The Internet and Ethiopia's IP Law, Internet Governance and Legal Education: An Overview

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

Abstract

The current information age requires intellectual property laws to catch up with and proactively regulate unfolding technological realities. The dynamic advances in the domain of the Internet have thus necessitated corresponding changes in Ethiopia's intellectual property legal regime including copyright laws in relation with computer programs, databases, online service provision and Digital Rights Management systems (DRMs). New issues are also steadily arising owing to the increasing commercialization of the Internet in relation with the quest for the presence of trade names in cyberspace and protection from similar or confusingly similar trade names. Likewise, the applicability of patent laws to the digital environment and the patentability of software-related inventions are contentious. This article briefly deals with these issues. Also addressed in this article are issues relating to Ethiopia's roles in the global Internet governance ecosystem, and the extent to which Ethiopian legal education is catching up with the unprecedented changes wrought by the advent of the Internet.

Key terms

Intellectual property, copyrights, patents, trade names, internet governance, cyber law, Ethiopia

DOI http://dx.doi.org/10.4314/mlr.v9i1.5

- This article is thematically a sequel to another article titled "The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media" published in the same issue of this journal.

- The authors kindly 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.

[♣] 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), 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.

Acronyms

DRMs	Digital Rights Management systems
EPO	European Patent Office
EU	European Union
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IPRs	Intellectual Property Rights
OSPs	Online Service Providers
TRIPs	Trade Related Aspects of Intellectual Property Rights
WIPO	World Intellectual Property Organization

> "*The registration of a domain name does not have any trademark status. It is up to the requestor to be sure he is not violating anyone else's Trademark.*" ♣

Introduction

The rapid technological changes over the last decades have provided an enormous number of new and innovative goods and services. The advent of Internet, in particular, has dramatically transformed the way of doing business. Along with all these opportunities, the Internet is also bringing new set of challenges to existing legal regimes around the world. Intellectual property law is arguably among the legal regimes challenged by the rapid development of the Internet. It has become very easy to infringe intellectual property rights ("IPRs") through the use of electronic technologies.[1] In this context, the first three sections of this short article examine the main challenges and loopholes of the major Ethiopian intellectual property laws in the context of the Internet.

The fourth section outlines the state of Internet governance in Ethiopia by briefly addressing issues such as Ethiopia's role in the global and regional Internet governance frameworks as well as domestic multi-stakeholder initiatives, if any. Section 5 considers the need for enabling Ethiopian legal education to prepare law students to a legal profession which is increasingly oriented by the Internet. A case is made towards introducing a new mandatory 'cyber law' course within the present law school curriculum in order to make the legal education system fit for purpose in the digital age.

1 Copyrights and the Internet

The advancement of the internet has changed the underlying assumptions of traditional copyright law since technological developments have made copyright

♣ John Postel (1994), *Domain Name Structure and Delegation*, Request for Comments 1591, March 1994, p. 6.

[1] Philip Weiser (2003), The Internet, Innovation, and Intellectual Property Policy, *Columbia Law Review*, Vol. 103, No. 3, pp. 534-613.

material easier to access and reproduce, and more difficult to protect.[2] Furthermore, digital contents transmitted over the Internet evoke unique copyright issues. Although the Internet affects almost every aspect of copyright issues, this section focuses on the major and topical legal issues namely: (i) legal protection of software programs, (ii) legal protection of databases, (iii) liability and obligations of online service providers and (iv) Digital Rights Management systems.

1.1 The Legal Protection of Computer Programs

The first major issue regarding copyright as it applies to the online environment concerns the legal protection of software programs. One of the striking features of software is that it can be very expensive to develop but can be reproduced quickly, at a very low cost.[3] That every form of use of computer software involves some form of copying also makes the nature and extent of protection to be accorded complex.[4] This unique nature of software programs necessitates the provision of specific rights protection against unauthorized reproduction or copying.

Nevertheless, whether what forms of intellectual property protection – be it patent or copyright – are best placed to adequately protect the rights and legitimate interests of computer programmers is often debatable. The predominant form of legal protection accorded to computer programs in current international, regional and national intellectual property laws is copyright. The primary justification is that since the underlying 'source code' is written in a form of human language – e.g., English, or other language – computer programs are eligible to copyright protection as any other 'literary work'.[5]

Chief among these instruments include the Trade Related Aspects Intellectual Property Rights (TRIPs) Agreement which protects computer programs 'whether in source or object code' as literary works.[6] Similarly, the WIPO Copyright Convention affords copyright protection for computer programs 'whatever may be the mode or form of their expression'.[7] The basic difference between the TRIPs and WIPO Treaty rules is that the latter pursue

---

[2] United Nations Conference on Trade and Development, *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community*, 2012, p. 36.

[3] Ian Lloyd (2014), *Information Technology Law*, 7th Edition, Oxford University Press, p. 323; see also Hector MacQueen and others (2009), *Contemporary Intellectual Property: Law and Policy*, 2nd Edition, Oxford University Press, p. 241.

[4] Diane Rowland and Elizabeth Macdonald (2000), *Information Technology Law*, 2nd ed. Cavendish Publishing Limited, p. 21.

[5] Ian Lloyd, *supra* note 3.

[6] Art 10(1), *Trade Related Aspects Intellectual Property Rights (TRIPs) Agreement*, 1994.

[7] Arts 4 and 5, *WIPO Copyright Treaty*, 1996.

rather 'technology-neutral' and 'generic phraseology' than the former.[8] A major regional instrument specifically dedicated to deal with computer programs is the European Union Directive on the Legal Protection of Computer Programs.[9]

Ethiopia's Copyright and Neighbouring Rights Protection Proclamation No. 410/2004 (hereafter referred to as 'the Copyright Proclamation') provides protection for computer software as 'literary work'.[10] This law defines computer program as 'a set of instructions, expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a machine-readable medium, of causing a computer to perform or achieve a particular task or result'. Given the dynamic nature of the field, the provision of a definition to computer programs is clearly significant so that legal certitude can be guaranteed.

