IMPLICATIONS OF THE ETHIOPIAN COMPUTER CRIME PROCLAMATION ON FREEDOM OF EXPRESSION

Dagne Jembere [*] and Alemu Meheretu [**]

ABSTRACT

Freedom of expression is a fundamental right recognized under the Constitution of the Federal Democratic Republic of Ethiopia (FDRE Constitution, hereafter) and international human rights instruments. The enjoyment of such right has been expanded through the advancement of the internet. Indeed, the internet has become a global mass medium of communication and expression of all kinds. The internet has also given rise to new challenges. In order to address these challenges, States have enacted various pieces of legislations such as computer crime law, data protection law and digital signature law. Like many other countries, Ethiopia enacted Computer Crime Proclamation in 2016 in order to protect the national economic and political stability of the country. However, the proclamation establishes serious offenses that are likely to adversely impact on enjoyment of freedom of expression. This article examines the implications of the Ethiopian Computer Crime Proclamation on the exercise of the right to freedom of expression and argues that the proclamation impinges on freedom of expression.

Key words: freedom of expression, internet, computer crime, limitation, human rights, Ethiopia

1. INTRODUCTION

A number of human rights instruments such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the African Charter on Human and Peoples' Rights (ACHPR) and the FDRE Constitution have recognized the right to freedom of expression. Introduction of internet has boosted the exercise of freedom of expression. Various states and human rights bodies have taken steps to enhance internet access and protect human rights of internet users. However, some states, including Ethiopia, insisted on limiting internet access and online freedom of expression through imposing strict criminal sanctions on internet users and service providers. Though legislation of computer crime law is

[*] LL.B (Dilla University) LL.M (Jimma University),Lecturer in Law, School of Law of Mettu University
[**] LL.B, LL.M, PhD, Assistant Professor in Law, School of Law of Jimma University

important as the very openness of the internet with the capacity to promote technical innovation renders it open to exploitation by unscrupulous profit-minded criminals,[1]such law should not impair freedom of expression of the internet users.

Ethiopian cyber crime regime seems under-developed because of the country's short history of computer and internet penetration.[2] There are about less than 5% internet users in Ethiopia out of the country's total population.[3]The pace of regulation of cyber activities in the country has not been as quick as the development of computer systems in the country.[4] The 1957 penal code had no computer specific provisions to deal with computer crimes. Although, the 2004 FDRE criminal code stipulates some provisions on computer crimes; they are short of regulating the complicated cybercrime. Given their nature, type, impact, and targets of cyber crimes and criminals, computer abuses were not sufficiently criminalized under the 2004 criminal code.[5] Furthermore, the existing Ethiopian Criminal Procedure Code does not provide for rules which guide justice actors in the investigation and prosecution of cyber crimes.

In response to the under-regulation of cyber activities, Ethiopia has been taking some policy and legislative measures including the National Information and Communication Technology Policy and Strategy in 2009 (ICT Policy) and Criminal Justice Policy of 2011. The relevant sections of the policies aim preventing computer crimes and taking remedial measures.[6] Recently, the Ethiopian parliament has promulgated computer specific law, Computer Crime Proclamation No. 958/2016(the Proclamation). The proclamation repealed the computer crime provisions of the criminal code and, provided for conditions of liability, procedural and evidence rules.

Computer crime laws are often justified on the basis of protecting individuals' reputations, national security or countering terrorism. But in practice, they have been used by some governments to censor content that the government and other powerful entities do not like or

[1] Johanna Granville, *Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions, 49* Australian Journal of Politics and History 102,109 (2003).
[2]KinfeMicheal, *Development in Cybercrime law and practice in Ethiopia*, 30 Computer Law and Security Review 720 (2014).
[3]http://www.internetlivestats.com/internet-users-by-country/accessed on January 21, 2018.
[4] KinfeMicheal&HalefomHailu, *The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media*, 9MLR 108, 129 (2015).
[5]MolalignAsmare, *Computer Crimes in Ethiopia: An Appraisal of the Legal Framework*, 3 International Journal of Social Science and Humanities Research 92, 103 (2015).See alsoHalefomHailu, *The State of Cybercrime Governance In Ethiopia*, (2015) available at http://www.global.asc.upenn.edu/the-state-of-cybercrime-governance-in-ethiopia/*accessed on March 31, 2017*
[6]*Ibid* at 98.

agree with.[7]Criminal law has to come to picture as a last resort due to its strong impact on human rights.[8]Hence, all misbehaviors in cyber activities will not always require the use of intrusive criminal law measures, minor infringements can be regulated under civil law.[9]Yet, with a view to regulate illicit cyber activities, the Proclamation created new computer crimes such as criminalization of online defamation and criminal liability of internet service providers.This article examines the possible impacts of such criminalization on freedom of expression. The article is organized into four sections. The first section lays background by briefly highlighting the nature, scope and normative contents of the right to freedom of expression. The second section explains the standards for limiting the right. The third section explores regulation of internet in Ethiopia and its impact on the right to freedom of expression. The fourth section concludes the discussions.

2. FREEDOM OF EXPRESSION ON THE INTERNET

The term 'freedom of expression' has existed since ancient times and has been widely used and conceptualized by various groups, including scholars, politicians, activists, and laypersons.[10] However, there have been controversies among authors on whether the term 'freedom of expression' includes sign language, pictographs, pictures, movies, plays, and so forth.[11]It is clear that all expression requires conduct of some sort, and any conduct can be communicative. Accordingly, freedom of expression should be considered as freedom of communication, and that there are no limits on the media of communication that such freedom encompasses.[12] In cognizance of this view, the United Nations Human Rights Committee (UNHRC hereafter) considered that electronic and internet-based modes of expressions are protected like freedom of expression offline.[13] Accordingly, it called upon states to adopt all necessary steps to ensure every individual's access to the internet. The UN rapporteur on

[7]UNHRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue A/HRC/17/27, (2011).Para. 34.
[8] Nils Jareborg, *Criminalization as Last Resort (Ultima Ratio),* 2 Ohio St. J. Crim. L. 521 (2005)
[9]United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* 52 (2013).
[10] UNESCO, *Privacy, free expression and transparency: Redefining their new boundaries in the digital age*, 47 (2016)
[11] Larry Alexander, *Is There a Right of Freedom of Expression?,*8 (Cambridge University Press 2005).
[12]*Ibid.*
[13]UNHRC, *General comment Number 34*, adopted on 102nd session Geneva, 11-29 July 2011at para. 12.

freedom of expression has been consistently urging states to promote universal internet access and be cautions against rules limiting data content on internet.[14]

Under Article 19 of the ICCPR, Article 9 of the ACHPR and Article 29 of the FDRE Constitution, two elements of freedom of expression are expressly recognized. The first element, the right to seek and receive information, is a key component of democratic governance as the promotion of participatory decision-making processes is unattainable without adequate access to information. Ensuring access to information can serve to promote justice. The UNHRC has emphasized that the public and individuals are entitled to have access, to the fullest extent practicable, to information regarding the actions and decision-making processes of their governments. [15] The internet and digital technologies have expanded the possibilities of individuals and media to exercise the right to freedom of expression and freely access online information.

