2009; Draft Proclamation to Legislate, Prevent and Control Computer Crime, July 2013; Draft Electronic Transactions Law, October 2014 (On file with Authors).

discussed in another article (by the same authors) which is concurrently published in the same issue of this journal. [13]

The aim of this article is not to provide a deeper analysis of each theme covered herein, and it rather introduces the subject to the Ethiopian legal discourse so that constructive discussions could be evoked among interested academics, lawyers, prosecutors, students and judges. Future academic works can be geared towards addressing specific legal issues raised by the Internet in the Ethiopian context. For purposes of convenience, this article interchangeably uses the term 'Internet' and 'cyberspace'.[14]

1. Technological Convergence and the Law in Ethiopia

1.1 Regulatory and legislative impact of technological convergence

Digital technology is what allows the convergence of media (from print to television) with telecommunications (fixed or mobile) and computing industries (hardware and software).[15] The definition of "convergence" is sometimes elusive as it has technological, economic, and regulatory dimensions.[16] But, it mainly deals with the integration between the telecommunications, broadcasting and information technology sectors. Convergence may also mean the

[13] Note that any standard text on Internet law allocates a chapter to issues of Internet governance whose various aspects are partly regulated through law – hence Internet law. See, for instance, part I of Lillian Edwards and Charlotte Waelde's, Editors (2009), *Law and the Internet,* 3rd edition, Hart Publishing; *see* also Chapters 20 and 26 of Ian Lloyd's, *Information Technology Law*, 7th Edition, Oxford University Press, 2014.

[14] The term 'cyberspace' refers to the invisible, intangible world of electronic information and processes stored at multiple inter-connected sites, with controlled access and manifold possibilities for interaction. In essence, cyberspace is a virtual space created by the existence of the Internet. Of course, as some commentators claim, the Internet constitutes only a 'small' portion of cyberspace. Whereas the term 'Internet' refers to a network of networks that transmits packets of data through computer networks that are assembled at their destination. It refers to both the technical and physical infrastructures that enable switching of data packets from the source computer to the destination. *See* Klaus Grewlich (1999), *Governance in Cyberspace: Access and Public Interest in Global Communications,* Kluwer Law International, p. 1; *see* also Victor Mayer-Schonberger, (2001), The Authority of Law in Times of Cyberspace*, Journal of Law, Technology and Policy,* Vol. 1, p. 2; Jay Krasovac, Cyberspace: The Final Frontier for Regulation, *Akron Law Review*, Vol. 31, No. 101, 1997/98, p.1.

[15] *See* the International Telecommunications Union, *Trends in Telecommunication Reform: Convergence and Regulation*, 1999, p. 3, available at <http://www.itu.int/itudoc/itu-d/trends99>/ (Last accessed on 25 September 2015).

[16] See Yo-li Liu (2011), The Impact of Convergence on the Telecommunications Law and Broadcasting-Related Laws: A Comparison Between Japan and Taiwan', *Kio Communications Review,* No. 33, p. 1.

combination and integration of previously separate end-user equipment, such as telephones, televisions and personal computers, into a single device. This convergence of technological platforms in turn leads to changes in the industries, markets, policies and regulations in the respective sectors.

Historically, telecommunication, broadcasting, and other related areas were separate industry segments; they used different technologies and were governed by different regulations.[17] Services such as phone, data and video were treated differently and the means of delivering these services were entirely different. But now, the distinction is blurred as we can make telephone calls, watch television, and share music on handheld devices such as smartphones *via* the Internet.[18] The question would be whether the apparatus is really a phone, or a television set or a computer. The other question would be how such a mobile phone can be regulated, and whether it should be regulated by the telecommunications laws or the broadcasting law or the other Information and Communication Technology (ICT) related laws.[19]

Convergence in the telecommunications, broadcasting and IT industries thus raises a number of legal and regulatory issues and problems which need to be addressed by governments and regulators.[20] From the regulatory and legal perspective, these three sectors use the same technologies but they are subject to different regulatory bodies and legislation. This creates uncertainty with respect to the regulation and classification of services. For instance, it is not clear whether audiovisual content offered through the Internet or a mobile telephone can be defined as telecommunications or broadcasting service. There are also potential conflicts in regulation as different standards of content regulation are applied to telephony, sound and television broadcasting, print media and the Internet.[21] Convergence also affects licensing frameworks. Traditionally, different service categories require separate licenses. On the other hand, digital convergence requires unified license as these different services (broadcasting, voice and data) can be offered in the same platform.

---

[17] Jovan Kurbalija (2014), An *Introduction to Internet Governance*, 6th Edition. Diplo Foundation, pp. 64-65.

[18] *Ibid.*

[19] John Ubena (2009), Why Tanzania Needs Electronic Communication Legislation? Law Keeping up with Technology, *Law Reformer Journal* , Vol. 2, No. 1, p. 22.

[20] Angeline Lee, Convergence in Telecom, Broadcasting and IT: A Comparative Analysis of Regulatory Approaches in Malaysia, Hong Kong and Singapore, *Singapore Journal of International & Comparative Law*, Vol. 5, 2001, pp. 674 -695.

[21] The International Telecommunications Union and InfoDev, *ICT Regulation Toolkit*, November 2006, available at <http://www.ictregulationtoolkit.org/6> (Last accessed on 25 September 2015).

In order to address the challenges of convergence, reforms are now underway in many countries. Even though there is no single model that best fits regulatory, economic, social, technological circumstances for every country, there are two prevalent approaches to convergence regulation. The first approach is called "sector-specific". According to this approach, telecommunication, broadcasting and information technology sectors are treated differently and regulated by separate regulatory agencies.[22] In the converged environment, this approach creates duplication and uncertainty for regulatory activities that are common to different industries.

The second approach is "converged regulator" in which all communications services including telecommunications, broadcasting and information technology are regulated under the umbrella of one regulatory body.[23] Reports show that increasing convergence in the ICT sector has led more countries to create common regulator with responsibilities over the telecommunications, broadcasting and information technology sectors. For instance, in the United Kingdom, the Communications Act 2008 created the Office of Communications (Ofcom) which combines five former regulatory agencies and became the regulator for television, radio, and telecommunications.[24] Several other countries also introduced similar approach, following the logic that a converged regulator is better suited to respond to new technologies and the overlapping services offered by formerly separate categories of service providers. There are also some countries that either do not take adequate measures or did not implement anything. The question is, therefore, where Ethiopia fit in this picture. The following discussion illustrates the state of affairs in Ethiopia.

1.2 Ethiopia's regulatory and legislative response to technological convergence

The Ethiopian government sees ICT as central to the country's development, to enhance the provision of information and services to its citizens and as a tool of poverty reduction.[25] Among the several ICT projects currently underway in Ethiopia, one is migration from analogue to digital broadcasting. Ethiopia is working to undertake digital switch by the end of 2016 following the decision of the International Telecommunications Union (ITU) that member countries must transform their broadcast system to digital technology.[26] The ultimate result of

[22] *Ibid.*
[23] *Ibid.*
[24] *Ibid.*
[25] The Federal Democratic Republic of Ethiopia, *The National Information and Communication Technology Policy and Strategy*, Addis Ababa, August 2009, p. 2.
[26] Ethiopia to Switch Country to Digital by End of 2016, *Balancing Act*, 23 October 2014, available at <http://bit.ly/1cn3maD> (Last accessed on 25 September 2015).

these developments is the increase of converged information, communications and entertainment services on broadband networks. This, in turn, would pose challenges to regulatory and legislative frameworks as overlaps between functions and uncertainties in the classification of services are inevitable and existing legislation that regulates the sector would become largely obsolete.

It is vital to note that it was only in 2011 that the Ethiopian government realized the converging trend of historically different sectors. Until 2011, Ethiopia treated the telecommunications, broadcasting, and ICT sectors separately and they were regulated by separate bodies under different laws. The Ethiopian Telecommunications Agency (ETA) was established by the Telecommunications Proclamation No. 49/1996 (as amended in 2002) as a regulatory authority responsible for regulating the telecommunications industry and make sure the observance of Telecommunications legislation. The Ethiopian Broadcasting Authority (EBA), established by Proclamation No. 178/1999, was responsible to regulate the broadcasting sub-sector. The EBA was re-established by the Broadcasting Service Proclamation No. 533/2007 with additional regulatory powers. According to this Proclamation, EBA is empowered to plan, permit and control the use of the radio wave allocated for broadcasting service.[27] The EBA is also responsible to regulate advertisement and print media.[28]

In the year of 2003, the government established the Ethiopian ICT Development Agency (EICTDA) with a mandate to regulate and support information technology services in the country.[29] While the EBA was confined solely to the broadcasting sector, the ETA and EICTDA continued to share responsibilities across the regulatory divide. In 2011, the government made some efforts toward sector reform, following the adoption of Proclamation No. 691/2010 (as amended in 2011) by which a new Ministry of Communication and Information Technology (MCIT) was established with the intent to bring the aspects relating to communications handled by the former Ministry of Transport and Communications, as well as the regulatory powers of ETA and EICTDA together.[30] A new Directorate, the Communications and Information Technology

[27] Art 7(6), Broadcasting Service Proclamation, *Federal Negarit Gazeta,* Proclamation No. 533/2007.

[28] Art 31, Advertisement Proclamation, *Federal Negarit Gazeta,* Proclamation No.759/2012; see also Art 11 (1), Council of Ministers Government Communication Affairs Office Establishment Regulation, *Federal NegaritGazeta,* Regulation No. 158/2008.

[29] A Proclamation to Provide for the Establishment of Ethiopian Information and Communication Technology Development Agency, *Federal Negarit Gazeta*, Proclamation No. 360/2003.

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

Standardisation and Regulation Directorate, was created under MCIT to handle all regulatory issues of Telecommunications, Postal and Information Technology.[31]

While the Ethiopian government has moved one step forward in converging the regulatory bodies for telecommunications, postal and Information Technology services, the question which remains to be answered is whether the existing regulatory and legislative frameworks fully meet the new requirements of convergence. The present *status quo* in Ethiopia does not indicate substantial shift from a sector-specific approach because telecommunications and broadcasting are regulated by separate authorities and subject to scattered pieces of legislation. This approach poses challenges to existing regulatory functions. For instance, while the overall spectrum management is entrusted upon the MCIT, the EBA is also responsible to plan, permit and control the use of the radio wave allocated for broadcasting service.[32] This clearly demonstrates the inevitable overlapping of jurisdiction between the two authorities, which may also lead to over regulation – or 'regulatory overkill'.

Another instance is the uncertainty as to who regulates the new service created by digital technology and under what law. Webcasting of radio and television programs on the Internet, for instance, use radio waves and therefore are subject of the broadcast regulation. These services also use the Internet and hence subject to the telecommunications laws. As already described above, digital convergence has blurred the distinction among telecommunications, broadcasting and information technology services and devices. Unless the respective legislative and regulatory frameworks are converged accordingly, whether a given electronic communication service should be regulated by the telecommunications laws or the broadcasting law or the other ICT related laws remains uncertain.[33]

In 2014, the government announced two draft laws following the plan to migrate from analogue to digital broadcasting. The first draft law deals with the establishment of "Broadcast Network Administration Authority" and the other piece of draft legislation concerns mass media which would repeal the Broadcasting Service Proclamation No. 533/2007. Under the draft "Mass Media Proclamation", the EBA is replaced by the "Ethiopian Mass Media Authority" with additional powers of regulating the "Broadcast Network Administration Authority" and Webcasting/Online Broadcasting services.[34]

---

[31] *See* details at <http://bit.ly/1HrW9Um> (Last accessed on 25 September 2015)
[32] Art 7(6), Broadcasting Service Proclamation, *supra* note 27.
[33] Ubena, *supr*a note 19, p. 23.
[34] Art 7, the Draft Mass Media Proclamation, 2015 (Amharic: Authors' Translation) [On file with authors].