Nonetheless, the scope of the Copyright Proclamation regarding as to what aspects of a computer program are protected against copying is rather limited in contrast with other benchmark instruments. A contentious issue regarding computer programs concerns whether this protection extends to other aspects of the program, beyond literal code. It has been argued that all aspects of a computer program, other than the source code should not be protected by the copyright.[11]

The EU Computer Programs Directive, for instance, clearly stipulates that it protects the source code but not interfaces of the computer program whereas, as noted above, TRIPs clearly provides that both the source and the object code are subjects of protection.[12] The Ethiopian Copyright Proclamation does not clearly provide whether a particular interface of a computer program constitutes copyright subject matter. That the definitional proviso is couched in such generic manner seems, however, to allow broader than narrower interpretation of the scope of protection accorded to computer programs. While 'technological-neutrality' is much desirable in a fast-moving field like information technology, there is meanwhile the need for clarity with the view to ensure legal certainty.

Another area of ambiguity latent in the Ethiopian copyright law is that it does say little, if not none, with respect to possible protection to 'preparatory design materials' of computer programs. These materials are basically those

---

[8] *The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty*, Document Prepared by the International Bureau of WIPO, (year of publication undisclosed), pp. 8-9.

[9] *European Union Directive on the Legal Protection of Computer Programs*, Directive 2009/24/EC, 2009.

[10] Arts 2(30) cum 14, the Copyright and Neighbouring Rights Protection Proclamation, *Federal Negarit Gazeta,* Proclamation No.410/2004.

[11] Chris Reed and John Angel (2003), *Computer Law,* 5th ed., Oxford University press, p. 222

[12] Art 1(2), EU Directive on the Legal Protection of Computer Programs, *supra* note 9.

which form part of the early design and programming process of computer programs. Such materials are given due copyright protection under the EU Directive on the Legal Protection of Computer Programs.[13] On top of the lack of explicit recognition of such materials as 'objects of protection', Ethiopian law seems to rather implicitly deny protection under one of its provisions. For instance, such materials might be judged as 'subject-matters not protected' merely because they are akin to 'ideas, procedures, concepts, formula etc' under Article 5(a) of the Copyright Proclamation. Overall, as any preliminary literary work, preparatory design materials deserve protection under Ethiopian copyright law in so far as the requirements of 'originality and fixation' are satisfied.

Whether the Ethiopian copyright law recognizes the notion of 'fair dealing' by which free copying of computer programs for the purposes of 'research' or 'private study' is not clear. All what the law provides is that free 'reproduction' of computer programs is allowed only where this is needed for its lawful use, or to retain a back-up copy or for the purposes of adaptation.[14] The only limitation to the copyright for the purposes of research under the Copyright Proclamation applies with respect to the protection of 'performers, producers of sound recordings and broadcasting organizations', not concerning computer programs.[15]

Related to this is that the Ethiopian Copyright Proclamation does not address the issue of reverse engineering or 'de-compilation'. In simple parlance, 'reverse engineering' or 'de-compilation' refers to developing new models or sorts of computer programs relying largely on the pre-existing knowledge, knowhow and manufactured software products. As Ian Lloyd writes, given that a lawful user cannot be prevented from using a program for its normal purpose, some aspects of reverse engineering must be considered legitimate.[16]

Indeed, the EU Computer Programs Directive allows reverse engineering under limited circumstances.[17] Moreover, the Directive permits the studying or testing 'the functioning of the program in order to determine the ideas and principles which underlie any element of the program'.[18] The underlying rationale behind permitting 'reverse engineering' is to set the stage for new generation of advanced and efficient products based on previously existing knowledge, and meanwhile addressing inherent gaps.

---

[13] *Id.*, Art 1(1).
[14] Art 14 cum Art 9(2)(d), The Copyright Proclamation, *supra* note 10.
[15] *Id.*, Art 32(b) cum Arts 26-31.
[16] Lloyd, *supra n 3*, p. 33.
[17] Art 6, EU Directive on the Legal Protection of Computer Programs, *supra* note 9.
[18] *Id.*, Art 5(3).

The Ethiopian copyright law is not straightforward when it comes the right of users of computer programs to freely copy or adapt with the view to uncovering errors – or bugs and hence to rectify them. The nearest the Ethiopian law comes in this regard is when it allows 'adaptation that is indispensable for using the computer program'.[19] But, it remains unclear whether such adaptation involves 'correcting bugs' inherent in computer programs. In contrast, the EU Directive on the Legal Protection of Computer Programs explicitly puts limitation to the copyright when reproduction is needed for the purposes of correction of errors'.[20]

Such copyright 'limitations' are often inserted because software programs usually have bugs that are planted in, either deliberately or inadvertently. What makes a strong case for the legitimacy of such copying or adapting in order to correct bugs is the recent revelations by Edward Snowden. The disclosures have unveiled systemic practices of installing bugs – or backdoors – by the collusion of software companies and spy agencies so that personal communications could easily be intercepted by spies.[21] Also making the matter more imperative is that with fast developing ICT in Ethiopia, business automation and digitalization are increasing, and both governmental and private organizations engage in multi-million birr software procurements.