Freedom of expression also includes the right to dispatch information or idea a person has through any media he/she wants. Information or ideas that may be regarded as critical or controversial by the authorities or by a majority of the population, including ideas or views that may shock, offend or disturb, are also covered under this element of freedom of expression.[16]The scope of information protected under this right covers information from political discourse,[17]and commentary on one's own [18] or on public affairs, [19] canvassing, [20] discussion on human rights, [21] journalism, [22] scientific research, expression of ethnic, cultural artistic expression, [23] teaching,[24] linguistic and religious identity and, advertising.

[14]UNHRC, *UN Special Rapporteur's Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by Abid Hussain, E/CN 4/2002/75, 30 January (2002) at para. 6.
[15] General Comment Number 34, *supra* note 13.
[16] Council of European Union, EU Human Rights Guidelines on Freedom of Expression Online and Offline, Foreign Affairs Council meeting, Brussels, 12 May 2014.
[17]UNHRC, *Mika Miha v. Equatorial Guinea*, Communication No. 414/1990,
[18]UNHRC, *Fernando v. Sri Lanka*, Communication No. 1189/2003, Views adopted on 31 March 2005.
[19]UNHRC, *Coleman v. Australia*, Communication No. 1157/2003, Views adopted on 17 July 2006
[20]UNHRC, *Concluding observations on Japan*, (CCPR/C/JPN/CO/5).
[21] UNHRC, *Velichkin v. Belarus*, Communication No. 1022/2001, , Views adopted on 20 October 2005.
[22] UNHRC, *Mavlonov and Sa'di v. Uzbekistan*, Communication No. 1334/2004, , Views adopted on 19 March2009.
[23] UNHRC, *Shin v. Republic of Korea*, Communication No. 926/2000, , Views adopted on 16 March 2004.
[24]UNHRC, *Ross v. Canada*, Communication No. 736/97, , Views adopted on 18 October 2000.

Freedom of expression has many contributions to overall development of human beings. It helps for fulfillment of individual's dignity by enforcing self-regulation.[25] As it enhances political participation and search for truth, it contributes to development of democracy, rule of law, peace, stability and inclusive development.[26]In other words, freedom of expression is important for two main reasons : (1) it is essential to express ourselves in words, music, dance or any other form of expression for the realization of our humanity, and (2) freedom of expression is the foundation of other human rights and social goods ranging from democracy to human, social and economic development.[27]

On the other side, internet has created new opportunities by which individuals disseminate information to a mass audience and that have an important impact on the participation and contribution of citizens in decision-making processes. In the contemporary world, internet is becoming the preferred mode for political participation, education, employment, commerce or personal activities. It empowers citizens to speak up in a networked public sphere. Particularly, social media has changed the nature of political campaigning and will continue to play an important role in future elections and political campaigns around the world.[28]For instance, social media played important role in Arab Spring,[29] in shaping political debates,[30] by which societies struggled to knock down repressive governments.[31] Hence, for a state that subscribes to democracy, it would be a grave mistake to discount the voices of the internet as something that has no connection to freedom of expression. But, in some instances, technologies on internet can also be misused to inflame conflicts and malicious agitation by populists that do not believe in a healthy democratic discourse.[32] In such cases, internet can play extraordinary role in intensifying violence and chaos in the society. These issues necessitate cyber laws; criminal law being one of them.

---

[25] UNHRC, *General comment Number 34*, supra note 13

[26]WojciechSadurski, *Freedom of Speech and Its Limits*, 8-35 (Kluwer Academic Publishers 1999).

[27]Andrew Puddephatt, Freedom of expression and the internet, UNESCO 2016, p.19

[28] Vyacheslav Polonski, *The biggest threat to democracy? Your social media feed*, 2016 available at https://www.weforum.org/agenda/2016/08/ accessed on April 5, 2017.

[29]Tara Vassefi, *An Arab Winter: Threats to the Right to Protest in Transitional Societies, Such as Post-Arab Spring Egypt*, 29 American University International Law Review 1097, 1128 (2014).

[30]*Ibid*

[31]Sabiha Gire, *The Role of Social Media in the Arab Spring*, available at https://sites.stedwards.edu/pangaea/the-role-of-social-media-in-the-arab-spring/

[32]*Ibid.*

3. STANDARDS ON LIMITATION OF FREEDOM OF EXPRESSION: AN OVERVIEW

3.1. Limitation on Freedom of Expression under the ICCPR

Freedom of expression is one of the most frequently violated rights in the world.[33] It has always been the object of tension, struggle and contest between the state and the citizens and within society itself.[34]Whilst freedom expression is the extension of our humanity and essential for the realization of other human rights and social goods, it is not an absolute right. It is subject to certain restrictions. From the reading of Article 19 (3) of the ICCPR and jurisprudence of human rights bodies, the International Commission of Jurists has drawn principles of limitation of a right called 'Siracusa Principles' that are applicable to freedom of expression.[35] These principles, through providing the limitation clauses, elaborate on the contents of the provisions of the Covenant. According to the principles, any limitation of freedom of expression has to fulfill the following three-part-test:

Firstly, the limitation must be prescribed by law. Arbitrary limitation of freedom of expression is impermissible. Any limitation of freedom of expression must be preceded by a written and clear law. The UNHRC defined the concept of 'law' set out in Article 19 (2) of the ICCPR. In the Committee's view, to be considered as law, norms have to be drafted with sufficient clarity to enable an individual to adapt his behavior to the rules and made accessible to the public.[36]Clarity of the law is strictly required especially when the legislation is criminal law.[37] It is not acceptable to take away human rights by unclear, vague and irrational laws. The law or regulation must meet standards of clarity and precision so that people can foresee the consequences of their actions. Vaguely worded edicts whose scope is unclear will not meet this standard and are therefore illegitimate.[38]