It is important to be cautious against developing legislation that may rapidly become outdated due to an increasingly converged environment. Unfortunately, these draft laws also fail to make substantial shift from the traditional sector-specific regulatory approach. The draft laws neither fill up the existing regulatory gaps nor address the existing overlaps. For instance, 'Ethiopian Mass Media Authority' is empowered to regulate online broadcast but without touching the regulatory functions of the MCIT over telecommunications and information technology services.[35]

Several studies have indicated that radical changes to telecommunication, broadcasting and spectrum allocations laws are necessary because of convergence.[36] But a closer review of the draft laws reveals that the drafters did not carefully weigh the regulatory challenges created by convergence. Consequently, the overlap between the existing regulatory authorities could continue even after the enactment of the new laws.

Furthermore, maintaining the *status quo* will let the uncertainties, gaps and overlaps continue with other emerging services such as e-commerce. Given the rapid pace of development of ICT and digital convergence, it would therefore be worthwhile to reconsider the draft laws so that the drawbacks of convergence do not outweigh its benefits. To this end, it would be appropriate to unify the regulatory authorities dealing with telecommunications, broadcasting and information technology services and modify the respective laws accordingly. In case Ethiopia opts to separate the telecommunications and broadcasting/media authorities, it would be very demanding to ensure the close cooperation and coordination between the two authorities so that they are all focused on the same objectives.

[35] Note that the 'Ethiopian Mass Media Authority', per Art 7(12) of the Draft Mass Media Proclamation, is entrusted with the power to regulate online broadcasts, periodicals and advertisements. Whereas MCIT regulates telecommunications and information technology services as per the Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, Proclamation No. 691/2010 (as amended in 2011).

[36] Republic of South Africa Department of Communications, *A Green Paper on Electronic Commerce for South Africa*, 2000, available at <http://bit.ly/1IIa4WE> (Last accessed on 25 September 2015).

2. Telecoms and the Ethiopian Law

2.1 Overview of the telecom industry in Ethiopia

Owing to their role in the economic and social transformation, the Ethiopian government has made development of telecommunications one of its strategic priorities.[37] Ethiopia's broadband market is projected to significantly rise following massive improvements in international bandwidth, national fiber backbone infrastructure and 3G mobile broadband services.[38] 4G LTE services are also already deployed in Addis Ababa.[39] Ethiopia has made progress in ICTs, particularly with regard to laying out the infrastructure using undersea cables and mobile technologies. Several ICT infrastructure development projects are also underway such as the construction of the Ethio-ICT Village. The village, due to commence operation in the near future, would serve as a technology hub where various tech companies would be allocated spaces to offer their services.[40] A Recent annual report released by the National Bank of Ethiopia claims that in the 2013/14 fiscal year, the number of mobile subscribers surged by 19.2 percent and reached 28.3 million from 23.8 million a year ago.[41] Similarly, the number of fixed line subscribers slightly increased by 2.9 percent from 790,168 to 813,410 while the number of Internet subscribers surged by 39.2 percent on annual basis and reached 6.2 million from 4.4 million recorded the previous year.[42]

Despite all these progresses, however, communications penetration is still lagging behind compared to other African countries and there is the need to bridge the digital divide in Ethiopia. According to the World Bank and World Economic Forum, the underperformance of the Ethiopian telecommunication sector is attributed to the public monopoly and lack of competition.[43] On the other hand, the Ethiopian government takes a firm stand not to open up its telecommunications sector any time soon, the primary reason being that the telecom sector is the primary source of income to finance mega projects such as

---

[37] Federal Democratic Republic of Ethiopia, Ministry of Finance and Economic Development, *Growth and Transformation Plan (GTP) 2010/11-2014/15* , 2010, p. 75

[38] Ethiopia - Telecoms, Mobile and Broadband - Market Insights and Statistics, *Buddecomm*, 28 April 2015, available at <http://bit.ly/1IrQ4ra> (Last accessed on 25 September 2015)

[39] Ethio-telecom Launches the Fourth Generation Long-Term Evolution (LTE) Service in Ethiopia, *Ethio-Teleom Press Release*,12 March 2015, available at <http://www.ethiotelecom.et/> (Last accessed on 25 September 2015).

[40] *See* details at <http://www.ethioictvillage.gov.et/ > (Last accessed on 25 September 2015)

[41] National Bank of Ethiopia, *Annual Report 2013-2014*, 2015, available at <http://bit.ly/1JZDMqh> (Last accessed on 25 September 2015).

[42] *Ibid.*

[43] The World Economic Forum, *The Africa Competitiveness Report 2013*, 2013, available at <http://bit.ly/1aJs39V> (Last accessed on 25 September 2015).

the railway and telecommunication infrastructure development in high-cost rural areas.[44] The government also claims that privatization of the sector will not go in line with the government's development program which aims to expand access to ICT services to all rural areas.[45] According to this line of argument, the incumbent state-owned operator Ethio-telecom is best-placed to promote universal access to communications services.[46]

2.2 Legislative developments

The Ethiopian telecommunications sector is governed by various proclamations, regulations and directives. A close look at these legal regimes reveals that all are tuned by the policy choices of the government. The Ethiopian Investment Proclamation, for instance, provides that private investors are allowed to invest in the areas of telecommunications services but only jointly with the government.[47] Nevertheless, the state owned Ethio-Telecom, is the only service provider in Ethiopia so far. Indeed, the private sector is allowed to participate in resale of some telecommunication services such as airtime vouchers, fax and Internet services through cyber cafés and to provide value added services.

The types of value added services allowed to be provided by the private sector include short messaging services (SMS), payment transaction services, infotainment services, location based services, Call Center Services, and virtual Internet services.[48] To provide these value added services or act as a reseller, obtaining a license from the MCIT and signing service delivery agreement with Ethio-Telecom is required. Licensees are also obliged to interconnect their equipment and systems only with Ethio-Telecom's infrastructure or network, to use equipments approved by the MCIT, and not to provide any service other than the services they are licensed for.[49]

---

[44] Katrina Manson, Ethiopia's Leader aims to Maintain Tight Rein on Key Businesses, *The Financial Times*, 27 May 2013, available at <http://on.ft.com/1F0f0Cc> (Last accessed on 25 September 2015).

[45] Forum for Social Studies, *Public Policy Dialogue on the Delivery of Telecom Services in Addis Ababa*, 2014, available at <http://bit.ly/1F0fGaJ> (Last accessed on 25 September 2015).

[46] Note that Ethio-telecom is a wholly state-owned enterprise established in 2010 by the Council of Ministers Regulation No. 197/2010 with the purpose, among things, to provide and make accessible next generation network based world class standard information technology services. Ethio-Telecom replaced the previous telecom provider Ethiopian Telecommunication Corporation.

[47] Article 6(2), Investment Proclamation No.769/2012.

[48] Ministry of Communications and Information Technology, *Value Added Services License Directive,* Directive No. 3/2011.

[49] *Ibid*; see also Ministry of Communications and Information Technology, *License Directive for Resale and Telecenter in Telecommunication Services Directive,* Directive No. 1/2002.

Of all the legislative developments in this sector, the Telecom Fraud Offence Proclamation is the most recent, and there is some public confusion as to its reach. The major features of this legislation are briefly highlighted below.

2.2.1 The Telecom Fraud Offence Proclamation - A premier

According to the preamble of the Telecom Fraud Offence Proclamation (TFO), (i.e., Proclamation No. 761/2012), its objectives are to: (i) ensure that the telecom sector is promoting peace, democratization and development in Ethiopia, (ii) protect the public monopoly over telecommunications; (iii) safeguard national security, and (iv) bridge existing legal gaps.[50]

The Proclamation was criticized since its draft stage by the media and some Internet activists. Al Jazeera was reportedly the first international media outlet to criticize the Proclamation and claimed that Ethiopia has criminalized the use of Voice over Internet Protocol (VoIP) services such as Skype with up to 15 years of imprisonment.[51] Subsequently, other media outlets and international organizations such as the BBC, Reporters Without Borders, Human Right Watch and Freedom House reiterated the story. Although these reports created much confusion among the public, they were later found to be erroneous.[52] Unlike the reports by internet activists and the media, the Proclamation does not create new criminal offences, as all the criminal offences precede the Proclamation. The Proclamation only reforms existing offences or extends some activities already criminalized under existing laws to telecommunication services. The Proclamation contains 19 provisions out of which nine are substantive criminal rules. Some of the substantive criminal rules of greater importance stipulated under part two of the Proclamation are briefly highlighted below.

a. Offences related to unauthorized telecommunications equipment

The first type of act penalized under the Proclamation concerns unauthorized manufacturing, assembly, import or offer for sale of any telecommunications equipment.[53] This prohibition is not new to the Ethiopian telecommunications legal regime. The now repealed Telecommunication Proclamation No. 49/1996 (as amended in 2002) had prohibited manufacturing, import or distribution of radio communication equipment and TVRO (Television receive only) without

[50] The preamble of the Telecom Fraud Offences Proclamation, *supra* note 10.

[51] Zenebe Beyene and Abdissa Zerai, The Role of ICTs in Governance, State building, and Peace Building in Africa: The Case of Ethiopia, *CGCS Occasional Paper Series on ICTs, State building, and Peace building in Africa No. 2*, 2014, p. 16.

[52] Daniel Berhane, Official: Skype and Similar Activities are not Banned in Ethiopia, *Horn Affairs*, 21 June 2012, available at <http://bit.ly/1PbNgCo> (Last accessed on 25 September 2015).

[53] Art 3 (1), Telecom Fraud Offence Proclamation, *supra* note 10.

prior approval of Ethiopian Telecommunication Agency (Agency).[54] The law had further empowered the agency to specify any other telecommunication equipment that requires prior approval before it may be connected to the telecommunication system.[55]

The principle under the Telecommunication Proclamation No. 49/1996 (as amended in 2002) was, therefore, allowing the manufacture, import, distribution, use or possession of any telecommunications equipment without prior approval unless the equipment is TVRO, radio communication or falls under those specified by the "Agency" to be approved before they may be connected to telecommunication systems.

The TFO Proclamation reversed this approach by requiring prior approval for any telecom equipment unless that equipment falls under the category prescribed by the Ministry of MCIT as not requiring approval. As explained in the explanatory note of the Proclamation, the reason for changing this approach was that the implementation of Telecommunication Proclamation No. 49/1996 had caused practical problems. Since the Agency failed to specify telecommunication equipment that requires prior approval, some people started to import and operate latest telecommunication equipments other than Radio communication and TVRO, and such equipment was found to be dangerous to national security or susceptible of bypassing the telecommunication system.[56] As a result, people who possessed them could not be prosecuted since this would amount to creating a criminal offence not prohibited by law.[57]

But we know little at this point whether the MCIT has prescribed types of approved telecommunications equipment. Even though this appears to be necessary for the enforcement of Article 3 of the Proclamation, no detail information is available at the time of writing. What we do know is that there are several court cases dealing with importing and operating 'illegal' telecommunication equipment, and provision of international calls. For instance on 30 December 2013, the Federal High Court sentenced 7 individuals to rigorous imprisonment ranging from 3 to 12 years for illegally importing and installing telecommunications equipment such as satellite modem and hypermedia gateway that could receive calls from abroad and transmit them to

[54] Art 14 (2) cum Art 14 (4), Telecommunication Proclamation, *supra* note 11. The Proclamation defines TVRO as an 'apparatus used only for reception of satellite television broadcast'.
[55] *Id.*, Art14 (1).
[56] Explanatory note to the Telecom Fraud Offence Proclamation, 2012, p. 5 (On file with authors).
[57] *Ibid.*

recipients of the callers without the knowledge of Ethio-Telecom.[58] It was also reported that Ethio-Telecom lost Birr 5,356,569 due to these frauds.[59] Similarly, additional eleven individuals including foreigners were accused on similar activities on 29 November 2014 for causing loss of over USD 11 million to Ethio-telecom.[60]

b. Offences related to the provision of telecommunication services or operators

The provision of telecommunication service without license, the provision of call back service and bypassing Ethio-Telecom are criminalized under the Telecom Fraud Offence Proclamation.[61] These offences also had been regulated under the predecessor telecom legislation which prohibited engaging in 'private or commercial telecommunication services' without a license.[62] Art 4 of the Proclamation excluded the prohibition on the "private use of telecommunication service without license", and rather aggravated the penalties for "commercial telecommunication services" without license. The wordings of Art 4 'whosoever provides telecom service without license' implied legalizing licensed private telecommunication services. Nevertheless, the practice reveals otherwise since license is allowed only for value added services and resale of some telecommunications service as noted above.