1.2 The Legal Protection of Databases

Value of databases has increased significantly following the advent of the internet and many jurisdictions that protect databases under copyright laws.[22] Without prejudice to the protection accorded to the content, a database may qualify for protection in its own right. In this regard, the Ethiopian Copyright Proclamation protects databases as 'derivate works' provided that "the collections are original by reason of the selection or arrangement of their contents".[23]

The law further provides that the reproduction of the whole or a substantial part of a database without authorization of the owner of copyright is also forbidden, even for personal purpose.[24] In this sense, the Ethiopian law is commendably on track with technological developments by providing protection to databases. The recent hikes in the number of databases in Ethiopia make the provision of database protection quite significant. This is in stark contrast with

[19] Art 14(2)(c), The Copyright Proclamation, *supra* note 10.
[20] Recital 13, EU Directive on the Legal Protection of Computer Programs, *supra* note 9.
[21] See generally Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man*, Guardian Faber Publishing, 2014.
[22] Lloyd, *supra* note 3, pp. 391-393.
[23] Art 4(1)(b), The Copyright Proclamation, *supra* note 10.
[24] *Id.*, Art 9(2)(c) .

the reported decline – or stagnation, in the growth of databases in Europe where adequate legal protection are provided.[25]

Ethiopian law protects 'databases' only within copyright law proper. This, in turn, means that those databases which might not pass the requirements of copyright ability – i.e. originality and fixation – would be outside any form of legal protection. The fact that certain databases may not fulfil these requirements has triggered certain countries and regional blocs to provide for what are generally called '*sui generis* database rights'. A case in point, in this regard, is the EU which has already adopted an all-out Directive on the Legal Protection of Databases which embodies 'sui generis database right' along with copyright protection of databases.[26]

Similarly, the WIPO has proposed an international treaty on the legal protection of databases which embodies such unique database rights for non-copyrightable databases.[27] For a database to enjoy '*sui generis*' protection, it need not be an intellectual creation so long as it is systematically or methodically organized. Unlike copyright which protects a database for its original selection and arrangement, a '*sui generis'* right protects against extraction and reutilization of the contents of the database.[28] This is somehow akin to the rule in Ethiopian copyright law that bans reproduction of a database as a whole or substantial part of a database even for personal purposes.[29]

Therefore, the Ethiopian legislature is expected to consider the inclusion of these rights with the view to provide comprehensive level of protection to databases. An obvious advantage of recognizing such rights would be an impetus and incentive for the creation of new useful databases in Ethiopia.

1.3 Liability and Obligations of Online Service Providers

The third fundamental legal challenge raised by copyright laws in the internet context concerns the liability of online service providers (OSPs) such as search engines, websites, internet service providers, and hosting services. These OSPs provide network access to customers or subscribers who may post materials that infringe copyrights.[30] Whenever anyone places images or text on a webpage, for instance, there is a potential violation of the copyright owner's exclusive right in the material. In that capacity there is no doubt that the individual responsible for

[25] Lloyd, *supra* note 3, p. 373.
[26] Art 3 cum Arts 8 – 11, *The EU Directive on the Legal Protection of Databases*, Directive 96/9/EC, 1996.
[27] Lloyd, *supra* note 3, p. 381.
[28] MacQueen and Others, *supra* note 3, p. 214.
[29] Art 9(2)(d), The Copyright Proclamation, *supra* note 10.
[30] Gerald Ferrera *et al* (2004), *Cyber Law: Text and Cases*, South-Western Cenage Learning, p. 102.

unauthorized copying of a work is the direct infringer and will primarily incur liability.[31]

But in the Internet context, there are several difficulties to sue the primary actors for publishing copyrighted materials. One is that identifying or locating the individuals responsible for violating the copyright owner's exclusive right in the material may be difficult and sometimes impossible as the Internet permits anonymity.[32] And, even if the individuals who are responsible for the copyright infringement are identified, it is not cost effective to go after every user who has violated the copyright. Because of these reasons, copyright holders have avoided targeting the end user of the copyrighted works and have focused on the OSPs.[33]

Therefore, the question as to what extent OSPs are liable for the infringing actions of their subscribers or for linking to sites that contain infringing information remains to be a contentious issue. In many national laws and international model laws, it is a well-established principle that OSPs are not required to review, monitor or classify the content that they host, and are therefore not held liable for the transmission of prohibited content unless they have specific knowledge of the illegal content or fail to take corrective action.[34] For instance, the principle under the European Union Electronic Commerce Directive is that OSPs are not liable for any third party content transmitted or stored through or in their networks. But under exceptional circumstances prescribed under this Directive, OSPs can be held liable for any illegal content transmitted or stored in their system.[35]

Even though this is the established principle of many contemporary legal regimes, OSPs may be subject to other legal and administrative obligations. The UK Digital Economy Act 2010 is a good example in this respect, although it is not yet put into force. According to Article 3 of this Act, copyright owners can make a copyright infringement report to the OSP who provided the Internet access service. and the OSP who receives such report is obliged to notify its subscribers and, among other things, advice that the copyright owner may apply to a court.[36] Furthermore, Article 4 of the UK Digital Economy Act obliges OSPs to provide infringement lists to copyright owners when requested by the latter.[37]

---

[31] Lloyd, *supra* note 3, p. 548.
[32] *Ibid.*
[33] *Ibid.*
[34] *See*, for instance, Article 12, *European Union Electronic Commerce Directive*, Directive 2000/31/EC, 2000; see also Title II, the US Digital Millennium Copyright Act, October 1998.
[35] *Ibid*, Arts 12, 13 and 12.
[36] Art 3, UK Digital Economy Act, 2010.
[37] *Ibid*, Art 4.

These issues are not properly addressed under the Ethiopian Copyright Proclamation or in any other existing or proposed legislation in Ethiopia. As the law stands now, the liability and responsibility of OSPs for the infringing actions of their subscribers is uncertain and this may affect the development of online service providers. Recent legislative initiatives in Ethiopia such as the draft mass media, cybercrime law and electronic transactions laws embody rules that address the issue of intermediary liability in their respective remits.[38] Whilst these legislative initiatives are necessary to bridge the gaps in existing laws, one major concern is that the issue will fall under different legal regimes with the potential risk of unnecessary overlaps and redundancies. If the draft laws are enacted as in their current content, there will be increasing risk of 'over legislation' and this brings in problems in interpretation, administration and enforcement of the laws. The drafters are thus expected to work in concert and reconsider the aforementioned concerns.

1.4 Digital Rights Management Systems

Among the various means of ensuring the copyright of authors in audio-visual works is the use of Digital Rights Management systems which represent the technical means of restricting the reproduction of protected works. Also called 'rights management information systems and technical protection measures', they are mechanisms built into products such as CDs, DVDs, databases and websites to prevent unauthorized access and use.[39] Nevertheless, as these mechanisms emerge as tools of protecting copyrights, means of circumventing them have also been devised so that reproduction of the works could be made without any technical restriction.