Secondly, the limitation should aim at legitimate purpose. The covenant provides that the objective of the prescription consists of respecting the rights and reputation of others or the

[33] Michael O'Flaherty, *Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment Number 34*, 12 HRLR 627,632 (2012),
[34]*Ibid*. at 633.
[35]American Association for the International Commission of Jurists, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (1985).
[36]UNHRC, *Keun-Tae Kim v. The Republic of Korea*, Communication No. 574/1994, CCPR/C/64/D/574/1994, 4 January 1999, para 25
[37]Gary Slapper, *Clarity and the Criminal Law*, 71The Journal of Criminal Law, 475, 477 (2016).
[38]UNHRC, Keun-Tae Kim v. The Republic of Korea, *supra* note36.

protection of national security, public order, public health or public morality.[39]These are the only legitimate grounds to limit a speech and states may not add another ground.[40]UNHRC in its general comment number 34 stated that any restriction should not put the right to freedom of expression in jeopardy and the relation between right and restriction and between norm and exception must not be reversed.[41]

Thirdly, the limitation must be necessary in a democratic society. This standard requires that the conditions, restrictions and penalties imposed on the exercise of the right have to be proportional with the legitimate aim to be pursued. Hence, if less restrictive alternative is available, the state has to use it. It also necessitates balancing the benefit of the limitation with the harm that it imposes on the exercise of the right. Freedom of expression is a building block of democratic society; thus democracy cannot exist or survive without true implementation of the right. Therefore, freedom of expression is a right that must be upheld as much as possible; restrictions should be applied only when it is really necessary in a democratic society.

In sum, limitations to freedom expression are not permissible unless they are provided for by clear and precise laws (the test of legality), serve one of the legitimate interests listed under the Covenant (the test of legitimacy), and are strictly necessary to meet the intended purpose (the test of proportionality).

3.2. Limitations on Freedom of Expression under the FDRE Constitution

The FDRE Constitution has guaranteed freedom of expression.[42]The Constitution stipulates that freedom of expression, in principle, cannot be limited on account of the content or effect of the point of view expressed.[43]However, it also states that limitation to freedom of expression can exceptionally be made in order to protect the well-being of the youth, and the honor and reputation of individuals, and to prohibit propaganda for war as well as the public expression of opinion which is intended to injure human dignity.[44]The Constitution further requires that any limitation to freedom of expression for the intended purposes should be made through laws.

[39]ICCPR, General Assembly Resolution 2200A (XXI) of 16 December 1966, Article 19(3).
[40] General Comment Number 34 *supra* note 13,Para. 21.
[41]*Ibid.*
[42] Constitution of the Federal Democratic Republic of Ethiopia, Federal *Negarit Gazeta*, Proclamation No. 1/1995Article 29 (2).
[43]*Ibid*, Article 29 (6).
[44]*Ibid.*

From the constitutional provision of limitation to freedom of expression, we can vividly discern the two-part-tests i.e. the tests of legality and legitimacy.

However, the constitutional provision of limitation to freedom of expression is problematic to some extent for two reasons. Firstly, the clause "public expression of opinion which is intended to injure human dignity" listed as a ground of limitation lacks clarity. The clause may be open to uneven application. Secondly, the Constitution does not provide explicit provision that require the necessity of the limitation to be imposed on the right. In short, the test of proportionality is not explicitly indicated. However, the latter problem could be addressed by virtue of Article 13(2) of the Constitution which requires the human rights provisions in it to be interpreted in conformity with international human rights instruments. Accordingly, Article 29 of the Constitution should be interpreted in conformity with Article 19(3) of the ICCPR.

As noted above, the Constitution under Article 29(6) prohibits the imposition of limitation on the effect of the content of the speech. This shows that deceitful laws intended to smash dissents by the government are not permissible. It also shows that the limitation of the right should be narrowly designed to make sure that the exception will not swallow the rule.

Other subsidiary laws which could in principle protect freedom of expression have been enacted. For instance, Proclamation on Freedom of Mass Media and Access to Information was promulgated in 2008 aiming at the realization of the right to access to information by requiring establishment of free media.[45] This proclamation has contribution in enhancing the right to access to information. But, in actual terms, the proclamation eroded freedom of expression by inviting actions like implicit political intervention that increases self-censorship.[46]

4. REGULATION OF INTERNET IN ETHIOPIA AND ITS IMPACT ON FREEDOM OF EXPRESSION

The computer crime proclamation limits freedom of expression online by providing, inter alia, provisions that prohibit computer data which contains contents that affect liberty and reputation of persons[47] and disturb the public.[48] It also provides criminal liabilities of internet service

[45] Freedom of Mass Media and Access to Information Proclamation, Federal *Negarit Gazeta* Proclamation No.590/2008, preamble.
[46]Getaneh Mekuanint, *An Examination of Freedom of the Mass Media and Information Proclamation (590/2008) Vis-àvis its Practices,* A Thesis Presented to Addis Ababa University (2013) *(unpublished).*
[47]Computer Crime Proclamation, Federal *Negarit Gazeta,* Proclamation No. 958/2016Article 13.

providers for the illegal contents produced by their users.[49] Limitation to online freedom of expression by itself is not wrong for computer networks provide ample opportunity for the propagation of scurrilous material about others. Some online conducts are hazardous for the wellbeing of the society and disturb peace and security of the public. But, such limitation has to be assessed in light of the three-part-test noted above.

4.1. Regulation of Content Data and Criminal Liability of Internet Service Providers

Internet may be abused to stalk or harass an individual, group or organization.[50]Cyber stalking is a wrongful act in which a person harasses a victim using electronic communication, such as e-mail or instant messaging or messages posted to a website or a discussion group. Although merely having the ability to do something does not necessarily motivate a person to carry out that action, the fact that cyberspace can support such behavior on pretext of anonymity and a false sense of power cannot be underestimated.[51] Thus, the response of a state through crafting anti-cyber stalking laws or amending traditional anti-stalking laws to account for technological advances in the internet and electronic communications is appropriate. Nevertheless, anytime speech is regulated, there exists the possibility that the law may infringe it. Therefore, an anti-cyber stalking law should be flexible enough to account for technological advances in the use of the internet and carefully crafted to ensure consistency with protections of freedom of expression.[52]

Some jurisdictions including ours criminalized online defamation.[53] Defamation can be defined as the wrongful, intentional publication or communication of words or behavior concerning another person which has the tendency to undermine his status, good name or reputation.[54] For a statement to be considered as defamation, the words complained of to be defamatory should refer to specific person and be published or communicated to at least one person other than the defamed person.[55] Some authors argue that due to availability of self-help mechanism on internet