The Telecom Fraud Offence Proclamation made amendments to offences concerning the provision and use of call back services[63] which, again, were already prohibited by the Telecommunications Proclamation No. 49/1996 (as amended in 2002). The penalty under the Telecommunications Proclamation for the use or provision of call back services was 2 to 5 years of imprisonment and a fine of up to Birr 10,000.[64] It further treated the 'use 'and 'provision 'of call back service separately, perhaps because penalizing these acts in the same manner would be not justifiable.

---

[58] *Court sentences, Fines Offenders for Corruption,* The Federal Ethics and Anti-Corruption Commission of Ethiopia Press Release, 2013, available at <http://bit.ly/1JZKaxO> (Last accessed on 25 September 2015).

[59] *Ibid.*

[60] Fasikaw Tadesse, 11 Individuals Accused of Telecom Fraud, *Fana Broadcasting Corporate*, 29 January 2015, available at <http://bit.ly/1PyJhAb> (Last accessed on 25 September 2015) [Amharic: Authors' Translation].

[61] Arts 4, 8 and 9, Telecom Fraud Offence Proclamation, *supra* note 10.

[62] Art10 (1) cum Art 24 (4), Telecommunication Proclamation, *supra* note 11.

[63] Note that 'call back services' are defined under Art 3(2) of the telecom fraud offence law as 'the use of dial tone of a foreign telecom operator for international connection without the knowledge of the domestic telecom operator or fraudulently making international calls into apparent domestic calls and shall include services that are identified as call-back by the international telecommunication union'.

[64] Art 25 (1), the Telecommunication Proclamation, *supra* note 11.

The Telecom Fraud Offence Proclamation has raised the punishment for the provision of call back services from 5 to 10 years of imprisonment, as opposed to imprisonment from 2 to 5 years in the previous law. The fine upon the violation of the provision of call back services is also raised from a maximum of Birr 10,000 to the equivalent of 5 times the unauthorised income earned during the period of service provision. On the other hand, the Proclamation reduced the penalty for "use" of call back service from sentences of between 2 and 5 years and a fine of up to Birr 10,000 to sentences of between 3 months and 2 years and a fine of between Birr 2,500 and Birr 20,000.[65]

Another criminal offence stipulated in the Proclamation concerns illegal telecom operators. Under Art 9(1) of the Proclamation, it is prohibited to: (a) establish any telecommunication infrastructure other than that established by Ethio-Telecom; and (b) bypass the telecommunication infrastructure and provide domestic or international telecommunication services. Imprisonment for such criminal offences is between 10 years and 20 years, with a fine equivalent to ten times the revenue estimated to have been earned from the illegal activity. This severe penalty demonstrates the commitment of the government to preserve public monopoly over telecommunications. The Proclamation also penalizes the use of telecommunications services provided by illegal operators with imprisonment from 3 months to 2 years, and fine between Birr 2,500 to Birr 20,000.[66]

c. Offences related to telephone Call Services through the Internet

In Ethiopia, telephony services through the Internet also called voice over Internet services were initially criminalized for the first time by the 2002 Telecommunication Proclamation.[67] This prohibition, however, came to public awareness when the draft Telecom Fraud Offence Proclamation was enacted and drew sever admonishment from rights groups, activists and the media.

Although the Ethiopian government had tried to convince the public that the reports were untrue and voice over Internet services are not banned in Ethiopia, it continued to create much uncertainty among the public who make use of voice over Internet services including Skype, GoogleTalk, Viber, whatsapp and so on. It also remained the main, among others, basis for international human right groups who report on the state of Internet freedoms in Ethiopia. This sub-section briefly highlights how the Telecom Fraud Offences Proclamation treats VoIP services in comparison with the approach of other countries.

[65] Art 8(2), the Telecom Fraud Offence Proclamation, *supra* note 10.
[66] *Id.*, Art 9(2).
[67] Art 24(3), the Telecommunication Proclamation, *supra* note 11.

How other countries treat voice over Internet services

Different countries regulate VoIP services in different ways depending on their prevailing public policy. The current regulatory treatment for voice over Internet services ranges from complete prohibition to unconditional permissibility.[68] According to a guideline document on VoIP (Voice over Internet Protocol) adopted by the South Asian Telecommunications Regulator's Council (SATRC), VoIP services are usually regulated in different ways in SATRC member countries.[69] For instance, while VoIP is allowed only for licensed Internet protocol telephony service providers in Bangladesh and Bhutan, Maldives allows VoIP only for personal and individual use, but not open to be provided as a telecom service by operators.[70] On the other hand, VoIP is legal in India but it is illegal to have VoIP gateways inside the country.[71] From the SATRC member countries, it is only Afghanistan that prohibits VoIP service.[72]

Other countries outside the SATRC member countries also regulate VoIP services in different ways. For instance in South Korea, only providers registered with the government are authorized to offer VoIP services and reports show that South Korean regulators have decided to let mobile operators charge users extra fees for VoIP applications or block their use entirely.[73] Likewise, in the United States, the Federal Communications Commission requires all interconnected VoIP service providers to comply with requirements such as the universal service contribution and emergency services.[74] VoIP providers are also subject to different regulatory framework in European Union (EU) countries such as to contribute for universal service obligation fund.[75]

The Regulatory Treatment of VoIP in Ethiopia

As stated above, the regulatory treatment of VoIP varies from jurisdiction to jurisdiction depending on prevailing market conditions and relevant national legislations. In the Ethiopian case, the close reading of the current legislation

---

[68] See South Asian Telecommunications Regulators' Council, *SATRC Guideline on Key Regulatory Issues on Voice-Over-IP in SATRC Countries*, 2012, p. 24.

[69] *Ibid.*

[70] *Ibid.*

[71] *Ibid.*

[72] *Ibid.*

[73] The International Telecommunications Union, *ICT Statistics News Log - Regulators Enable Mobile Operators to Charge More Fees for VOIP (South Korea)*, 2012, available at <http://bit.ly/1RskbkS> (Last accessed on 25 September 2015).

[74] Nathaly Rey, *Ruling Voice over IP Challenges for Regulators in Latin America*, The International Telecommunication Union, The Future of Voice Project, 2006. Available from: <http://bit.ly/1cFreHf> (Last accessed on 25 September 2015).

[75] European Commission, *The Treatment of Voice over Internet Protocol (VOIP) under the EU Regulatory Framework, An Information and Consultation Document*, 14 June 2004, p. 10.

suggests that VoIP services are neither completely prohibited nor unconditionally permitted. They are rather prohibited in a qualified manner. Art 10 of the Telecom Fraud Offence Proclamation is relevant to this issue which stipulates:

> '(3) Whosoever provides telephone call or fax services through the Internet commits an offence and shall be punishable with rigorous imprisonment from 3 to 8 years and with fine equal to five times the revenue estimated to have been earned by him during the period of time he provided the service'.
>
> '(4) Whosoever intentionally or by negligence obtains the service stipulated under sub-article (3) of this article commits an offence and shall be punishable with imprisonment from 3 months to 2 years and with fine from Birr 2,500 to Birr 20,000'.

It is worthy at this juncture to compare the 2002 legislation and the Telecom Fraud Offence Proclamation as this may shed some light to what degree VoIP is banned in Ethiopia. Even the private use of VoIP was illegal under the 2002 legislation but has been tolerated under the TFO Proclamation. Art 24 (3) of the Telecommunication Proclamation No. 49/1996 (as amended in 2002) provided that *"the use or provision of voice communication or fax services through the internet are prohibited."* Either providing or using these services was punishable from 2 to 5 years and fine up to Birr 10,000.

While the 2002 legislation completely banned "the use or provision of voice communication" services through the Internet, the Telecom Fraud Offence Proclamation outlaws unauthorized 'provision of telephone call' services and "obtaining the service" from those illegal providers. The issue of outlawing VoIP services in Ethiopia must also be put into context. Given the prevailing public policy and market conditions in the country, Ethio-telecom is the sole service provider. Private investment in the sector is not allowed except for value added and resale services. The prohibition of 'providing telephone calls services' should, therefore, be construed in light with this market and public policy condition. Concomitantly, we can make the following points.

First, the Telecom Fraud Offence Proclamation does not ban VoIP services categorically. Rather, it forbids unauthorized "provision of telephone call" services and "obtaining the services" from illegal providers. As the law currently stands, the use of VoIP is not forbidden in Ethiopia unless the service is obtained intentionally or by negligence from unauthorized providers as stipulated under Art 10(3). Secondly, as opposed to the total ban of 'voice communication' (including personal computers to other personal computers) under the 2002 legislation, the wording of Art 10 (3) of the TFO Proclamation which refers to 'telephone call' implies that the Proclamation prohibits only telephone call services to a landline or mobile phone. The wording of Art 10(3)

that singles out 'telephone call' from 'voice communication' could not be accidental. [76]

Moreover, Art 10(3) should be read cumulatively with Arts 2, 4 and 9 of the Proclamation. Given the broader definitions under Art 2(1) of the Proclamation, it could even be argued that Ethiopia treats VoIP services as telecommunication service and not as computer-based 'information service'. And, hence VoIP is subject to same regulation as public switched Telephone Network (PSTN) or traditional telecom services. Furthermore, establishment of any telecom infrastructure other than the infrastructure established by Ethio-telecom or by-passing the same is not allowed under Art 9 of the Proclamation. Consequently, the cumulative reading of these provisions suggests that the Proclamation forbids not VoIP as such but unauthorised VoIP service providers or those who bypass the telecom infrastructure to provide domestic or international telecommunications services. Clearly, VoIP operators are in competition with the traditional telecom operators in many countries, and Ethiopia is merely prohibiting the heralding of such competition based on the prevailing public policy in the country.

There is practical evidence which demonstrates that Ethiopia is not banning VoIP, but is rather investing to expand the service. Ethio-Telecom, has deployed 4G LTE services in Addis Ababa which enables customers to make Mobile VoIP Calls at a fraction of the price of traditional mobile.[77] This latest technology does not support traditional circuit-switched telephony service, but all-Internet Protocol (IP) based communication services. Article 10 of the Proclamation is not, therefore, a redundancy to the 2002 legislation, it is rather a sort of reform which makes it even more progressive than the 2002 legislation.

Since the uncertainty about the regulation of VoIP in Ethiopia has not vanished, it would be necessary to rewrite the law in clear terms and make sure that the regulation of VoIP does not hamper investments, decrease business competition, retard technological growth, and prevent consumers from having access to better services. It is also vital to note that regulating VoIP in the same manner as the Public Switched Telephone Network (PSTN) is impractical due to the different technology used for VoIP services.[78]

---

[76] Samson Yoseph, Ethiopia's Ban on Skype: An Excessive Stretch, *Circle ID*, 20 June 2012, available at < http://bit.ly/1JZQIfV> (Last accessed on 25 September 2015).

[77] See details at <http://www.ethiotelecom.et/> (Last accessed on 25 September 2015).

[78] Jimar Sanders, Voice over Internet Protocol: An International Approach to Regulation, *Georgia Journal of International and Computer Law*, Vol. 35, 2004, p. 593.

3. Cybercrime and the Ethiopian Law[79]

3.1 An overview of Ethiopian Cybercrime Law

As noted above, the pioneering set of cybercrime rules in Ethiopia are introduced as part of the Criminal Code of 2004.[80] The Code penalizes a short list of computer crimes most notably computer hacking, spreading malware and DoS attacks.[81] It also criminalizes acts committed with the view to 'facilitate the commission of computer crime'.[82] There are two basic common threads among these cybercrime rules. One is that all of the listed crimes, except the fourth one – adding and abetting commission of computer crime – are punishable when committed both intentionally and negligently. Second, they are punishable when the perpetrator acted in the absence of any authorization to do so – 'without authorization' as the law calls it. Notably, this feature does not apply to the fourth type of computer crime under the Code.