With the view to mitigate such circumvention of technical means of protecting copyrights, the copyright laws of several countries prohibited circumvention of these technologies and provide remedies when violations occur.[40] The EU copyright law, for instance, requires member states to sanction production, promotion or sale of circumvention tools and to provide remedies against those who are affected by such unlawful actions.[41] Ethiopian law, however, does not provide anything with respect to DRM systems and their unlawful circumvention. This lacuna appears to be a major one given that the widespread unlawful reproduction of copying in Ethiopia could very well be mitigated through such techniques, and copyright law should not only ban

[38] Art 48 (3), the Draft the Mass Media Proclamation, supra n 34; see also Art 16, the Draft Proclamation to Legislate, Prevent and Control Computer Crime, *supra* note 12; Arts 10-12, the Draft Electronic Transactions Proclamation, *supra* note 12.

[39] See MacQueen and Others, *supra* note 3, p. 239.

[40] *Id.*, p. 261.

[41] Arts 6-7, *The EU Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society*, Directive 2001/29/EC, 2001.

circumvention practices but also encourage the domestic use and development of these technological mechanisms.

2 Trademarks and the Internet

Trademark is another area of law that is significantly challenged by the advent of the Internet. With the emergence and increasing commercialization of the Internet, many businesses have sought to establish a presence in cyberspace.[42] Typically, they will seek domain name which incorporates the real-life identity of the companies.[43] As the commercial attractiveness of the World Wide Web increased, more and more commercial organizations have sought to develop a presence.[44] In short, the sale of goods and services online has brought a new dimension of trade and service mark law and practice, where traders or companies have opted to use domain names.[45]

Companies conducting business online have an obvious incentive to maintain a website with a domain name that matches their company, logo, or service.[46] The interplay of domain name with trademark laws is not, however, straightforward. It is rather challenging due to two factors: one is that names of businesses may be shared by many individuals, a typical example being McDonalds; and secondly generic top level domains such as <.com> or <.net> may be obtained by anyone from anywhere in the world.[47]

Under the trademark law, different parties may use the same trademark if they are using it in different categories of goods and services and there is no

[42] Lloyds, *supra* note 3, p. 403.
[43] *Ibid.*
[44] *Ibid.*
[45] See Jennifer Golinveaux (1999), What's in a Domain Name: Is "Cybersquatting" Trademark Dilution?, *University of San Francisco Law Review*, Vol. 33, pp. 641-670; see also *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community*, *supra* note 2, p. 37. Domain names are essentially translations of IP numbers or addresses into a more semantic or meaningful form. Under IPv4, an IP address is a 32 bit string of 1s and 0s. This string will be represented by four numbers from 0 to 255 separated by dots/periods—for example, 153.110.179.30. However, that an IP number tells most people little or nothing; <ethionet.et> is much more easily remembered and catchy. Thus, the main reason for domain names is mnemonics – i.e., domain names make it easier for humans to remember identifiers. *See* Lee Bygrave and *et al*, The Naming Game: Governance of the Domain Name System, in Lee Bygrave and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions*, Oxford University Press, 2009, p. 147.
[46] Wayne Hale (2001), "The Anti-cybersquatting Consumer Protection Act & Sporty's Farm L.L.C. V. Sportsman's Market, Inc.", *Berkeley Technology Law Journal,* Vol. 16, No. 1, p. 206.
[47] Lloyds, *supra* note 3, p. 403.

likelihood of confusion.[48] On the contrary, only one company can register a particular domain name as it should be unique. Conflict is, therefore, inevitable since companies conducting business online have an obvious incentive to maintain a website with a domain name that matches their company, logo, or service.[49]

The question which remains to be answered is, therefore, whether trademark owners have an overriding right to claim a domain name that is identical to their trademark. If domain names were equivalent to trademarks, the use of domain name would amount to a trademark infringement. This is not, however, a settled issue and hence disputes are underway throughout the world as to whether the owner of the real-world trademark or the owner of the domain name online owns a particular domain name.[50]

Disputes over ownership of domain names arise under three circumstances: (1) a domain name can be akin to a trademark – whether registered or not, and those who use it for offline business might want to own one on the Internet; (2) cyber-squatting (3) reverse domain name hijacking – where owners of trademarks aggressively pursue policies to prevent other Internet participants from using any rendition of a name that includes or alludes to their trademark.[51]

It is common for people to register a domain name of a famous trademark or brand and then try to get the company (the trademark owner) to buy the domain name back at high price. This is commonly referred to as "cybersquatting"[52] and adopting anti-cybersquatting legislation is becoming a trend.[53] In the U.S., for instance, there is an anti-cybersquatting statute which enables a trademark owner to bring a civil action against any person who, with 'a bad faith intent to profit from that mark', 'registers, traffics in, or uses a domain name' that is 'identical or confusingly similar' to a distinctive or famous mark, including personal names which are protected as marks.[54]

A related concept is called 'reverse domain name hijacking' which represents an attempt to use procedures with bad intent to deprive a registered domain name of a domain name holder.[55] A plain illustration for this practice is when a

---

[48] *Ibid.*
[49] Golinveaux, *supra* n 45, pp. 647-648.
[50] Ferrera and Others, *supra* note 30, p. 49.
[51] Lloyds, *supra* note 3, pp. 717-718.
[52] Note that Cybersquatting represents a situation in which a registrant registers a mark or personal name as a domain name on the Internet and then exacts a price to turn the domain name over to the name's owner. Golin veaux, *supra* note 45, p. 647.
[53] Thekla Hansen-Young (2005), "Whose Name is it, Anyway? Protecting Tribal Names from Cybersquatters", *Virginia Journal of Law & Technology,* Vol. 10, No. 6, pp. 2-18.
[54] Anti-cybersquatting Consumer Protection Act, 15 U.S.C, § 1125(d)(1), 1999.
[55] Lloyds, *supra* note 3, p. 408.

well-known business –say Hilton– files a complaint against a holder of a domain name called <himton.com> alleging domain name hijacking. Such practices are generally regarded inappropriate by critical internet resource administers such as the Internet Corporation for Assigned Names and Numbers (ICANN).