---

[48]*Ibid* Article 14.
[49]*Ibid* Article 16.
[50]Michael Newton, *The Encyclopedia of High-Tech Crime and Crime-Fighting*, 74 (2002)
[51]Basu, S. and Jones, R.P., *Regulating Cyber stalking*, 2 JILT 1, 16 (2007).
[52]*Ibid*.
[53] Computer Crime Proclamation, *supra* note 47 Article 13 (3).
[54]SanetteNel, *Defamation on the Internet and other computer networks*, 30 The Comparative and International Law Journal of Southern Africa, 154, 155 (1997).
[55]TerKahLeng, *Internet defamation and the online intermediary*, 31Computer Law and Security Reviews 68 (2015).

for individuals who allege that their reputation is affected by statements of others to give counter speeches; online defamation should not be legally treated equally with its offline counterpart.[56] This argument was developed before invention of social networking platforms that came up with suitable systems to reply to any statement of users instantaneously. This shows that the argument holds water better in the current online communications. However, this argument gets some credence as long as there is reasonable expectation that the plaintiff is able to respond to the defamatory statement. But, the undeniable fact is that the ability to remedy the defamation by counter speech allows the person defamed on internet to keep his or her name intact than any other legal remedy.[57]

The other controversial issue in the regulation of cyber activities is about the responsibilities of Internet Service Providers (hereafter ISPs) with regard to the content data that are originally provided by the users and are made available on internet passing through services of ISP. ISPs provide complex technological infrastructure, consisting of different physical and logical elements that help communication on internet. ISPs are a broad range of actors, mainly private ones, who act as intermediaries by providing a range of internet services.[58] Nowadays, the networked society has stepped into the era of the internet platform, which is built by the ISP where the massive network services are provided and users are given with the authority to control their data online while the ISP plays only passive role.

There are various kinds of ISPs depending on the services they provide. An ISP may be access provider that connects an end user's computer to the internet, using cables or wireless technology, or also facilitating the equipment to access the internet. An internet access provider is a type of ISP that provides individuals and other ISP companies access to the internet.[59] Access providers are structured hierarchically to control the physical infrastructure needed to access the internet and make the infrastructure available to individual subscribers in return for payment.[60] They may or may not control content of the data that passes through their service depending on their purpose and terms of service. An ISP may also be a transit provider that allows interaction

[56] Jeremy Stone Weber, *Defining Cyber libel: A First Amendment Limit for Libel Suits against Individuals Arising from Computer Bulletin Board Speech*, 46 Cas. W. Res. L. Rev. 235,261 (1995).
[57] *Ibid* at 265.
[58] Bradley Mitchell, *ISP-Internet Service Providers*, October17,2016, available at https://www. lifewire.com/internet-service-providers-817781 accessed on May 11, 2017.
[59] http://searchmicroservices.techtarget.com/definition/IAP-Internet-access-provider accessed on March 27, 2017.
[60] Hossein Bidgoli, *The Internet Encyclopedia*, California State University Bakersfield, California, 199 (2004).

between a computer and the access provider, and hosting providers, and whose function is merely transmission of data, mere conduit role.[61] Internet transit is the business relationship whereby an ISP provides access to the global internet. Internet transit can be imagined as a pipe in the wall that says "internet this way".

Other types of ISPs are hosting providers. They are bodies, typically companies that rent web server space to enable their customers to set up their own websites. It may be any person or company who controls a website or a webpage which allows third parties to upload or post materials. Social media platforms like *facebook* and *twitter*, blog owners, and video and photo sharing services are usually referred to as hosts. A hosting provider has one or several computers with available space or servers, with access to transit providers, which may be used for its own purposes or for use by third parties, who make content available from other computers connected to access and transit providers. A hosting provider will offer technologies to feature content on the web, to send, receive and administer emails, store files, etc.

There have been two opposing positions regarding the role of ISP on the contents provided by their users. Proponents of network neutrality contend that ISPs should act as passive conduits rather than managing their networks actively and differentiate traffic, because such network management could negatively affect competition and freedom of expression.[62] Differently, skeptics of network neutrality tend to see more active network management as meeting a consumers' demand[63] and traffic differentiation as the only way for ISPs to safeguard a return of investment into next-generation internet architecture.[64]

In the modern world, regulation of cyber activities is important to achieve social, political and economic ends. Regulating internet without the involvement of ISP is unthinkable. But, gate keeping ISPs would have a negative effect on receiving and imparting information.[65] Concerning the regulation of cyber activities through ISPs, the UNHRC stated that any restriction on the

---

[61] *Ibid*

[62] Barbara Van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 Journal on Telecommunications and High Technology Law 329, 392 (2007).

[63] Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debat*e, 3 Journal on Telecommunications and High Technology Law 23, 68 (2004)

[64] Robert E. Litan& Hal J. Singer, Unintended Consequences of Net Neutrality Regulation) 5 Journal on Telecommunications and High Technology Law 533, 596 (2007).

[65] Jasper P. Sluijs, *From Competition to Freedom of Expression: Introducing Article10 ECHR in the European Network Neutrality Debate*, 12 HRLR 509, 554 (2012).

operation of ISPs is only permissible to the extent that it is compatible with the three-part-test.[66] Therefore, imposing blanket criminal responsibility on ISP is impermissible. No ISP that simply provides technical internet services such as providing access, or searching for, or transmission or caching of information should be liable for content generated by others disseminated using those services as long as it does not specifically intervene in that content or refuse to obey a court order to remove that content where it has the capacity to do so.[67]Here, it is noteworthy to mention that according to the general theory of criminal liability, anyone who participates in a crime in the capacity of author, accomplice and accessory after the fact may be held liable. Though all ISP may participate in some way in the transmission or diffusion of the information; it would be unfair to hold them all responsible for an offence. Therefore, cybercrime law should limit liability principally and sometimes solely to the person(s) directly involved in the infraction or damage.

The grounds for ISP's liability shall be subject to the role they played in producing the content. This is so because the unlawfulness may result from the communicative acts performed by individuals or businesses as originators of content. In most of the cases, intermediaries do not have the operational or technical capacity to review contents produced by third parties. Neither they have, and nor are required to have, the legal knowledge necessary to identify the cases in which specific content could effectively produce an unlawful harm that must be prevented. Even if they have the required number of operators and attorneys to perform such an undertaking, as private actors, intermediaries are not necessarily going to measure the value of freedom of expression when making decisions about third-party produced contents for which they might be held liable. If blanket liability is imposed on the ISP for the third party's content data that passes through their service, in view of their liability, they can be expected to end up suppressing all of the information they think, from any point of view, could potentially result in a judgment against them. A system of this kind would seriously affect small and medium-sized ISP, as well as those who operate under authoritarian or repressive regimes.