The law restricts its scope only when the act was committed 'without authorization'. This means that potentially punishable acts that are done by 'exceeding authorization' that is already given are not punishable under the Code. The draft cybercrime legislation, however, changes this and renders the act publishable if it done 'without authorization' or 'by exceeding authorization' already granted by law, contract or practice.[83] Also notable about the cybercrime rules is that they are all punishable, not only when perpetrated against a standalone computer, but also against a computer system and computer network.

---

[79] Note that the discussion under this section is partly adapted from the lead author's article, Kinfe Micheal Yilma (2014), Developments in Cybercrime Law and Practice in Ethiopia, *Computer Law and Security Review*, Vol. 30, No. 6, pp. 720-735.

[80] Etymologically, cybercrime – also called Internet crime, high-tech crime, computer crime or online crime – is a portmanteau for crimes committed within or through cyberspace. Cybercrime is broadly defined to cover all ways in which computers and other types of portable electronic devices such as cell phones and PDAs capable of connecting to the Internet are used to break laws and cause harms. *See* Samuel McQuade, III, Editor (2009), *Encyclopedia of Cybercrime*, Greenwood Press, p. 43; *see* also Vagelis Papakonstantinou, Cyberspace and Cybercrime, *in* Hamid Jahankhani and *et al* (eds.), *Handbook of Electronic Security and Digital Forensics*, World Scientific Publishing Co., 2010, pp. 455-457. The root term cyberspace refers to a computer-generated public domain which is said to have neither territorial boundaries nor physical attributes. *See* Brian Loader, Editor (1997), *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, Routledge, p.1. Note that the nomenclatures 'cybercrime and computer crimes' are interchangeably used throughout this article although the Ethiopian law uses the terms computer crimes.

[81] Arts 706, 707 and 708 respectively, Ethiopian Criminal Code, *supra* note 9.

[82] *Id.*, Art 709.

[83] The Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12.

The cybercrime rules in the 2004 Criminal Code are slightly outdated due to changes that have occurred in the field of cybercrime since the enactment of the Code. This has recently prompted the Ethiopian government to draft modern and comprehensive cybercrime legislation. The limitations of the Code are mainly threefold. *Primarily*, the Code criminalizes only three items of cybercrimes and hence does not address new varieties of the offence. In addition to common forms of cybercrime such as hacking, spreading malware and DoS attacks, a range of new cybercrimes have emerged in the wake of the enactment of the Code. This is said to have rendered these rules inadequate in the wake of economic, social and political risks posed by cyber-attacks.[84] Related to this, recent digitization efforts and expansion of ICT infrastructure meant higher vulnerability to cyber threats which could not adequately be addressed by the narrowly defined rules of the Criminal Code.[85]

Secondly, the computer crime rules of the Code do not provide tailored procedural and evidentiary provisions that would be necessary in the investigation and prosecution of such offences.[86] As the Code currently stands, the basic rules of criminal procedure, enacted as far back as 1961, continue to apply to computer crime regulation. Worse still, Ethiopia has not codified its evidence law proper other than a set of rules scattered across various pieces of legislation. Such procedural and evidentiary rules are too outdated to be applied to the cybercrime given the peculiarity and novelty of these online crimes.

Thirdly, the cybercrime rules of the Code were not crafted to take full account of the cross-border nature of this form of criminal behaviour and the need for international cooperation in the prevention, investigation and prosecution of cybercrime.[87] Indeed, post enactment of the Code saw formation of international as well as regional treaties on cybercrime. This in turn required Ethiopia to adopt the requisite legal framework as part of the regional and global efforts against cybercrime.[88]

Besides the computer crime law proper, cybercrimes are also addressed in other Ethiopian laws. A case in point is 'cyberterrorism' regulated under the controversial anti-terrorism legislation which makes cyberterrorism a punishable

[84] Explanatory Note to the Draft Proclamation to Legislate, Prevent and Control Computer Crime, July 2013, p. 2 (Amharic: authors' translation) [On file with the authors]; see also Preamble of the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12, para 3.

[85] *Id.*, p. 4.

[86] *Id.*, p. 3; see also the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12, para 4.

[87] *Ibid.*

[88] *Ibid.*

offence.[89] It penalizes endangering, seizing, putting under control, causing serious damage to or disruption of electronic information communication services.[90] The telecom fraud offence legislation also contains a handful of telecom offences that technically resemble typical cybercrimes. These offences are 'unlawful interference', 'unlawful interception' and 'illegal access to a telecom network, telecom system or telecom services'.[91] The telecom fraud offence law defines 'telecom services' broadly to include, among others, Internet service and data communication services, and this makes telecom offences fall within the category of cybercrimes.[92] These offences are similar to cybercrimes such as 'illegal access to a computer system', 'interference with a computer system' and 'illegal interception' which is punishable under the draft cybercrime law.[93]

3.2 Major reforms under the Draft Cybercrime Law

Three significant reforms are introduced by the draft computer crime law. The *first* is that it adds a range of new cybercrimes into the statute book. It puts computer crimes into four major categories: 'crimes against computer system and data'; 'computer-related forgery, fraud and theft'; 'illegal content data'; and 'miscellaneous computer offences'. Whilst Category I retains the four computer crimes already regulated under the 2004 Criminal Code, it also introduces 'interception of private communications' as a new crime.[94] This crime concerns intentionally intercepting 'non-public communication services' without authorization or in excess of authorization.[95]

All the remaining categories introduce new computer crimes currently unregulated under the Criminal Code. Under category II, computer-related forgery, fraud and identity theft are categorically punishable.[96] Child pornography, spamming, online defamation, intimidation and crimes against public security are all made punishable under Category III.[97] The last category contains miscellaneous crimes namely, 'breach of duty and hindrance of

[89] Art 3(6) cum Art 2(7), Anti-Terrorism Proclamation, *Federal Negarit Gazeta*, Proclamation No. 652/2009.
[90] *Ibid.*
[91] Art 5, Telecom Fraud Offence Proclamation, *supra* note 10.
[92] *Id.*, Art 2(1).
[93] Arts 3-4 and 6, the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12.
[94] *Id.*, Art 6.
[95] *Ibid.*
[96] *Id.*, Arts 8 – 10.
[97] *Id.*, Arts 11 – 14.

cybercrime investigations', 'liability of juridical persons' and 'liability of Internet service providers'.[98]

The *second* major reform introduced by the draft cybercrime legislation is the provision of detailed procedural and evidentiary rules that are vital in investigating and prosecuting computer crimes. Under the Criminal Code, rules of procedure and evidence applicable to other types of crimes apply to cybercrimes. While Ethiopia, as indicated earlier, never had codified evidence law proper (other than rules of evidence scattered in various laws), the 1961 Criminal Procedure Code does not address the cybercrimes of the digital age as it was adopted over 50 years ago.[99] In response to this state of affairs, the draft law provides procedural and evidentiary rules, particularly on admissibility of electronic evidence, preservation and production of electronic data and search and seizure of computer data.[100]

The *third* important aspect of the draft law is that it contains a definitional provision that defines a set of technical concepts, as opposed to the 2004 Criminal Code which is devoid of such definitions. This is particularly important because certain computer-related concepts would inevitably be technical to judges, who have to apply them in real cases. It, for instance, defines terms such as 'communication service', 'computer system', 'computer data', 'computer program', 'traffic data', and 'network'.[101]

Finally, another notable feature of the draft law is that most of the crimes are punishable when they are committed intentionally and therefore only a few cybercrimes are punishable when committed negligently. The drafters justify this position taken under the draft on grounds of low level of ICT literacy in Ethiopia and the likelihood of a potentially higher number of criminal acts committed as a result of the gullibility of users.[102] Moreover, penalizing negligent acts would mean punishing unsuspecting 'newbies' to technology. Certainly, this view holds water given the fact that only recently have computers and the Internet become more accessible in Ethiopia.

---

[98] *Id.*, Arts 15 – 17.

[99] Criminal Procedure Code of the Empire of Ethiopia, *Negarit Gazeta,* Proclamation No. 185/1961.

[100] Arts 18 – 22, the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12.

[101] *Id.*, Arts 2(1-4), 2(6-7).

[102] Explanatory Note to the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 84, p. 4.

3.3 The institutional framework for cybersecurity in Ethiopia

The MCIT is the principal government organ in charge of ICTs in general. It has the powers and duties to initiate policies and laws in ICT areas.[103] The MCIT also sets and implements standards to ensure provision of quality, reliable and safe ICT services.[104] The Ministry is, therefore, the principal policy organ concerning cybersecurity in general and cybercrimes in particular. Each regional state has, however, its own Communications and Information Technology Agency entrusted with implementing on the ground laws, policies and standards on ICTs adopted at the federal level. The Ethiopian Information Network Security Agency (INSA) is a parallel organ with statutory powers to formulate national policies, laws and standards to ensure security of information and computer based key infrastructure and oversee its enforcement.[105]

Whilst the Ministry is bestowed with the broader mandate in connection with ICTs regulation in general, INSA is specifically dedicated to deal with information security. In so far as initiation of legislation is concerned, the MCIT has so far drafted E-commerce legislation (in cooperation with UN Economic Commission for Africa), and INSA has recently drafted comprehensive computer crime legislation.[106] Lawyers at INSA have played a key role in the crafting of the telecom fraud offence law. Moreover, the Agency claims that it saved the country substantial costs over the past few years, in particular by prosecuting telecoms fraudsters.[107]

With respect to cyber policing and enforcement, the Federal Police Commission has the primary responsibility to investigate crimes relating to 'information network and computer systems'.[108] This no doubt relates to investigation of cybercrimes committed against or through information networks and computer systems. INSA also assumes significant powers in taking all the necessary 'countermeasures' to defend cyber or electromagnetic attacks on information and computer based infrastructures, or on citizens' psychology.[109]

---

[103] Art 10 (1(a)) cum Art 24, Proclamation to Provide for the Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, *supra* note 30.

[104] *Id.*, Art 24(1/b).

[105] Art 6(2), Information Network Security Agency Re-establishment Proclamation, *Federal Negarit Gazeta*, Proclamation No. 808/2013.

[106] Note that both of these bills are at a draft stage at the time of writing.

[107] See Interview with Director of INSA, Brigadier General Teklebirhan Weldearegay, *Zemen Magazine*, December 2012, pp. 15-18 (Amharic: authors' translation).

[108] Art 6(5), Ethiopian Federal Police Commission Establishment Proclamation, *Federal Negarit Gazeta*, Proclamation No. 720/2011.

[109] Art 6(4), Information Network Security Agency Re-establishment Proclamation, supra n 105.

Moreover, it provides assistance and support in respect of preventing and investigating cybercrime, to (federal) police and other organs empowered by law.[110] The draft computer crime proclamation gives both the Federal Police and INSA enforcement powers with a leadership role to be assumed by the Federal Police Commission which shall establish a special 'cyber unit'.[111]

The National Intelligence and Security Service (NISS) has some generic powers that might be construed as covering the right to investigate cybercrimes. It, for instance, has the power to 'follow up and collect intelligence and evidence on other serious crimes which are threats to the national interest and security', and to work in collaboration with other relevant organs.[112] Given the potentially serious damage that cybercrime causes particularly when committed against critical infrastructure, it is likely that NISS might be involved in the investigation of cybercrimes especially in collecting intelligence on cybercriminals. Yet, it might be necessary to empower various organs in the investigation of cybercrime, and it is equally important to provide details (in subordinate rules) with regard to the requisite institutional coordination that must exist between these organs to ensure that they all work towards the same goal.