In the Ethiopian context, the threat of cybersquatting is high as many companies in Ethiopia are slow or reluctant to accept the Internet as a potential commercial avenue and they may not secure their domain name (identical with their trademark) before anyone else does. In an interview with local media outlet, a manager of one private company engaged in web-hosting services stated that "[…] companies need websites to interact with customers therefore eventually they will end up deciding to buy a domain name which usually takes time. But when they do because the domain name is already taken they have to pay a higher price and secure it from me".[56]

The interviewee further explained that he secures the registration of domain names of companies such as real estate companies, banks and manufacturing companies 'before anyone else does and then auctions them to whoever is interested'.[57] In other words, if a well-known real estate company in Ethiopia wants to have a website and its trade name is already registered by others with the intention of selling it to trademark owners, the company is required to pay high price (up to 5,000 dollars) to get it back from the private web-hosting service providers.[58] Even though this practice is the exact definition of 'cybersquatting', the country has no adequate legal framework to address the interplay of domain name with trademark laws.

The primary legal frameworks governing trademark in Ethiopia include the Trade Mark Registration and Protection Proclamation No. 501/2006, Trademark Registration and Protection Council of Ministers Regulation No. 273/2012, Commercial Registration and Business Licensing Proclamation No. 686/2010, and Trade Competition and Consumer Protection Proclamation No 813/2013. But, these legal frameworks do not address issues relating to cybersquatting. The term 'domain name' in the trademark context is not mentioned in any existing or draft legislation in Ethiopia. This makes it difficult to enforce the existing laws in the area of domain names.

The low level of Internet penetration and use which partly translates into the lack of awareness into the real challenges that domain names present to

[56] SnetsehayAssefa, Domain Name Game – Web Hosting: Highway to the World, *Addis Fortune*, Vol. 15, No. 777, 23 March2015, available at <http://bit.ly/1IIaMTJ> (Last accessed on 25 September 2015).

[57] *Ibid.*

[58] *Ibid*. Currently, there are 15 companies that have secured Certification of Competence (COC) from the MCIT and are engaged in web hosting.

trademark might have so far arrested legislative initiatives in the field. As highlighted in Section 4, the participation of both the government and the private sector, in the global Internet governance forums has indeed been quite low, if not nil. Although the Ethiopian government is the sole institution for critical Internet resource administration in the country, it has not been active in the ICANN public meetings, or has never been represented at the Country Code Names Supporting Organization (ccNSO) of ICANN, despite the fact that the Ethiopian government, through the MCIT, manages the '.et' domain name.[59] With respect to the <.et> domain name space, whist there are businesses and individuals who use the domain, there presently appears to exist no mechanisms to deal with disputes over ownership of the domains between trademark holders and other registrants.

Parallel to the Universal Dispute Resolution Mechanism (UDRP) operated by ICANN to deal with trademark *versus* domain name disputes relating to generic top level domains (gTLDs) such as <.com>, <.net> etc, there are national counterparts to deal with disputes over Country Code Top Level Domains (ccTLDs) such as <.co.uk>, <.et>. A good case in point is the one operated by Nominet that operates the <.co.uk> domain name space which has been in operation since 2001.[60] With increasing use of domain spaces including ccTLDs in Ethiopia, the need for the MCIT to put in place a procedure to deal with trademark *versus* domain name disputes cannot be overemphasised.

Another issue relating to trademarks in cyberspace relates to the essentially 'territorial' scope of trademark protection and the 'global' nature of the Internet. This particularly becomes an issue if the same or similar mark registered for the same or similar goods is used by traders based on WebPages.[61] Under present trademark law, when trademarks are identical, there would be infringement where one of the owners solicits business in the territory of another. To solve this conundrum, it may be appropriate to introduce the use of disclaimers.[62] The latter would be instrumental in avoiding possible confusion among consumers on the Internet. While the risks of such forms of trademark infringement are present in Ethiopia, the existing Ethiopian trademark legislation does not specifically address this new challenge presented by the Internet. Any future legislative amendment is, therefore, expected to consider whether 'disclaimers' are fit for purpose to deal with the matter once introduced into the law.

---

[59] Kinfe Micheal Yilma (2014), The State of Internet Policy Making in Ethiopia: An Introduction, *University of Pennsylvania, Center for Global Communication Studies Media Wire*, 14 October 2014, available at <http://bit.ly/1GyU1o6> (Last accessed on 25 September 2015).

[60] MacQueen and Others *supra* note 3, pp. 715-716.

[61] *Id.*, pp. 727-728.

[62] *Id.*, pp. 729-701.

3. Patents and the Internet

In relation to the applicability of patent laws to the digital environment, the patentability of software-related invention is one of the most contentious issues. Whilst the protection of computer software under copyright regime is recognized in almost all jurisdictions, its patentability remains controversial. In the United States, for example, the patentability of software was recognized back in 1981. In the *Diamond v. Diebr* case, the US Supreme Court held that a process for curing synthetic rubber employing a mathematical formula and a programmed digital computer is patentable subject matter.[63] Under U.S. Patent Act 1952, whoever invents or discovers any new and useful process, machine, manufacture of composition of matter may obtain a patent. This law does not exclude software from patentability.