[66] General Comment Number 34 *supra* note 13, para. 43.
[67] Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, *Freedom of Expression and the Internet*, OEA/Ser.L/V/II CIDH/RELE/INF.11/13, 31 December 2013. para.97

There is an international consensus appeared to develop around the notion that holding ISP liable for third party's content of which they lack knowledge or control over is prejudicial to the functioning of electronic commerce and the exercise of freedom of expression.[68] If liability is assigned to ISP from the wrongful act of their users, this shows that the primary concern is not so much with guilt but with preventing or compensating for these negative consequences.[69] This kind of attributive liability introduces strict liability in regulation of cyber activities. Doing so affects the broadly shared and deeply felt intuitions regarding the individuality of responsibility and the relationship between responsibility and guilt, requirement of blameworthiness.[70] Even though strict criminal liability can be justified under criminal law when we see the whole activities done to commit the crime, it has chilling effect on freedom of expression.[71] If ISPs are made liable for the contents provided by the third parties, they will employ strict systems by which they check against prohibited contents.

International and regional human rights bodies established that online intermediaries should not be liable for third party's content as long as they do not specifically intervene in that content.[72] Subsequent reports of the UN Special Rapporteur on Freedom of Expression and regional human rights systems repeat this point emphasizing that the authors of unlawful speech should face the legal consequences of publishing it.[73] For these experts, requiring online intermediaries to monitor content hosted on their sites results in greater censorship and is inconsistent with the right to freedom of expression.[74] A group of international civil society organizations consolidated the ideas of aforementioned instruments into the "Manila Principles on Intermediary Liability," which also advocates a broad approach to protect ISPs from

[68]Lisl Brunner, *The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia*, 16, Human Rights Law Review, 163, 174 (2016).
[69] Anton Vedder, *Accountability of Internet access and service providers – strict liability entering ethics?*, 3 Ethics and Information Technology 67, 73 (2001).
[70]*Ibid*.
[71]Kenneth W. Simons, *when is Strict Criminal Liability Just*, 87 J. Crim. L. & Criminology 1075, 1137 (1997).
[72] General Comment Number 34 *supra* note 13, para. 43. See also the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, Joint Declaration On Freedom Of Expression And The Internet, (2011) at para 2.
[73] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 7 at para 102.
[74] Joint Declaration on Freedom of Expression and the Internet *Supra* note 72 at para 2(b);

liability.[75] Generally, there is international consensus on the fact that holding ISP liable for the content produced by third parties severely undermines the enjoyment of the right to freedom of expression, because it leads to self-protective and over-broad private censorship.[76]

However, if an ISP involves in editing of content data, this presupposes that the ISP not only has knowledge but also contributes to the illegal content. For instance, there are some webpages that provide access to some resources and take the role of editing the contents posted in the webpage. Therefore, such ISP could be considered as content provider hence, liable. Similarly, some ISP have terms of agreements to control the content of data which is passing through their services hence, have some duties on content data posted on their web. Such duties of the webmaster may include ensuring that the web servers, hardware and software are operating correctly, designing the website, generating and revising web pages, replying to user comments, and examining traffic through the site. In such cases, if they are made responsible for the third parties' data on their website, they can take measure against it. Likewise, social media hosts like Facebook page or group creators can control what are posted on their pages. In such cases, Facebook page can be compared to a noticeboard where third parties can post comments but the host has ultimate power to control postings and block users. Such hosts cannot be passive instruments or mere conduits of information. They can prohibit postage of illegal content. Accordingly, such hosts can be made responsible for they know about the illegality of the statement and can take measures against the data unless they thought to take responsibility for the statement.

4.2. Impacts of Internet Regulation on Freedom of Expression in Ethiopia

The Computer Crimes Proclamation comprises of six parts: i. General provisions dealing with definition of terms, ii. Provisions on computer crimes, iii. Preventive and investigative measures, iv. Evidentiary and procedural rules, v. Institutions playing a role in the prevention, detections and investigations of computer crimes, and vi. Miscellaneous provisions. The Proclamation touches a range of issues and creates a number of new criminal offenses that are likely to negatively impact on the exercise of freedom of expression. This section discusses the provisions of the proclamation that have negative repercussions on the enjoyment of freedom expression.

[75] Manila Principles on Intermediary Liability, Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation (24 March 2015), See also The Manila Principles on Intermediary Liability Background Paper, 30 May 2015, at 6–8: 20–1.

[76] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 7 at Para. 40.

As discussed above, according to the Constitution, freedom of expression cannot be limited on account of the content or effect of the point view expressed. As against this principle, the proclamation creates a number of offenses related to content under the caption of 'obscene or indecent crimes against minors', 'crimes against liberty and the reputation of persons', 'crimes against public security', and 'dissemination of spam'.[77]For instance, Article 13 establishes a series of offenses criminalizing 'intimidation' by disseminating any content; 'causing fear, threat, or psychological strain' by sending or repeatedly transmitting information about someone or by keeping their computer communication under surveillance; and disseminating any defamatory writing. The provisions are very general to capture as many conducts as possible. There is neither legal nor practical definition of "intimidation," "threatening" or "causing fear." Lack of clarity of these provisions has negative repercussions on free speech. Because, in normal course of things, people make rush comments in the heat of emotion with no intention of causing a harm but may be, he/she is simply exasperated by certain conditions.[78] It is unfair to label, for instance, comments made in such cases on internet as a crime and such criminalization may lead individuals to refrain from posting their ideas on other person under the pain of punishment.