The constitutional devolution of judicial power is also based on the federal arrangement. The law that determines the judicial power of federal courts provides that federal courts shall have criminal jurisdiction, among others, over offences regarding the 'security and freedom of communication services' operating within more than one region or at the international level.[113] The terminologies apparently capture communication services and networks such as the Internet. With regard to federal courts, the law confers upon the Federal First Instance Court – the initial tier of federal courts – the jurisdiction to try the criminal acts indicated under Art 4(7) of the Federal Courts Proclamation, including cybercrime.[114] In contrast, the Federal High Court is given first instance jurisdiction to try computer crimes under the draft computer crime legislation.[115]

---

[110] *Id.*, Art 6(7).

[111] Art 23, the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12.

[112] Art 8(6), National Intelligence and Security Service Re-establishment Proclamation, *Federal Negarit Gazeta*, Proclamation No. 804/2013.

[113] Art 4(7), Federal Courts Proclamation, *Federal Negarit Gazeta*, Proclamation No. 25/1996.

[114] *Id.*, Art 15(1).

[115] Art 26, the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12.

A cursory reading of Art 4(7) of the Federal Courts Proclamation implies that regional state courts may adjudicate cybercrime cases that are committed within their own territories, so long as the crimes do not have any spill-over effect on other neighbouring regional states or even countries. However, state judicial jurisdiction on cybercrime is to be set out by the respective court proclamation of each regional state. In practice, there is no much clarity on the jurisdiction of regional courts in entertaining cybercrime cases.

For instance, the Southern Nations, Nationalities and Peoples Regional State (SNNPR) Courts Proclamation is vague, if not silent, on the jurisdiction of regional courts in cybercrime cases. It generally provides that 'regional courts have jurisdiction over regional matters except those expressly reserved to federal courts'.[116] The conclusion that can be derived from this provision is that the competent court of that state will entertain the case if a cybercrime incident takes place within the regional state. However, the level of court in the regional state which entertains cybercrime cases is not clear under the law.

4. Electronic Privacy and the Ethiopian Law[117]

Ethiopia does not have laws that are specifically designed to deal with privacy in general and electronic privacy in particular except a few set of rules contained in various pieces of legislation that guarantee the right to privacy in an indirect fashion. The 1995 Constitution of the Federal Republic of Ethiopia prohibits all forms of intrusion into private communication. It provides that 'everyone has the right to the inviolability of his […] correspondence including […] communications made by means of telephone, telecommunications and electronic devices.'[118]

International human rights treaties ratified by Ethiopia such as the International Covenant on Civil and Political Rights (ICCPR) are also relevant given that their relevant privacy provisions have been interpreted in the context of the present digital reality.[119] More importantly, Ethiopia is likely to ratify the recently adopted African Union (AU) Convention on Cybersecurity and

[116] Art 3(1), Revised Southern Nations, Nationalities and Peoples Regional State Courts Proclamation, *Debub Negairt Gazeta*, Proclamation No. 43/2002.

[117] Note that a few paragraphs of this section are partly drawn from the lead author's article, Kinfe Micheal Yilma (2015), Data Privacy Law and Practice in Ethiopia, *Journal of International Data Privacy Law,* Vol. 5, No. 3, May 2015, pp. 179-182.

[118] Art 26 (2), The Federal Democratic Republic of Ethiopia Constitution, *Federal Negarit Gazeta*, Proclamation No. 1/1995, 21 August 1995.

[119] *See*, for instance, Human Rights Committee, *General Comment 16: Article 17 (Right to Privacy),* U.N. Doc. HRI/GEN/1/Rev.1, 8 April 1988, para 8.

Personal Data Protection which deals with electronic privacy at length.[120] This would ultimately make the Convention part of the Ethiopian law thereby adding a new body of privacy law.

Although enacted in the pre Internet era, subsidiary instruments such as the Ethiopian Civil Code also have bearings on electronic privacy. The rules that guarantee personality rights such the 'the right to inviolability of correspondence' and 'the right to one's image' could possibly be read in the context of the Internet.[121] Interestingly, the right to one's image has recently been invoked before the Cassation Division of the Federal Supreme Court, although not in the context of electronic privacy.[122]

The freedom of information law also has rules that could potentially safeguard electronic privacy. While recognizing the right of every citizen to have access to information held by public bodies, it provides that such rights may be restricted should 'public' and 'private' (sic) interests so require.[123]According to this rule, in order to protect the privacy of individuals, public bodies 'may' deny access to public records that may contain personal information. The law further provides that concerned public record officers must reject requests for 'personal information' where disclosure of such information may constitute 'unreasonable' disclosure.[124]

What is commendable about the freedom of information law is that it has very crucial notification and intervention rules by which a data subject – the person about whom data is requested – will be notified of any requests made with respect to information that he declared confidential, and s/he will be allowed to intervene to protest disclosure of his information.[125] The law has another category of information whose disclosure may be restricted as 'confidential information', which include information provided to the public body under contractual confidentiality agreements and which may not be disclosed except with the consent of the data subject.[126] The freedom of information law is the only legislation in Ethiopia that contains a comprehensive and lengthy definition of 'personal information'.[127]

---

[120] Arts 8-23, Chapter II, *The African Union Convention on Cybersecurity and Personal Data Protection*, AU Doc. EX.CL/846(XXV**)**, 27 June 2014.

[121] Arts 27-28 and 31, Ethiopian Civil Code, *Negarit Gazeta*, Proclamation No. 165/1960

[122] Ethiopian Supreme Court Cassation Division: *Riyan Miftah v. Elsewdi Kebels Plc* [2013] File No. 91710.

[123] Art 11(1), Freedom of Mass Media and Access to Information Proclamation, *Federal Negarit Gazeta*, Proclamation No. 590/2008.

[124] *Id.*, Art 16.

[125] *Id.*, Art 19.

[126] *Id.*, Art 18.

[127] *Id.*, Art 2(8).

The law also implicitly embodies some basic data protection principles. For instance, while requiring public bodies (*de facto* data controllers) to maintain public records in accordance with the code of practice issued by the Ombudsman, it implies what is called the 'principle of data security'.[128] The 'principle of data quality' is also latent in the law where it provides that public bodies or data controllers shall make sure that corrections are made on personal information kept.[129] Also to be inferred from the law is the 'principle of individual participation' as the law requires public bodies to notify data subjects when requests for data concerning them are made and they would be invited to a lodge protest, if need be.[130]

The Ethiopian Criminal Code of the 2004 is perhaps the most important legislation that deals with electronic privacy in a more direct fashion. Among others, the Code penalizes violation of the privacy of correspondence' including electronic communications.[131]This offence is punishable only upon complaint and accusation – i.e. only where victims lodge complaints to the authorities.[132] Cybercrime rules of the Criminal Code also have some bearing on electronic privacy. More particularly, the provisions that penalize hacking and cracking of computers, computer systems and computer networks are basically meant to protect electronic privacy.[133]

Another important legislation is the advertisement proclamation which recognizes the need to regulate certain advertisements since they may harm the 'rights and interests of individuals' – including electronic privacy.[134] The law explicitly provides that unsolicited advertisements sent to subscribers' telephones shall be prohibited unless the subscriber has consented in advance.[135] In effect, the law adopts what is elsewhere called 'opt-in' approach of communications by which electronic communications must be addressed to individuals only after consent is secured *a priori*. The law, however, carves out an exception to those advertisements addressed by the telecom provider Ethio-Telecom itself and public advertisements.[136] Given that most advertisements sent over to subscribers are from Ethio-Telecom itself, we suggest that the exception should rather be restricted only to those relevant and perhaps mandatory service advertisements other than every commercial and sometimes

[128] *Id.*, Art 38.
[129] *Id.*, Art 38(3).
[130] *Id.*, Art 19.
[131] Art 606, Ethiopian Criminal Code, *supra* note 9.
[132] *Ibid.*
[133] *Id.*, Art 706; see also Yilma, *supra* n 79, pp. 725-726.
[134] Para 3, Preamble, Advertisement Proclamation, *supra* note 28.
[135] *Id.*, Art 22(2).
[136] *Ibid.*

political advertisements and communications of the telecom provider. Moreover, there should be an option for a subscriber to 'opt-in' at the time of subscription or to 'opt-out' at a later stage.

Regrettably, the law fails to explicitly regulate unsolicited communications through electronic mail – also called spam. Yet, it includes 'telecom' and 'Internet website' among the channels through which advertisements could be disseminated to the public.[137] The reference to 'Internet website, albeit ambiguous, could be understood to mean advertisements set over web-based emails while the term 'telecom' clearly includes dissemination of advertisement through phones. Interestingly, the draft cybercrime law criminalizes dissemination of commercial advertisements through e-mail and further sets forth exceptional circumstances where spamming will not be punishable.[138]

The initiative to regulate spam is commendable on its own although most spam destined to emails are from overseas and indeed from those highly sophisticated spammers. The challenge ahead is thus formidable as policing and prosecuting such offenders would require significant technological and institutional readiness. In this light, the proclamation defines its scope in a feasible manner that covers only advertisements sent via websites hosted in Ethiopia or abroad but by a person residing or an organization incorporated in Ethiopia.[139]

The draft data protection legislation also has significant bearings on electronic privacy.[140] Overall, the draft legislation is a detailed instrument that addresses a range of issues related to electronic privacy such as the definition of key terminologies including personal data and processing of data, jurisdictional rules, a list of data protection principles, rights of data subjects, rules on notification procedures by data controllers, and enforcement provisions.[141] As the bill currently stands, it is crude and needs refinement before enactment, but it could certainly serve as a good starting point.

---

[137] *Ibid*. These references are simply inaccurate as there is nothing as such called 'Internet website'. Both terms, although related, are slightly different. The term 'Internet' refers to both the physical and technical infrastructure through which content – the web – runs. Metaphorically, the Internet denotes the bones and the veins whereas the web represents the blood that runs through them.

[138] Art 14, the Draft Proclamation to Legislate, Prevent and Control Computer Crime, supra n 12; these exceptions are: (i) where there is prior consent from the recipient, or (ii) where the primary purpose of the advertisement is to introduce existing users or subscribers with new products or services, or (iii) where the advertisement contains valid identity and address of the sender, and valid and simple way for the recipient to reject or unsubscribe receipt of further advertisement from the same source.

[139] *Id.*, Article 3(3).

[140] Draft Ethiopian Data Protection Act, *supra* note 12.

[141] *Ibid.*

Adopting a comprehensive data protection law would be beneficial on many fronts. One is that it would help in bringing under one roof rules on data privacy that are presently scattered in different pieces of legislation, thereby making them more accessible. Secondly, it would appropriately set out the relevant elements of a data protection regime such as principles of data protection, rules of collection, processing, data retention, and transfer of personal data. It would also be the right instrument to establish an independent data protection authority that oversees implementation of the data protection rules. Any upcoming data privacy law could draw useful lessons from benchmark instruments such as the Council of Europe Data Protection Convention 108,[142] the EU Data Protection Directive 95/46,[143] and OECD Guidelines on Privacy and Cross-border Flow of Personal Data.[144]

5. Electronic Commerce and the Ethiopian Law

The advent of open electronic networks such as the Internet has dramatically transformed the way of doing business. The Internet has come to a new global marketplace and presents unique opportunities for customers and business in all sectors. It creates new businesses, new channels of distribution and new methods of reaching the customer.[145] E-commerce is rapidly growing worldwide and its potential to transform the landscape of the economies of both the developed and developing countries has been recognized.[146] Accordingly, governments around the world have enthusiastically embraced e-commerce as a positive development that should be encouraged; and numerous governments have pledged to foster e-commerce is a major public policy objective.[147]

As the full potential of the Internet is not explored by Ethiopian companies and consumers, e-commerce in Ethiopia is at the early stage of development. Only banks and few other companies are familiar with e-commerce. And hence,

---

[142] *Council of Europe Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data*, ETS 108, 28 January 1981.

[143] *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, OJ L281/31, 1995.

[144] OECD on Privacy and Cross-border Flow of Personal Data, C(80)58/FINAL, 2013

[145] European Commission, Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signature and Encryption, COM (97) 503 final, 08.10.1997, para 1.