Unlike the US system, there is a clear-cut exclusion of computer programs from patentability under the European Patent Convention.[64] Despite this exclusion, however, there is a well established case law and practice of the European Patent Office (EPO) that allowed patentability of the so-called 'computer related inventions' that involve a technical effect.[65] In order to qualify as a non-patentable computer program "as such" and patentable computer programs, the EPO has introduced an additional requirement called the "technical effect", which does not appear in the convention.[66]

The Inventions, Minor Inventions and Industrial Designs, Proclamation No. 123/1995 is the primary legislation in Ethiopia that governs patents. Like that of the European Patent Convention, the Proclamation excludes computer programs from patentability.[67] The difference between the EU system and Ethiopia's legislation is that the former allows software patent under limited conditions whereas the Ethiopian system excludes it categorically. Although the trend seems towards protection of software under patent law, the Proclamation has remained in operation for more than two decades without any revision. It is not also clear why computer programmes are excluded from the patent system so far as they are new, industrially applicable and involve an inventive step like any other technology.

---

[63] Lloyd, *supra* note 3, p. 548.
[64] Art 52, European Patent Convention, 1973.
[65] Andres Guadamuz Gonzalez (2006), "The Software Patent Debate", *Journal of Intellectual Property Law & Practice*, Vol. 1, No. 3, pp. 196-206.
[66] Lloyd, *supra* note 3, p. 310.
[67] Art 4(1)(c), Inventions, Minor Inventions and Industrial Designs Proclamation, *Federal Negarit Gazeta,* Proclamation No. 123/1995.

4. Ethiopia and Internet Governance

The term 'Internet governance' refers to the process by which critical internet resources such as domain names and Internet protocol addresses are administered through a bottom-up multi-stakeholder model of governance.[68] The Ethiopian government is completely absent from the global internet governance ecosystem, especially with regard to Internet governance forums. Although it is the sole institution in charge of critical Internet resource administration in the country, the Ethiopian government has not been active in the ICANN public meetings, the UN Internet Governance Forum (IGF), or sub-regional IGF forums such as the African Internet Governance Forum (AfIGF) and the East African Internet Governance Forum (EAfIGF).[69] Ethiopia did not also have a seat at the World Conference on International Telecommunications (WCIT) held in December 2012 in Dubai, UAE despite the country's early membership to the ITU.[70]

Moreover, the Ethiopian government has never been represented at the Government Advisory Committee (GAC) or the Country Code Names Supporting Organization (ccNSO) of ICANN, although the Ethiopian government, through MCIT, manages the '.et' domain name. The Ministry is entrusted by law to 'assign and monitor government domain names and register addresses'.[71] It is also required by law to coordinate all stakeholders for the creation and proper utilization of country code top level domain, and facilitates their proper implementation.[72] The Ministry has since prepared guidelines through which '.et' domain names are allocated to government departments.[73] But, it remains unclear whether the Ministry as a 'registry' convenes a multi-stakeholder forum in the utilization of these resources as mandated by law.

It is also rare to see notable participation from Ethiopian civil societies, industry, or academia in the Internet governance ecosystem. Potential stakeholders have also not been keen on holding the government accountable for

---

[68] Kurbalija, *supra* note 17, pp. 5-7; *see* also Lee Bygrave, Introduction, *in* Lee Bygrave and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions*, Oxford University Press, 2009, pp. 1-3.

[69] Kinfe Micheal Yilma, *supra* note 59.

[70] Note that Ethiopia joined the International Telecommunications Union on 20 February 1932. See details at <http://bit.ly/1bYhS98> (Last accessed on 25 September 2015)

[71] Art 24(1(g)), A Proclamation to Provide for the Definition of the 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).

[72] *Id.*, Art 24(1)(h).

[73] *Domain Naming Guidelines for Ethiopian Government Websites (.gov.et), Version 1.3*, year unknown, available at <http://bit.ly/1GILFN6> (Last accessed on 25 September 2015).

its statutory obligation to coordinate all stakeholders in the management of the country code top level domains. Ethiopia is a member of the African Telecommunications Union (ATU) which is notably a multi-stakeholder forum where non-state actors play a key role.[74] But, no private organization from Ethiopia is so far a member to the ATU including Ethio-telecom, unlike other African telecom providers presently members to ATU.[75]

Yet, it is important to mention the commendable participation, if not decisive roles, of some individual Ethiopians in the Internet governance ecosystem. Noteworthy examples include Ms. Sophia Bekele, who spearheaded a widely known – and controversial – bid to run the dotafrica (.africa) top level domain, and Dr. Dawit Bekele, regional director of the Internet society.[76] ICANN's fellowship program has also recently enabled few young academics to attend its public meetings held across the globe, which has in turn opened doors for them to join stakeholder groups within ICANN.

The value in taking part in the global as well as regional Internet governance platforms is that most decisions affecting the manner through which critical Internet resources are administered are routinely made at these fora. Unlike the traditional top-down governance model where nation-states are the major players, Internet governance, as noted above, follows bottom-up multi-stakeholder mechanism where everyone takes part in an equal footing. Therefore, full engagement of the Ethiopian government and non-state actors such as civil societies, academics etc is undoubtedly vital.

5. Ethiopian Legal Education and the Internet

The far-reaching effects of the Internet are also felt in the domain of legal education. Over the years, legislatures have extensively been enacting cyberspace-specific statutory regulations which partly depart from traditional legal principles.[77] Almost every lawyer at present is likely to encounter some cyber law issues given the unprecedented ubiquity of the Internet.[78] This consequently necessitates the need to realize how law and cyberspace interact, particularly through specifically dedicated law courses.[79] Specific law courses

[74] *See* details at <http://bit.ly/1zgfDIn> (Last accessed on 25 September 2015).
[75] *See* details at <http://bit.ly/1JbGDJk> (Last accessed on 25 September 2015).
[76] *See* personal profile of Dr. Dawit Bekele at <http://bit.ly/1OIy8MD> ; see personal profile of Ms. Sophia Bekele at <http://bit.ly/1EFF9ay> (Last accessed on 25 September 2015).
[77] Eric Goldman (2008), "Teaching Cyberlaw", *Saint Louis University Law Journal*, Vol. 52, p. 750.
[78] *Ibid.*
[79] Lawrence Lessig (1999), "The Law of the Horse: What Cyberlaw Might Teach", *Harvard Law Review,* Vol. 113, p. 502.

titled as 'cyber law', 'Internet law' or 'cyberspace law' or 'law and the Internet' have been launched to acquaint students with legal aspects of the Internet in most developed countries.[80] In short, the rapid proliferation of the Internet has prompted legal education reforms in these countries.