Article 14 of the proclamation is affected by similar problems. It prohibits dissemination of content data that incites violence, chaos or conflict among people. But, as the phrases "incites violence," "incite chaos" or "incite conflict" are fluid, they can be interpreted to trample political discourses, critics directed towards corruption, dissents and debates among the people. As criminal categories provided under the provisions are directly related with freedom of expression, government authorities may interpret these provisions malevolently to deny discussions on matters of public concern.[79]Ethiopian civil societies have been voicing their concern that the law would be used to crackdown critical comment and political opposition.[80]

Practically, Ethiopian government has been claiming that social media platforms are disturbing security of the country. This accusation is primarily pointed to Facebook which seems almost

[77]Computer Crime Proclamation, *supra* note 46, Article 12-15
[78]Chuck Easttom& Det. Jeff Taylor, *Computer Crime, Investigation, and the Law*, 415 (Stacy L. Hiquet 2011).
[79]Halefom *supra* note 5.
[80] Kimberly Carlson, *Ethiopia's new Cybercrime Law allows for more efficient and systematic prosecution of online speech*, Electronic Frontier Foundation, June 9, 2016, available at https://www.eff.org/deeplinks/2016/06/ethiopias-new-cybercrime-law-allows-more-efficient-and-systematic-prosecution-online; accessed on April 2, 2017, Tinishu Soloman, *New Ethiopian law targets online crime*, The Africa Report, June 9, 2016, http://www.theafricareport.com/East-Horn-Africa/new-ethiopian-law-targets-online-crime.html accessed on April 2, 2017.

synonymous to internet.[81] Ethiopia ranks 7thout of the top ten African countries with the most Facebook users.[82]Facebook has played invaluable role in facilitating the 2015 Ethiopian election being the forum of political debates and discussions between the electorate and political parties' leaders and members.[83] It has also heightened protests in Oromia and Amhara states that forced the government of Ethiopia to declare state of emergency in 2017.[84] Exasperated by these challenges at home, the former Prime Minister of Ethiopia, Hailemariam Dessalegn, claimed before the UN General Assembly that social media has empowered populists and other extremists to exploit people's genuine concerns and spread their message of hate and bigotry without any inhibition.[85]Likewise, some also argued that social media have despoiled civility in Ethiopia.[86]But, these assertions were debunked by the empirical research conducted as there is practically insignificant number of hate speech communicated between Ethiopians through Facebook.[87]

Despite the fact that the words of Article 13 and 14 are vague, the drafters of the proclamation claimed that they have adopted a technology-neutral approach in drafting the substantive provisions asserting that such language allows the provisions to be applied to both current and future technologies in regulation of cybercrime.[88] Nevertheless, as the words of Articles 13 (1) and (2) and 14 are vague, they give no clear notice to individuals. Therefore, they fail the test of clarity and precision required from the law that limits freedom of expression.

Criminalization of defamation on internet by the proclamation has also a chilling effect on freedom of expression. It can lead to the imposition of harsh sanctions, such as a prison sentence, suspension of the right to practice journalism or a heavy fine. Even if it is applied with moderation like made punishable upon complaint and punishable by simple punishments, it still casts a long shadow to freedom of expression because, the possibility of being arrested by the police, held in detention and subjected to a criminal trial will be in the back of the mind of a

[81]Gagliardone, I. et al. *Mechachal: Online debates and elections in Ethiopia. From hate speech to engagement in social media* 16 (2016).and See Leo Mirani, *Millions of Facebook Users Have No Idea They're Using the Internet*, available at http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internetaccessed April 4, 2017.
[82]http://www.ethiocyberlaws.com accessed on April 4, 2017.
[83]Gagliardone, I. et al, *supra* note 81.
[84]Ezana Sehay, *How Social Media Is Despoiling Civility In Ethiopia*, available at http://www.ethiocyberlaws.com/
[85]http://www.un.org/apps/news/story.asp?NewsID=55022#.WN0vDmdlDIW accessed on April 5, 2017.
[86]Ezana Sehay *supra* note 84.
[87]Gagliardone, I. et al *supra* note 81.
[88]The Explanatory note of Computer Crime Proclamation, page 5.

person when he or she is deciding whether to expose, for example, a case of high-level corruption. Therefore, criminal law is not appropriate measure that a state has to take against online defamation as it has the capacity to enmesh free online expressions.

UNHRC has recognized the threat posed by criminal defamation laws on freedom of expression and recommended that defamation should be decriminalized. [89] Similarly, the African Commission on Human and Peoples' Rights adopted "Declaration of Principles on Freedom of Expression in Africa" that clearly and fully affirmed the three-part-test. [90] In deciding on communication brought before it, the Commission stated that the fact that a state can limit freedom of speech by laws does not mean that national law can set aside the right to express and disseminate one's opinions guaranteed at the international level.[91]By the similar understanding, the Commission adopted a resolution that called up on all African states to decriminalize defamation stating that criminal defamation laws constitute a serious interference with freedom of expression and impedes the role of the media as a watchdog, prevent journalists and media practitioners to practice their profession without fear and in good faith.[92]It is vivid that criminal defamation laws impose similar threat on bloggers, whistle blowers and human rights defenders on internet. African Court of Human and People's Rights has also ruled out criminalization of defamation in *Konate* V. *Burkina Faso case*.[93] Reasoning that the restriction of a right shouldn't destroy the essence of the rights guaranteed by the Charter, the court ruled that the Burkina Faso's law that provided sentence of imprisonment and fine for defamation violates freedom of expression.[94]

One may argue that the regulation of online defamation under the computer crime proclamation is right because internet has high capacity to disseminate defamatory statements to every corner of the world in fraction of seconds. But, such an argument is not compelling because of the following reasons. *First*, as much as internet facilitates swift dissemination of defamatory statement, it also affords a self-help mechanism for a person in similar capacity to do battle with

[89] General Comment Number 34 *supra* note 13, para 47
[90]*Declaration of Principles on Freedom of Expression in Africa*, African Commission on Human and Peoples' Rights, 32nd Session, 17-23 October 2002: Banjul, The Gambia.
[91]ACHPR, *Civil Liberties Organization and Media Rights Agenda v. Nigeria*, Comm. Nos. 140/94, 141/94, 145/95 (1999), para. 40.
[92] ACHPR, *Resolution on Repealing Criminal Defamation Laws in Africa*, Res 169(XLVIII) (2010).
[93]ACHPR, *LohéIssa Konatév. The Republic of Burkina Faso*, App. No. 004/2013, 5 December (2014).
[94]*Ibid*.

the statement made against him or her. *Second*, as argued by the human rights bodies, criminalization of defamation may terrify individuals thereby making them refrain from giving their valuable comments and suggestions about others. This undermines the essence of online freedom of expression. For instance, the works and behaviors of individuals, especially, of government officials may not be scrutinized by members of the public. This renders criminalization of online defamation too excessive measure in comparison to its adverse effects on the essence of freedom of expression. *Thirdly*, online defamation can be effectively controlled by tort law or administrative measures which have less threat to free speech. Accordingly, criminalization of online defamation doesn't pass the test of proportionality of limitation of freedom of expression. Hence, both the positive and the negative justifications for criminalization of online defamation are missing.