[146] The Federal Republic of Ethiopia Ministry of Capacity Building, *The National ICT for Development (ICT4D) Five Years Action Plan for Ethiopia [2006 – 2010],* Draft Version 4.02, 2006, p. 7.

[147] Thomas Smedinghoff and Hill Bro (1999), Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce, *The John Marshall Journal of Computer and Information Law*, Vol. 17 , p. 725 .

cash is still the most dominant medium of exchange in the country. Lack of conducive legal and regulatory environment is identified among the barriers to the development of e-commerce in Ethiopia by the relevant policy documents of the country such as the National ICT for Development (ICT4D), Five Years Action Plan for Ethiopia (2006–2010), National ICT Policy of 2009, National Information Security Policy of 2011,[148] and the Growth and Transformation Plan (GTP) (2010/11-2014/15).

The creation of enabling legal, regulatory and institutional frameworks is the primary strategic recommendation of the World Bank for ICT-enabled transformation in Ethiopia.[149] In this regard, the World Bank has recommended the enactment of legal frameworks that address several electronic transaction issues such as digital signature, electronic identification, electronic payment, and cybersecurity.[150] At the time of writing, Ethiopia has not yet set a comprehensive legal framework for e-commerce and related legal matters. This section explores the major legal challenges associated with e-commerce in Ethiopia and highlights the defining features of recently drafted e-commerce legislation.

5.1 Major legal challenges for e-commerce in Ethiopia

When parties to a transaction use electronic records to replace paper and employ an electronic medium as the mode of communication, they face unique legal and security concerns. For instance, data messages could be intercepted and manipulated, the validity of documents could be denied, and personal data could be illicitly collected.[151] In addition to the absence of new legislation commensurate with new technological developments, existing legal traditions also create barrier to conducting transactions in electronic form.

The first fundamental legal concern caused by online transaction concerns the legality and enforceability of the transaction.[152] This legal concern emanates from the fact that existing laws governing business and evidentiary issues are designed primarily to facilitate paper-based transactions. For certain transactions to be legally enforceable, existing Ethiopian legislation embodies formality requirements such as "written form", "signature" or "original document" requirements. Although all transactions are not required to comply with specific form under the Ethiopian legal system, there are legal provisions that oblige

[148] *National Information Security Policy of the Federal Democratic Republic of Ethiopia*, September 2011.
[149] Marc Lixi and Mariana Dahan (2014), *ICT as an Enabler of Transformation in Ethiopia,* The World Bank, January, pp. 69-71.
[150] *Ibid.*
[151] European Commission, *supra* note 145.
[152] Smedinghoff & Bro, *supra* note 147.

specific transactions to fulfil certain formality requirements. The Ethiopian Civil Code, for instance, prescribes that certain transactions should be in 'written' form.[153] Furthermore, it stipulates that transactions required to be in 'writing' shall be supported by a special document and 'signed' by all parties who are to be bound by it and attested by witnesses.[154] The words of the Civil Code that require "special document", "handwritten signatures", or "thumb-marks" clearly indicate the exclusion of electronic documents and electronic signatures.[155]

The effects of non-fulfilment of these formality requirements render the transaction void and no party can claim the enforcement of such transactions.[156] Moreover, contracts or transactions required to be in written form should also be proved in the same formality and by producing the original document.[157] In addition to such formality requirements, certain transactions are also required to be authenticated by the notary public.[158]

The question which remains to be answered is, therefore, whether electronic records and electronic signatures meet the legal formalities; whether an electronic record constitutes an "original" for evidentiary purposes.[159] Clearly, the Ethiopian Civil Code of 1960 was initially designed to facilitate paper-based transactions, and does not accommodate these with technological changes. The requirement of contracts to be in written (paper document) form, signed by manuscript signatures and evidenced in a particular way can only apply in the physical world environment. Therefore, the major laws in Ethiopia, such the Civil Code and the Commercial Code, have no provisions for the use of electronic contracts and other related electronic transactions. Of course, this should not come as a surprise since the legislature of the 1960s could not have possibly foreseen the pace of technological changes such as the Internet. Over all, the existing rules that require transactions to be in 'writing' and 'signed' are generally perceived to constitute legal barriers to electronic transactions.[160]

The second major challenge to the e-commerce environment in Ethiopia relates to trust. While fulfilment of legal requirements is one thing, to have a

[153] Arts 1721 – 1726, the Ethiopian Civil Code, *supra* note 121.
[154] *Id.*, Art 1727.
[155] *Id.*, Art 1728 cum Art 1727.
[156] *Id.*, Art 1720 (1).
[157] *Id.*, Arts 2427, 2003 and 2005.
[158] Art 5, The Authentication and Registration of Documents Proclamation, *Federal Negarit Gazeta,* Proclamation No. 334/2003.
[159] Smedinghoff & Bro, *supra* note 147, pp. 731-732.
[160] *Ibid.*

sufficient degree of trust in an electronic transaction is something else.[161] People do not do or at least hesitate to do business in an environment they do not trust or with people they do not trust. Unlike the face-to-face nature of the paper-based world, electronic transactions are conducted between strangers who have no prior contractual relationships.

It has become necessary to assure all e-commerce actors that their sensitive data are not intercepted or illicitly collected, the documents they exchange are issued only by the person named therein as the sender and contain all but only such information that the sender intends to send and that any one of them cannot deny the validity of their undertakings.[162] Having taken this into account, ensuring that an electronic transaction is trustworthy requires consideration of four levels of trust. These are: authenticity, integrity, confidentiality and non-repudiation.[163] These four levels of trust remain the primary issues of e-commerce before a party will enter into binding legal commitments with significant economic consequences.[164]

The legal challenges of electronic transactions noted above have been the subject of extensive legislative efforts at international, regional and national level. At the international level, for instance, the United Nations Commission on International Trade Law (UNCITRAL) developed Model Law on Electronic Commerce in 1996, and Model Law on Electronic Signatures in 2001 which have served as the basis for legislation enacted in several countries. The United Nations also approved the Convention on the Use of Electronic Communications in International Contracts (UN E-Contracting Convention) in 2005. In the African context, the African Union (AU) adopted African Union Convention on Cyber Security and Personal Data Protection which covers three major areas, including electronic transactions.[165] All these international and regional legislations are intended to remove obstacles and enhance legal certainty in electronic transactions.

---

[161] Thomas Smedinghoff (2002), The Legal Requirements for Creating Secure and Enforceable Electronic Transactions, *IMF Seminar on Current Developments in Monetary and Financial Law*, p. 16.

[162] Naavi Vijayashankar (2004), *Cyber Laws for Every Netizen in India,* Ujvala Consultants Pvt Ltd, India, p. 54.

[163] Note that while authenticity relates to the source or origin of a document or message, integrity concerns the accuracy and completeness of the communication. Likewise, confidentiality is about protecting information so that unauthorized persons cannot have access to it, whereas non-repudiation is the ability to hold the sender or the recipient to his communication in the event of a dispute. *See* Smedinghoff & Bro *supra* note 147, pp. 773-775.

[164] Smedinghoff & Bro, *supra* note 147, p. 742.

[165] Part I, The African Union Convention on Cyber Security and Personal Data Protection, *supra* note 120.

5.2 The Ethiopian legislative response

5.2.1 Electronic payment laws

The process of formulating e-commerce related legislation in Ethiopia goes back to 2007 when the Ethiopia Commodity Exchange (ECX) was established by virtue of Proclamation No. 550/2007. ECX, *inter alia*, provided a centralized trading mechanism in which offers to sell and bids to buy are coordinated through electronic order matching system.[166] The Proclamation recognizes the 'validity' of electronic signature in relation to transfer of funds to and from ECX and its members' accounts established in these same institutions for the purposes of exchange transactions.[167] Even though its applicability is limited only to transfer of funds to and from ECX and its member's accounts, this proclamation is perhaps the first legislation to recognize electronic signature in Ethiopia. Arguably, the validity and enforceability of electronic records is also implicitly recognized under this legislation.

Another important legislation is the National Payment System Proclamation No.718/2011 which recognizes the legal validity and admissibility of electronic records and electronic signatures in relation to transfer of funds. Article 21 (1) of the proclamation reads:

> 'Where any law provides that information or any other matter shall be in writing, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for subsequent reference'.[168]

Accordingly, electronic records have the same legal effect as written documents provided that the electronic record is *"accessible so as to be usable for subsequent reference"*. This requirement is a standard to be met by electronic records in order to be considered as meeting the "writing" requirement. The requirement is also similar to the one stipulated under the UNCITRAL Model Law on Electronic Commerce.[169] Among the reasons why laws require the use of "writing" is to ensure that a document would remain unaltered over time and provide a permanent record of a transaction, to allow for the reproduction of a document so that each party would hold a copy of the same data, and to facilitate control and subsequent audit for accounting, tax or regulatory

[166] Art 6 (2), the Ethiopian Commodity Exchange Proclamation, *Federal Negarit Gazeta,* Proclamation No. 550/2007.
[167] *Ibid*, Art 25(7).
[168] Art 21(1), the National Payment System Proclamation, *Federal Negarit Gazeta,* Proclamation No.718/2011.
[169] Art 6, *The UNCITRAL Model Law on Electronic Commerce with additional article 5 bis* as Adopted in 1998, December 1996.

purposes.[170] Arguably, the requirement of *"accessible so as to be usable for subsequent reference"* is meant to achieve these purposes.

The National Payment System Proclamation recognizes the 'admissibility' of electronic records and electronic signatures in any court as evidence in relation to payment instructions, messages and funds transfers.[171] By recognizing the legal validity and admissibility of electronic records and electronic signatures, this law removes legal obstacles and it enhances legal certainty and commercial predictability where electronic communications and electronic signatures are used in connection with the payment system.

Although the instruments mentioned above could potentially play a crucial role in removing the barriers to electronic transactions resulting from traditional writing and signature requirements, they have two basic limitations. The first problem is that their scope of application is limited only to payment system or transfer of funds. Secondly, they do not provide any standard as to what type of electronic signature meets the legal requirement of "signature".

The nomenclature 'Electronic Signature' is a generic, technology-neutral term that universally refers to the various methods by which one can sign an electronic record.[172] These methods vary from very simple methods such as inserting a scanned image of handwritten signature in a word processing document, personal identification numbers (PINs), and clicking an 'OK-box' to very advanced methods such as using cryptology.[173] As to the question of what type of electronic signature meets the legal requirement of 'signature', there is no common answer as most laws follow varying approaches that range from a minimalist approach (that simply authorizes all electronic signatures satisfy legal signature requirements), to approaches that dictate electronic signatures satisfying legal signature requirements only when they possess certain security attributes, to a cryptography-based digital signature.[174]

Nevertheless, the first approach has been criticized on the ground that it does not take into account the fact that some types of electronic signatures are better than others. The third one is also less adopted as it recognizes only one form of technology.[175] The moderate approach provides that electronic signatures satisfy legal signature requirements only when they possess certain security attributes,

---

[170] *Ibid.*
[171] Art 23, The National Payment System Proclamation, *supra* note 168.
[172] Smedinghoff & Bro, *supra* n 147, p. 530.
[173] *Ibid.*
[174] *Ibid.*
[175] Stephen Blythe (2011), A Critique of Argentine E-Commerce Law and Recommendations for Improvement, *Annual Survey of International & Comparative Law*, Vol. 17, No. 1, p. 87.

and it is a progressive trend and widely recognized by most nations.[176] International instruments such as the UNCITRAL Model Law on Electronic Commerce (Art7), UNCITRAL Model Law on Electronic Signatures (Art 6), United Nations Convention on the Use of Electronic Communications in International Contracts (Art 9(3)), and European Union's Electronic Signature Directive (Art 5) have also adopted this approach.[177]

Current Ethiopian laws discussed earlier seem to adopt the minimalist approach. These laws define electronic signature as "data in electronic form, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message".[178] Furthermore Art 25(8) of the ECX Proclamation provides that: 'Notwithstanding provisions of any law, regulation, directive or customary practice that requires a signature [to] be handwritten in order to have legal effect or enforceability, *signature requirement is met if an electronic signature is used to authorize fund transfers'*.[179] [Emphasis Supplied]

According to these rules, any kind of electronic signature which is used o identify the signatory and to indicate the signatory's approval of the content of an electronic record meets the 'signature' requirement equivalent to handwritten signature. Although these laws focus on identity of the signatory as well as the

[176] *Ibid.*

[177] Note that under the UNCITRAL Model Laws and the United Nations Convention, electronic signature meets legal requirements of "signature" only when three cumulative requirements are fulfilled: (1) the method must identify the person; (2) the method must indicate the person's approval of the information in the message; and (3) the method must be as reliable as appropriate. Although what constitutes reliable under these laws would be determined by taking different factors into account, electronic signatures that satisfy the following four requirements are automatically qualified as "reliable"(Art 6 of UNCITRAL Model Law on Electronic Signatures): (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person; (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable. Under the EU directive for electronic signatures, only advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device satisfy the legal requirements of a signature in the same manner as a handwritten signature (Art 5). The directive defines 'advanced electronic signatures' in same manner the UNCITRAL Model Law defines 'reliable electronic signatures'.