In contrast, the curriculum of law schools in Ethiopia have remained generally stagnant for a long period.[81] Law Faculty of Addis Ababa University, for instance, used its curriculum for a long time without significant reform[82] until a major reform in the Ethiopian legal education occurred in 2006 under the auspices of the then Ministry of Capacity Building[83] which engaged the participation of Ethiopian Law Schools coordinated by Justice and Legal System Research Institute (JLSRI). One of the principal changes brought about by this reform was introduction of a new law school curriculum incorporating a range of skill-oriented courses.[84] This is perhaps dictated by the general belief that young lawyers graduating from African law schools often lack meaningful skills in key subjects.[85] In this sense, the focus of the curriculum reform was, *inter alia*, to embody skill-oriented courses that would enable students acquire skills which they will use upon joining the legal world. However, updating the legal education system to the changes brought about by the Internet received little attention although a new course titled "Introduction to Computers and the Internet (CoSc 201" was included as a compulsory 3-credit-hour course offered during the first semester of the first year.

Although commendable achievements were attained in the preparation of teaching materials as part of the reforms, the materials rarely make references to the interactions between the law and the Internet.[86] The Alternative Dispute

---

[80] Frank Easterbrook (1996), "Cyberspace and the Law of the Horse", *The University of Chicago Law Forum*, pp. 207-208.

[81] Abdi Jibril (2011) "The Need to Harmonise Ethiopian Legal Education and Training Curricula", *The Ethiopian Journal of Legal Education*, Vol. 4, No. 1, p. 52.

[82] *See* FDRE Ministry of Capacity Building, *Comprehensive Justice System Reform Program: Baseline Study Report*, 2005, p. 202.

[83] See Jibril, *supra* n 81, p. 95; see also *Reform on Legal Education & Training in Ethiopia*, 2006, (Unpublished), p. 9.

[84] *Ibid.*

[85] Thomas Geraghty and Emmanuel Quansah (2007), "African Legal Education: A Missed Opportunity and Suggestions for Change: A Call for Renewed Attention to a Neglected Means of Securing Human Rights and Legal Accountability", *Loyola University Chicago International Law Review*, Vol. 5, No. 1, p. 90.

[86] This also applies to the training manuals prepared under the auspices of the Federal Justice Organs Professionals Training Center which hardly give any attention to legal issues presented by the advent of the Internet. See *Federal Justice Organs Professionals Training Center Training Manuals,* available at <http://bit.ly/1zgf15t> (Last accessed on 25 September 2015).

Resolution teaching material, for instance, makes only a brief reference to 'online dispute resolution', albeit as an excerpt from an academic source without any correlation with Ethiopian law.[87] Teaching materials on Criminal Law also completely ignore computer crimes despite the fact that these crimes are regulated under the Ethiopian Criminal Code. Criminal Law II dedicates a chapter to deal with 'criminal law in a changing world' but no references are made to cybercrimes which certainly are among new developments in the field of criminal law and procedure.[88] Nonetheless, the teaching material on 'Criminology' discusses computer crimes at some length within the category of white collar crimes but in a relatively lower legal tone.[89]

The teaching material on 'Interdisciplinary II', a module that covers sociology, criminology and accounting, addresses issues such as online extortion, identity theft and other crimes related with electronic commerce in the context of organized crimes.[90] Since this module – as its name tells is a non-law course, it does not address the legal aspects of these issues. The 'Introduction to Computers and the Internet' teaching material commendably provides some basic introductory information regarding the Internet as well as domain names, Internet addressing etc.[91] These introductory discussions are very instrumental in acquainting law students with some basic information that they may apply in dealing with practical legal cases that involve the Internet.

No reference to Internet banking is to be found in the 'Banking, Negotiable Instruments and Insurance Law' teaching material.[92] Similarly, the 'Intellectual Property Law' module does not devote much to discuss the interactions between intellectual property and technologies such as the Internet. One only finds few references to computer software, programs, databases and piracy.[93] It also makes

[87] Tefera Eshetu and Mulugeta Getu (2009), *Alternative Dispute Resolution Teaching Material*, Justice and Legal System Research Institute, pp. 233, 271, 295.

[88] Glory Nirmala and Amha Mekonnen (2009), *Criminal Law Teaching Material*, Justice and Legal System Research Institute, pp. 314-349.

[89] Glory Nirmala (2009), *Criminology Teaching Material*, Justice and Legal System Research Institute, pp. 90, 108, 127-128, 135.

[90] *Interdisciplinary II Teaching Material*, Justice and Legal System Research Institute, 2009, p. 144.

[91] Abebe Regassa (2009), *Introduction to Computer and the Internet Teaching Material*, Justice and Legal System Research Institute, pp. 232-249.

[92] Fasil Alemayehu and Merhatbeb Teklemedhin (2009), *Law of Banking, Negotiable Instruments and Insurance Teaching Material*, Justice and Legal System Research Institute

[93] Balew Mersha and G/Hiwot Hadush (2009), *Law of Intellectual Property Teaching Material,* Justice and Legal System Research Institute , pp. 3, 19, 21-22, 29, 40, 58, 67, 70, 72-73, 93, 97, 113, 117, 119, 127, 142, 160, 187, 194-198, 202-207, 217, 219-220, 230, 239, 292.

a few references to the right to make available copyrighted materials *via* the Internet but without any discussion of how these issues would be applied in the context of Ethiopian law.[94] The 'Law of Property' teaching material does not also address the notion of 'digital properties' in the context of Ethiopian law of property.[95] Similarly, issues relating succession of 'digital assets' such as our online accounts are not included in the teaching material as it is structured around the rules of succession as conceived in the 1950s.[96]