The proclamation also provides for criminal liability of ISP. However, assigning criminal liability to ISP for content created by third parties has adverse effect on freedom of expression. The proclamation provides broader definition for ISP. It defines service provider as a person who provides technical data processing or communication service or alternative infrastructure to users by means of computer system.[95] In Ethiopia, Ethio-Telecom is the sole ISP that controls everything regarding internet in the country; private sectors like internet cafes,[96]web hosts and blog owners can provide value added services or act as a reseller by obtaining a license.[97] Oversea ISPs like Facebook, Google, and Twitter are also subjected to the law.[98]

In many national laws and international human rights law, it is a well-established principle that ISPs 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.[99]Thus, technical ISP should not be held criminally responsible in the event that it unknowingly distributes or hosts unlawful content created or uploaded by third party users. Despite this well-established principle of immunity of

[95] Computer Crime Proclamation *supra*47 Article 2(14)
[96]Ministry of Communication and Information Technology of the Federal Democratic Republic of Ethiopia, 1 Communication and Information Technology Statistical Bulletin 4 (2014).
[97]Ministry of Communications and Information Technology, *License Directive for Resale and Tele center in Telecommunication Services Directive,* Directive No. 1/2002.
[98] Computer Crime Proclamation *supra* note 47, Article 42. This provision adopted principle of internationality that helps to regulate cybercrimes from every corner of the world.
[99] Kinfe Micheal and Halefom Hailu, *The Internet and Ethiopia's IP Law, Internet Governance and Legal Education: An Overview,* 9MLR 154, 161 (2015).

the ISP for third party contents, the Computer Crime Proclamation made them criminally liable under various conditions. The first statement of Article 16 (1) of the proclamation makes an ISP liable if it is directly involved in the dissemination of the illegal content. The proclamation failed to define "direct involvement." It may mean direct participation in the dissemination of ready-made content data. But from the general theory of criminal liability,[100]one can learn that ISPs which play a role in providing access to third party content without knowing the content of that data shall not be considered as content publishers and made liable. For instance, Web hosts which facilitate publication of internet blogs and comments, though they are involved in the dissemination of the information, cannot be treated as publishers of the blogs.[101] This is because they are not involved in the postings of the blogs or comments which are made by independent parties from the web host.

In normal course of things, ISPs which are mere passive conduits of a data do not seek to exercise prior control over it nor do they have effective control over its content. Therefore, there is no moral ground to make a person involved only in dissemination of a data responsible unless that person knew or ought to know that the information disseminated is illegal.[102]Nevertheless, Article 16(1) of the proclamation deviates from this by making ISP criminally responsible for `directly` involving in the dissemination of some illegal content data without having knowledge of its content. Applying this rule to the internet access providers, hosts and transits, which by their very nature do not contribute to the content or do not know or expected to know the content of data, is simply preposterous. Yet, the broad definition of the ISP under the proclamation makes dissemination of the illegal content data by ISP with no prior knowledge of the content produced by third party punishable. This entails contradiction with the basic theory of criminal liability and tramples on the essence of freedom of expression and right to privacy as ISP would desist providing internet service in Ethiopia or simply try to censor each content of the users` data that pass through. This makes the provision short of passing the three-part-testas criminalization of ISP without cognizance of its content is not necessary in the democratic society.

[100]George P. Fletcher, *The Theory of Criminal Liability and International Criminal Law*, 10 JICJ 1029, 1044 (2012).
[101]Ter Kah Leng, *Internet defamation and the online intermediary*, 31 computer law & security review, 68,77 (2015).
[102]*Ibid*.

Article 16 (2) of the proclamation makes an ISP criminally liable if it had actual knowledge as to illegality of a content data passed through its service and failed to take measures to remove or disable access to the data. "Actual knowledge," provided here as a condition to assign criminal liability, is not clear. Where the ISP have actual knowledge of the illegality of the data, whatever it means, it is unnecessary to make it liable for the crime. Because, this puts private ISPs in the position to make decisions about the lawfulness or otherwise of the content and to protect themselves from liability and apply their maximum effort to censor data of their users. The strategic position they occupy in the communication networks prompts ISPs to employ a range of software solutions to reduce offending online data by using robust security systems.[103]Under such regime, in addition to being wary of their potential legal liabilities, ISPs are also fearful of any negative publicity that might arise from their failing to be seen to act responsibly.[104]

Article 16 (3) of the proclamation alike provides problematic provision that undermines freedom of expression and right to data privacy. It tries to adopt mechanism of notice and take down to prevent computer crime. According to mechanism of "notice and take down," in exchange for protection from liability, ISP are required to take down content data that a third party alleges to be unlawful. This procedure normally requires authorization from a qualified judicial organ to determine the legality of the content data. Nonetheless, the proclamation simply mandates administrative authorities to rule on legality issues and order the ISP to remove or disable access to the data where illegality is established. This usurps the courts` inherent judicial power conferred by the constitution.[105] Furthermore, administrative authorities cannot be fair and impartial in determining the legality of the contents of the data. Nor are they competent to handle the matter. Thus, contents which are legal may be simply removed due to erroneous decisions or for political motives. The fact that proclamation fails to provide for the right to appeal against such administrative decision exacerbates the problem. In the circumstances, the procedure of `notice and take down` envisaged in the proclamation is likely to invite arbitrary encroachment of freedom of expression.

[103] Wall, D.S. *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace* (Revised May 2011), 8 Police Practice & Research: An International Journal, 183 (2007/11).
[104]*Ibid*.
[105] FDRE Constitution *Supra* note 43 Article 78.

That said, mechanism of notice and take down itself has also its own pitfalls. Even assuming that the order to take down after the appropriate judicial organ decides the illegality of the content is in line with freedom of expression, it is unfair to take down one's data without providing fair hearing. The individual must be given fair notice to appear and explain the legality of his/her data before taking it down. To do away with the problem of mechanism of notice and take down, some states, typically, Canada, developed a human rights friendly system called "Notice and Notice" which dictates that the ISP shall not take down what users uploaded. Rather, after being notified by the competent judicial organ, ISPs are duty bound to notify the person that uploaded the content to do so.[106]This system is also buttressed under Manila Principles.[107] Nevertheless, the proclamation failed to provide the minimum guarantee that the mechanism of notice and take down provides.