[178] Art 2(8), The Ethiopia Commodity Exchange Proclamation, supra n 166*;* see also Article 2(11), The National Payment System Proclamation, *supra* note 168.

[179] *Id.*, Art 25(8).

approval of content, all types of electronic signatures cannot perform functions identified as characteristic of handwritten signatures. Furthermore, these laws ignore other fundamental legal issues of e-commerce such as integrity, confidentiality and non-repudiation. Adopting this approach is also a significant deviation from the international model laws noted above. In sum, it can fairly be concluded that the current legal framework in Ethiopia is not fully responsive to the changing needs of the information society and hence more comprehensive and conducive legal frameworks are needed.

5.2.2 The draft electronic transactions and signature laws

The importance of having comprehensive and conducive legal framework on electronic commerce is recognized by the Ethiopian government since 2009 following the adoption of different ICT related policies and strategies. Moreover, Ethiopia has adopted e-Government Strategy in 2011 and the development of robust national Public Key Infrastructure (PKI) has been identified as one key strategic project of this strategy.[180] The objective of the PKI project was to facilitate electronic transactions and provide the security required for such transactions.[181] Data encryption and digital signature for authentication, integrity and non-repudiation purposes are among the services that the PKI is expected to offer upon implementation.[182]

The need for electronic signature and electronic transaction laws has also been specifically recognized as one of the critical success factors of the PKI project.[183] Although the government of Ethiopia has been proactive in this regard, the laws are still at draft stage. The MCIT, for instance, had drafted electronic signature and electronic transaction laws following the adoption of the strategy. In the meantime, however, the responsibility to develop the national PKI and draft electronic signature law has been relegated to INSA. MCIT and INSA have finalized the development of electronic signature law and electronic transaction law respectively and these laws are set for public consultation. The defining features of these two draft laws are briefly reviewed in what follows.

a. The Draft Electronic Signature Law

As it stands now, the Draft Electronic Signature Law (hereafter referred to as DESL) contains 56 detailed provisions divided into five parts: 'general', 'electronic signature and electronic messages', 'digital signature and licensing', 'certificate authority and certification services', and 'miscellaneous provisions'.

---

[180] Ministry of Communication and Information Technology, *E-Government Strategy and Implementation Plan – Report,* January 2011, p. 110.
[181] *Ibid.*
[182] *Ibid.*
[183] *Ibid.*

The draft legislation recognizes in its preamble that existing Ethiopian laws have gaps and obstacles in relation to electronic transaction.[184] It also recognizes the need for legal recognition to electronic signature technologies so as to promote electronic commerce and electronic government in the country.[185]

According to the explanatory note, international model laws and conventions have served as the basis for the preparation of the DESL.[186] Except Articles 5 through 7, which address electronic signature in general, the entire DESL deals with cryptography-based digital signature. As thorough analysis is beyond the scope this article, we highlight only certain areas which we deem are of significant impact on the development of e-commerce in Ethiopia. These are freedom of contract; legal recognition of electronic signatures; PKI structure; functions of Root Certificate Authority (RCA) and Certification Authorities (CAs); regulation of CAs; rights and obligations of parties (CAs, relying parties and subscribers); and recognition of foreign digital certificates.

The first important feature of the DESL is that it recognizes the principle of 'party autonomy' by which parties are allowed to agree on issues of form requirements governing their communications.[187] In other words, parties to a contract are free to choose either to use electronic signatures or otherwise. Furthermore, the DESL authorizes parties to determine for themselves what constitutes an acceptable signature method. It also indicates that this freedom of form is not absolute as restrictions may be set by law for different public policy reasons. This approach is in line with major international legislation.[188]

Another significant feature of the DESL is that it deals with the validity, enforceability and admissibility of electronic signatures. Article 6(1) of the Draft Electronic Signature Law (DESL) recognizes the evidential value of electronic signatures by stating that "no electronic signature shall be denied legal effect, validity or admissibility as evidence in any legal proceeding, solely on the ground that it is in electronic form".[189] According to the explanatory note, this provision should not be misinterpreted as if all electronic signatures satisfy the legal requirements of a signature in the same manner as a handwritten

[184] The preamble of the Draft Proclamation to Provide for Electronic Signature, January 2015 (On file with authors).
[185] *Ibid.*
[186] The Explanatory Note to the Draft Proclamation to Provide for Electronic Signature, January 2015, p. 25 (On file with authors).
[187] Art 4, the Draft Electronic Signature Law, *supra* note 184.
[188] *See* the UNCITRAL Model Law on Electronic Commerce 1996 (Art.4); *see* also UNCITRAL Model Law on Electronic Signatures 2001(Art 5); European Union Electronic Signature Directive (preamble, para 16); United Nations Convention on the Use of Electronic Communications in International Contracts (Art 3).
[189] Art 6(1), the Draft Electronic Signature Law, *supra* note 184.

signature.[190] Although the legal effectiveness, validity or enforceability of electronic signature cannot be denied on the mere ground that it is in electronic form, only 'reliable' electronic signatures satisfy the legal requirements of a signature in the same manner as a handwritten signature.

While the 'reliability' of electronic signatures would generally be established on a case-by-case- basis, a digital signature supported by valid certificate would automatically be qualified as 'reliable' electronic signature.[191] The important aspect of this draft law is that 'reliable' electronic signatures and certified digital signatures enjoy rebuttable evidentiary presumptions. For those who use 'reliable' electronic signature or certified digital signature, the DESL provides a legal benefit in the form of evidentiary presumption that: (1) the electronic signature is the signature of the person to whom it correlates, (2) the electronic signature was affixed by that person with the intention of approving the electronic message, and (3) the electronic message and the signature have not been altered since the specific point in time to which the electronic signature was affixed.[192]

The third defining feature of the DESL is that it establishes hierarchical PKI structure whereby a higher authority designated as RCA will be responsible, among other things, to (*i*) issue licenses to CAs[193;] (*ii*) ensure the trustworthiness and the overall security of the crypto system; and (*iii*) issue policies, working procedures and standards that CAs shall follow.[194] In this regard, INSA is designated by law to serve as a 'Root Certificate Authority', to regulate cryptographic products and their transaction, set necessary criteria and develop operating procedures, develop cryptography infrastructure.[195] The draft law also

[190] The Explanatory Note to the Draft Electronic Signature Law, *supra* note 186, p. 15.

[191] Arts 6(2) and 8(1), the Draft Electronic Signature Law, supra n 184. Digital signature is defined under Art 2(3) of the draft Electronic Signature law as an electronic signature that uses asymmetric cryptosystem and meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) It is created using a private key that the signatory can maintain under his sole control; and (d) it is linked to the electronic message to which it relates in such a manner that any subsequent change of the electronic message or the signature is detectable.

[192] *Id.*, Arts 7-8.

[193] Note that Certification Authority is defined under Art 2(11) as 'a body corporate duly authorized to issue certificates and renders other services related to digital signatures and holds a license for this purpose […]'.

[194] Art 10, the Draft Electronic Signature Law, *supra* note 184.

[195] Art 6(9-10), the Information Network Security Agency Reestablishment Proclamation, *supra* note 105.

entrusts CAs with extensive functions including issuance of digital certificates to subscribers, provide encryption and time stamp services.[196]

In order to build trust in CAs and to encourage legal recognition of digital signatures, legislative approaches range from mandatory licensing of CAs to self-regulation without official endorsement or voluntary schemes.[197] In this regard, the DESL adopts a compulsory licensing scheme, i.e. no one can operate as a CA without obtaining a valid license form Root Certificate Authority.[198] According to the explanatory note, compulsory licensing approach is adopted because this offers strong assurance to the public that licensed CA is reliable and responsible for potential liability issues.[199]

The DESL also provides the rules of conduct by addressing the rights and obligations of participating parties in the PKI system including obligations and liabilities of CAs and subscribers.[200] With the view to acquaint players of electronic transaction regarding the rules of the game, the law requires a CA to, *inter alia*: (1) use secure and trustworthy systems and products every time it provides service, (2) disclose its practices and procedures, (3) suspend and/or revoke certificates, and (4) make warranties to its subscriber and relying parties.[201]

The DESL also specifies the obligations of the subscribers to: (1) provide accurate information, (2) maintain security of their private keys, and (3) request revocation of the certificate if security has been compromised.[202] Furthermore, relying parties are responsible to (1) follow explicit certificate verification procedures, (2) rely only on a recommended reliance limit and transaction type expressly stated in the certificate, and (3) observe policies, practice statements and other documents published by a CA.[203] The final notable aspect of the DESL is that it recognizes foreign digital certificates which will promote international electronic commerce. The DESL recognizes that digital certificates

---

[196] Art 24, the Draft Electronic Signature Law, supra n 182. The law further defines 'time stamp service' as a digitally signed notation appended to electronic message, digital signature or certificate indicating the correct date and time of an action.

[197] For instance, the European Union Directive on Electronic Signatures (Art 3) requires Member States not to make the provision of certification services subject to mandatory prior authorization.

[198] Art 11(1), the Draft Electronic Signature Law, *supra* note 184.

[199] The Explanatory Note to the Draft Electronic Signature Law, *supra* note 186, p. 10.

[200] *See* the provisions under Section III and IV of Part IV of the Draft Electronic Signature Law, *supra* note 184.

[201] *Id.*, Arts 28, 30, 36-37 and 43.

[202] *Id.*, Arts 48-51.