The teaching material on the 'Law of Evidence' makes a few references to electronic evidence but not in the desirable depth.[97] Issues concerning Internet sales through online retailers – increasingly emerging in Ethiopia, and auction platforms are not addressed in the teaching material on 'Law of Sales and Security Devices'.[98] The 'Law of Traders and Business Organizations' teaching material does not also include elements of Internet-related trading ventures.[99] The teaching material on the 'Law of Extra-contractual Liability' does not address defamation or slander in the online environment as well as online trespassing.[100]

Of the teaching modules, the 'Media Law' teaching material is by and large better in dealing with the Internet as a new media. It deals with 'computers, the web and the Internet' as new media in addition to traditional media such television and radio based broadcasting.[101] The material further deals with the global regulation of telecommunication by the ITU.[102] Moreover, it dedicates a chapter to 'regulation of audio-visual content and the Internet'.[103] While the inclusion of these topics is laudable, the discussion does not distinctly deal with the notions of 'Internet governance and Internet regulation' which are slightly

[94] *Id.*, pp. 142-143.
[95] Fasil Alemayehu (2009), *Law of Property Teaching Material*, Justice and Legal System Research Institute.
[96] Mellese Damtie and Solomon Fikre (2009), *Law of Succession Teaching Material*, Justice and Legal System Research Institute.
[97] Kahsay Debesu and Andualem Eshetu (2009), *Law of Evidence Teaching Material*, Justice and Legal System Research Institute, pp. 172, 176.
[98] Gadissa Tesfaye and Mebrathom Fetewi (2009), *Law of Sales and Security Devices Teaching Material*, Justice and Legal System Research Institute.
[99] Alemayehu Fentaw and Kefene Gurmu (2009), *Law of Traders and Business Organizations Teaching Material*, Justice and Legal System Research Institute.
[100] Abdulmalik Abubeker and Desta G/Michael (2009), *Extra-Contractual Liability Teaching Material*, Justice and Legal System Research Institute.
[101] *See* Hassen Mohammed (2009), *Media Law Teaching Material*, Justice and Legal System Research Institute, pp. 63-69.
[102] *Id.*, pp. 69-73.
[103] *Id.*, pp. 162-185.

different.[104] Moreover, the discussions do not assess the suitability of Ethiopian law to address the issues in question.

It is vital to point out that law modules such as 'Current Legal Topics' could possibly be used to teach law students the new developments in the legal field including one created by the proliferation of the Internet in all aspects of people's lives. The teaching guide on the 'Current Legal Topics'[105] could further be enriched and is certainly a good starting point to provide a glimpse of the impact of the Internet on the legal profession as a whole.

This state of affairs clearly reveals that the Ethiopian legal education system generally lags behind in terms of providing a curriculum that prepares students to a legal practice oriented by technologies in general and the Internet in particular. While some modules commendably introduce students to the basics of the Internet and its regulatory aspects, most relevant modules largely ignore the effects of the Internet on the subject matters addressed in the respective modules.

With the recent increasing enactment of cyber-related laws by the Ethiopian legislature, it is imperative to update the present legal education curriculum and embody elements of Ethiopian law that concern the Internet. The best approach in this regard would be to introduce a specific mandatory cyber law course – which could alternatively be named as 'Internet Law', 'Cyberspace Law' or 'Law and the Internet'. While crafting a specific course might be onerous in the short term due to the acute shortage of Ethiopian lawyers specializing in cyber law, existing law subjects that are in the course of being significantly reshaped by the advent of the Internet are expected to include the developments in the law commensurate with the advent of the Internet.

Conclusion

Ethiopian intellectual property law regime needs review in the light of the changes brought about by the Internet. In this regard, special consideration must be given to the protection of software under the patent and copyright regime,

---

[104] At the most basic level, 'Internet governance' refers to the multi-stakeholder bottom-up administration or management of critical Internet resources such as domain names and Internet protocols whereas 'Internet regulation' denotes the regulation of web content essentially by national governments of each country such as regulation of pornography or free speech on the Internet. See generally Jeanette Hofmann and Others, Between Coordination and Regulation: Conceptualizing Governance in Internet Governance, *HIIG Discussion Paper Series No. 2014-4*, 2014, available at <http://bit.ly/1AkYJn1>; (Last accessed on 25 September 2015); see also Milton Mueller, *Networks and States: The Global Politics of Internet Governance*, MIT Press, 2010, pp. 8-9.

[105] Yitayal Mekonnen (2009), *A Discussion Paper on the Course "Seminar on Current Legal Topics"*, Justice and Legal System Research Institute.

trademark protection, and the liability of online service providers. The recent amendment to the Copyright Proclamation has not addressed limitations of the law with respect to the legal protection of computer programs. This is more so unfortunate because one of the stated aims of the recent amendment is to 'provide legal protection that is compatible with an ever growing development of copyright and neighbouring rights'.[106]

Ethiopia's participation in the Internet governance ecosystem where all stakeholders take part in the policy development process needs due attention. Both the government and non-governmental actors have so far paid little, if any, attention in the global bottom-up, multi-stakeholder Internet governance ecosystem. In this regard, the MCIT is expected not only to revisit its approach of 'hibernation' from the global Internet governance processes, but it should also live up to its legal obligation to convene a multi-stakeholder forum in the governance of the '.et' domain-name space.

Another major theme of this article relates to legal education in the advent of the Internet, and it is noted that the Ethiopian legal education system should be able to prepare law students to the legal profession which is increasingly oriented by the Internet. It is thus strongly suggested that that the Ethiopian legal education must be updated in the light of the changes brought about by the Internet. With the view to adequately prepare students to a legal practice increasingly oriented by the Internet, the present law curriculum needs to embrace subjects as they pertain to the Internet. In particular, there is the need to include 'cyber law' as a compulsory course. ■

[106] Para 1 of the Preamble, A Proclamation to Amend the Copyright and Neighboring Rights Protection Proclamation, *Federal Negarit Gazette*, Proclamation No. 872/2014.