Article 27 of the proclamation imposes the duty to report the commission of cybercrime on ISPs when they come to know certain cybercrime is committed through their services.[108] Accordingly, ISPs are required to report to the investigative authority when they come to know commission of cybercrimes on their computer systems. Actually, this provision was drafted on the assumption that every ISP has the knowledge of content data that passes through its service.[109]However, as it is discussed somewhere in this article, most of the internet service providers are not in a position to know the content of the data through their services. The repercussion that such obligation can bring is that it has the potential to prompt service providers to preemptively monitor communications on their networks under the pain of facing penalties for non-cooperation.[110]

5. CONCLUSION

Considering its openness to be easily abused, Ethiopia has been trying to regulate internet since 2004, the computer crimes proclamation being the leading cyber law. Nonetheless, this proclamation has some provisions that have negative impacts on freedom of expression. Provisions of the proclamation that are sought to protect individuals' and the public rights provide vague words and surreptitious phrases that can be abused by government authorities.

[106] http://www.entertainmentmedialawsignal.com/online-infringement-canadian-notice-and-notice-vs-us-notice-and-takedown accessed on March 27, 2017.
[107] Manila Principles on Intermediary Liability *supra* note 75.
[108] Computer Crime Proclamation, *supra* 47 Article 27.
[109]The Explanatory Notes of Computer crime Proclamation at 37.
[110]Kinfe Micheal, *Some Remarks on Ethiopia's New Cybercrime Legislation*, 10 MLR 448, 453 (2016).

This indicates that they fail to fulfill standard of limitation of freedom of expression which requires clear and precise law.

The proclamation has criminalized online defamation. However, given the silencing effects of the criminal sanctions on freedom of expression, criminal law is not appropriate tool to regulate online defamation. Basically, internet has provided a self-help mechanism through which defamed persons can sustain their reputation. If that is not enough to correct the wrong behavior, civil remedies can be sought. Therefore, the sanctions of criminal law on internet defamation constitute unnecessary and disproportionate measures on the exercise of freedom of expression with regard to matters of public interest.

The proclamation also makes ISP criminally liable in principal capacity when certain illegal content data is transmitted through their services. Nevertheless, such regulation would compel ISPs to limit free speech subjectively under the pain of prosecution. It also allows administrative authorities to rule over legality of content data and order their removal. This may enhance arbitrary obstruction of political sensitive speeches. Such blanket criminalization attracts arbitrary blocks of individual's data by ISPs and unnecessarily limits freedom of expression.

BIBLIOGRAPHY

A. Journal Articles and Books

- Anton Vedder, *Accountability of Internet access and service providers – strict liability entering ethics?,* 3 Ethics and Information Technology 67 (2001).
- Barbara Van Schewick, *Towards an Economic Framework for Network Neutrality Regulation,* 5 Journal on Telecommunications and High Technology Law 329 (2007).
- Basu, S. and Jones, R.P., *Regulating Cyber stalking*, 2 JILT 1 (2007).
- Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debat*e, 3 Journal on Telecommunications and High Technology Law 23 (2004),
- Gary Slapper, *Clarity and the Criminal Law*, 71The Journal of Criminal Law, 475 (2016).
- George P. Fletcher, *The Theory of Criminal Liability and International Criminal Law*, 10 JICJ 1029 (2012).
- Jasper P. Sluijs, *From Competition to Freedom of Expression: Introducing Article10 ECHR in the European Network Neutrality Debate*, 12 HRLR, 509 (2012).
- Jeremy Stone Weber, *Defining Cyber libel: A First Amendment Limit for Libel Suits against Individuals Arising from Computer Bulletin Board Speech*, 46 Cas. W. Res. L. Rev. 235 (1995).
- Johanna Granville, *Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions, 49* Australian Journal of Politics and History 102 (2003).
- Kenneth W. Simons, *when is Strict Criminal Liability Just*, 87 J. Crim. L. & Criminology 1075 (1997).
- Kinfe Micheal & Halefom Hailu, *The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media,* 9MLR 108 (2015).
- Kinfe Micheal and Halefom Hailu, *The Internet and Ethiopia's IP Law, Internet Governance and Legal Education: An Overview*, 9MLR 154 (2015).
- Kinfe Micheal, *Development in Cybercrime law and practice in Ethiopia*, 30 Computer Law and Security Review 720 (2014).
- Kinfe Micheal, *Some Remarks on Ethiopia's New Cybercrime Legislation*, 10 MLR 448 (2016).

- Larry Alexander, *Is There a Right of Freedom of Expression?*,8 (Cambridge University Press 2005).
- Lisl Brunner, *The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia*, 16, Human Rights Law Review 163 (2016).
- Michael Newton, *The Encyclopedia of High-Tech Crime and Crime-Fighting* 74 (2002)
- Michael O'Flaherty, *Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment Number 34*, 12 HRLR 627 (2012),
- Molalign Asmare, *Computer Crimes in Ethiopia: An Appraisal of the Legal Framework*, 3 International Journal of Social Science and Humanities Research 92 (2015).
- Nils Jareborg, *Criminalization as Last Resort (Ultima Ratio),* 2 Ohio St. J. Crim. L. 521 (2005).
- Robert E. Litan & Hal J. Singer, Unintended Consequences of Net Neutrality Regulation) 5 Journal on Telecommunications and High Technology Law 533 (2007).
- Sanette Nel, *Defamation on the Internet and other computer networks*, 30 The Comparative and International Law Journal of Southern Africa 154 (1997).
- Tara Vassefi, *An Arab Winter: Threats to the Right to Protest in Transitional Societies, Such as Post-Arab Spring Egypt*, 29 American University International Law Review 1097 (2014).
- Ter Kah Leng, *Internet defamation and the online intermediary*, 31 computer law & security review 68 (2015).
- Wall, D.S. *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace* (Revised May 2011), 8 Police Practice & Research: An International Journal, 183 (2007/11).
- Wojciech Sadurski, *Freedom of Speech and Its Limits* (1999).

B. Laws

- Computer Crime Proclamation, Federal *Negarit Gazeta*, Proclamation No. 958/2016
- .Constitution of the Federal Democratic Republic of Ethiopia, Federal *Negarit Gazeta*, Proclamation No. 1/1995
- Freedom of Mass Media and Access to Information Proclamation, Federal *Negarit Gazeta*, Proclamation No. 590/2008.

- Ministry of Communications and Information Technology, *License Directive for Resale and Tele center in Telecommunication Services Directive*, Directive No. 1/2002.
- International Covenant on Civil and Political Rights Adopted And Opened for Signature, Ratification and Accession by General Assembly Resolution 2200a (XXI) of 16 December 1966.