[203] *Id.*, Art 52; according to Article 2(14), the phrase 'relying party' refers to 'a person who acts relying on the information contained in a certificate or in the authenticity of digital signature'.

issued by recognized foreign CAs will have the same legal effect as those issued by a national CAs provided that they satisfy recommended reliance limits and requirements provided under the DESL.[204]

b. The Draft Electronic Transaction Law

The Draft Electronic Transactions Law (hereafter referred to as DETL) contains 30 detailed provisions; we consider only four of them. First, the law recognizes the principle of 'party autonomy' by which parties involved in generating, sending, receiving, storing or otherwise processing electronic records are allowed to vary the effects the provisions of DETL by agreement.[205] In other words, the DETL applies where the parties involved in electronic transaction have not reached agreement on the issues provided for in the electronic transaction. This approach complies with the DESL and international model laws.[206]

Second, the DETL gives legal certainty in respect of the validity, enforceability and admissibility of electronic records.[207] The DETL also recognizes that retention of documents, records or information in electronic form satisfies legal requirements of record keeping provided that certain security attributes are fulfilled.[208] Furthermore, it contains detailed provisions on the formation and validity of electronic contracts.[209]

Thirdly, the DETL addresses the liability of 'network service providers' in respect of third-party material.[210] The principle adopted under the DETL is that "network service providers" are neither subject to any civil or criminal liability in respect of third-party material nor responsible to control the content of the data to be transferred.[211] It is only under exceptional circumstances stipulated under the DETL, 'network service providers' can be held liable for third party materials.[212]

Fourthly, the DETL deals with online consumer protection. The DETL provides several rights of online consumers and obligations of suppliers of goods or services through electronic communications.[213] Suppliers are responsible to provide extensive list of information to consumers and are liable

---

[204] *Ibid*, Art 22.
[205] Art 4, Draft Electronic Transactions Law, *supra* note 12.
[206] *Ibid*; see also Art 4, the UNCITRAL Model Law on Electronic Commerce, *supra* n 169
[207] *Id.*, Arts 5-7 and 9.
[208] *Id.*, Art 8.
[209] *Id.*, Arts 13-17.
[210] The DETL is slightly vague while it defines 'network service providers' as those 'who provide processing, storing, hosting, presenting or communication services'.
[211] *Id.*, Arts 11-12.
[212] *Ibid.*
[213] *Id.,* Art 18.

for any damage suffered by a consumer due to a failure by the supplier to utilize a secured payment system.[214] The DETL also protects online consumers form unsolicited commercial communications.[215] More importantly, the DETL makes any agreement to exclude any of the rights of online consumers or to waive legal obligations imposed on suppliers null and void.[216] Furthermore, the DETL extends the applicability of the Trade Competition and Consumer Protection Proclamation No. 813/2013 to electronic transactions.[217]

c. General Observations on the Draft Electronic Signature and Electronic Transaction Laws

Whilst the effort put in crafting these instruments is commendable, there are basic shortcomings that deserve due consideration. The first issue that deserves attention is the relationship between Draft Electronic Signature Law (DESL) and Draft Electronic Transactions Law (DETL) and other relevant instruments (draft and enacted). Although the DESL is specifically dedicated to deal with electronic signatures, it also deals with the legal effect, validity and admissibility of electronic records.[218] Likewise, the DETL gives legal recognition to electronic signature.[219] There are also other pieces of legislation such as the ECX and national payment laws that deal with electronic signatures and electronic records. Neither the DESL nor the DETL explicitly repeals the redundant and incoherent provisions in existing legislations. The liability of 'network service providers', 'CAs', and 'service providers' are addressed under the DETL, DEST and the draft cybercrime law respectively. It is not clear, however, whether these pieces of draft legislation are referring to the same institutions or not.

Furthermore, 'unsolicited commercial communications' is dealt with inconsistently under the DETL and the draft cybercrime law. Looking at all these laws, one can easily discern the unnecessary overlaps, redundancies and inconsistencies. Although it is true that piecemeal approach to legislation process is common in Ethiopia, it leads to problems in legal interpretation, enforcement and some times over legislation. Therefore, there is the need to create synergy among the drafters who usually come from different offices and make sure that the draft laws are in harmony with each other and with existing legislation so that they can move the country far enough toward the ultimate goal of facilitating e-commerce.

---

[214] *Id.*, Art 18 (5&6).
[215] *Id.*, Art 21.
[216] *Id.*, Art 22.
[217] *Id.*, Art 24.
[218] Art 5, the Draft Electronic Signature Law, *supra* note 184.
[219] Art 7, the Draft Electronic Transactions Law, *supra* note 12.

Moreover, important issues relevant to e-commerce such as taxation, jurisdiction, and privacy are totally ignored in the drafts. Taxation has emerged as a particularly relevant issue due to the large revenue that is generated through e-commerce; and the development of a suitable online taxation regime and framework poses a number of challenges to governments.[220] There is thus the need to address the problem of how companies could be taxed when they trade online. While the DETL defines what e-commerce is, for instance, it should also ascertain how matters of taxation would be handled under the same legislation.

As discussed above, the legal requirements of 'writing', 'signature' and 'original' are the barriers to e-commerce. Neither the DETL nor the DESL, however, explicitly addresses what constitutes 'original' in electronic transactions. A clear statutory provision covering the requirements of 'original' in relation to electronic record is thus required in order to create legal certainty and facilitate the development of e-commerce.

These draft laws also ignore the jurisdictional problems of electronic transactions. E-commerce is mainly conducted with no geographical boundaries – i.e., cyberspace. It is not limited to consumers and businesses located in a particular jurisdiction. A consumer can buy goods or services from almost anywhere in the world thereby giving rise to the notion of conflict of laws. The development of e-commerce requires not only certainty as to the legal validity, effectiveness and admissibility of e-transactions, but it also requires certainty as to where the transaction would be enforced, and under which law. These problems are not addressed explicitly under any of the draft laws.

7. The New Media and Ethiopian Law

The 'new media' refers to the media that rely on the use of computers for the purpose of production, distribution and communication of information to the public.[221] They are computer-mediated and Internet-driven, and emerged as an alternative to the traditional (analogue) media represented by television and radio broadcasting.[222] Ethiopian law has not so far been forthcoming in regulating this 'new media' because we can only find a patchwork of rules that regulate behaviour in this realm.

---

[220] United Nations Conference on Trade and Development, *Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries*, 2015, pp. 4, 46-65, 88-89.

[221] Lev Manovich (2009), *The Language of the New Media*, MIT Press, 2001, p. 19; *s*ee also Martin Lister *et al*, *New Media: A Critical Introduction*, 2nd Ed., Routledge, pp. 13-14.

[222] Nicholas Gane and David Beer (2008), *New Media: The Key Concepts*, Bloomsbury, p. 6.

For example, the definition of 'broadcasting services' under the Ethiopian Broadcasting Services Proclamation, only includes radio or television transmission programs conducted to educate, inform or entertain the public.[223] But, the categories of broadcasting service licences are set out illustratively in that 'other broadcasting services to be prescribed by the Authority' may also require licences.[224] Such an open-ended provision may potentially be applied in practice to require licensing of websites. Indeed, there have been reports that a legislation is underway that would fill this regulatory gap particularly by regulating the increasingly ubiquitous websites in Ethiopia.[225] This proposed legislation, aimed to supplant the proclamation that regulates freedom of information and mass media, is said to ban electronic dissemination of 'unconfirmed rumours', 'defamatory information', 'reports that incite violence' as well as 'reports that disparage religion, gender and ethnicity'.[226] While the text of the bill is not yet publicly available for closer scrutiny, one senses certain overlaps with some existing legislation and proposed bills.

For instance, the Telecom Fraud Offence law penalizes provision of 'telecom services' – which includes 'Internet services' – without the requisite license.[227] This, in essence, regulates provision of web-based services such as infotainment services which are commonplace in Ethiopia. Similarly, the draft cybercrime law, as noted above, has provisions that regulate dissemination of certain prohibited information through the Internet such as online defamation, intimidation and crimes against public security.[228] Unless the new media law is intended to result in just civil liability, it is imperative to reconcile these overlaps in due time before the law is enacted.[229]

The freedom of information and mass media law, issued in 2008, does not appear to treat the Internet within the purview of the 'the media' – 'mass media' as it calls them. In defining 'mass media', it refers only to 'printed matter and

[223] Art 2(2), Broadcasting Services Proclamation, *supra* note 27.
[224] *Id.*, Art 17(h).
[225] Alemayehu Anbessie, New Legislation to Regulate Websites Proposed, *Addis Admass*, 5 January 2015, available at <http://bit.ly/1FasZZ5> (Amharic: Authors' Translation) [Last accessed on 25 September 2015].
[226] *Ibid.*
[227] Arts 2(1), 2(5) and 4, Telecom Fraud Offence Proclamation, *supra* note 10.
[228] Arts 11 – 14, the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12.
[229] The Ethiopian Broadcasting Authority is reportedly finalizing a new draft legislation that aims to regulate transformation of analogue to digital broadcasting in the country. But, it remains unclear whether this upcoming legislation will regulate websites as such. *See* Mikiyas Tesfaye, Draft Broadcast Proclamation in the Pipeline, *Fana Broadcasting Corporate News*, 14 October 2014, available at: <http://bit.ly/1JsejWs> (Last accessed on 25 September 2015).

broadcasters'.[230] The nearest it comes to the Internet is when it describes 'broadcaster' as a body that disseminates broadcast programming, among others, *via* 'other electronic equipment.[231] Possibly, this could be understood to embrace broadcasting services through websites. The advertisement proclamation has also bearings on dissemination of commercial advertisements through the Internet which it recognizes as one means of advertisement dissemination. It, for instance, regulates the sort of commercial advertisement that could not be broadcasted through various means including the Internet such as advertisements of gambling or illegal products or services.[232]

This state of the law clearly illustrates that Ethiopia currently regulates the new media only indirectly and through rules that are scattered across various pieces of legislation. Therefore, it is imperative to move behind piecemeal regulation and put in place a coherent body of law. The obvious challenge amid such a legislative confusion is that individuals and entities whose rights and interests are adversely affected by the new media would find it difficult to seek appropriate legal recourse. Indeed, unregulated sphere means that a range of other illegal activities including pornography which has adverse effects on child upbringing, moral standards of the youth and social values at large might possibly mushroom in Ethiopia's emerging net.

Concluding Remarks

The advent of the Internet has significantly reshaped the fabric of societies from the way how crimes are committed, goods and services are transacted, and relationships are created. In the legal realm, it has profoundly challenged traditional legal principles and institutions thereby setting off new trajectories in the field of law and legal systems in general. These changes brought about by the information and communication technologies mainly the Internet are not, however, uniformly felt across the board since only a third of the global population have had basic access to the Internet. Ethiopia is among countries with limited connectivity to the Internet. The history of the Internet Ethiopia is only a little over a decade, and it is only recently that significant telecom infrastructural developments have commenced.

The delay in the proliferation of the Internet in Ethiopia has concomitantly arrested legislative initiatives in the field. Despite a few pieces of legislation currently in operation, most aspects of the law that regulate behaviour or activities on the Internet are yet to be enacted. This article has provided a critique of the developments in the field of Internet law in Ethiopia. We

[230] Art 2 (1), Mass Media and Freedom of Information Proclamation, *supra* note 123.
[231] *Id.*, Art 2(4).
[232] Art 25, Advertisement Proclamation, *supra* note 28.

sketched out legislative responses of the Ethiopian legislature to the advent of the Internet by outlining major sources of Internet law and their defining features. Among others, we have critically reviewed legal instruments governing (or due to be governing once enacted by the legislature) cybercrime, electronic commerce, telecommunications, electronic privacy, intellectual property and the new media.

While a lot remains to be undertaken, the efforts to harmonize the regulatory responses with the developments presented by the Internet are commendable. Despite the increasing convergence in the telecommunications, broadcasting and IT industries, Ethiopia has opted for sector-specific regulatory and legal approaches. In this context, there is a need for reconsidering the current regulatory and legal approach in the light of the benefits of a converged technological environment. Currently, Ethiopia does not have a comprehensive legislation governing electronic privacy. In this context, there is the need to streamline the adoption of the draft data protection law after having made the required changes based on benchmark instruments with due consultations with stakeholders and the general public.

E-commerce in Ethiopia is currently at the early stage of development, and this is partly due to the absence of a conducive legal environment. Ethiopia will thus benefit from speeding up the enactment of its proposed draft laws on Electronic Signature and Electronic Transaction as this would increase legal certainty and boost the trust of both business and consumers in the online environment. In so doing, due consideration should be given to the gaps within these draft laws. Ethiopia currently regulates the new media only indirectly, and through rules that are scattered across various pieces of legislation. It is, therefore, imperative to move behind piecemeal regulation and put in place a coherent body of law.

Due to the ambiguous words of the telecom fraud offences law, the regulatory treatment of VoIP in Ethiopia lacks some clarity. Since the regulatory definitions of VoIP have important implications, not only for regulation, but also for innovation, investments, and business competition, the law needs to be amended to avoid ambiguities. The MCIT is expected to prescribe approved telecommunication equipments and set standards as per art 3(3) of the law toward ensuring legal certainty. The ambiguous terms of the Proclamation may also cause problems in interpretation, administration and enforcement, thereby making it imperative to train the law enforcement and judiciary personnel accordingly. ■