JIMMA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE

SCHOOL OF LAW

HUMAN RIGHTS AND CRIMINAL LAW PROGRAMME

REGULATION OF CYBER ACTIVITIES IN ETHIOPIA: APPRAISAL OF COMPUTER CRIME PROCLAMATION IN LIGHT OF FREEDOM OF EXPRESSION AND RIGHT TO DATA PRIVACY

BY; DAGNE JENBERE TEREFE

JUNE, 2017

Regulation of Cyber Activities in Ethiopia: Appraisal of Computer Crime Proclamation in Light of Freedom of Expression and Right to Data Privacy

A Thesis submitted to Jimma University College of Law and Governance the School of Law in partial fulfillment of the requirements of LL.M. Degree in Human Rights and Criminal Law

BY: Dagne Jenbere

As advised by Dr. Alemu Miheretu Negash (Assistant Professor of Law)

June, 2017

Declaration

I, Dagne Jenbere Terefe, do hereby declare that the thesis "Regulation of Cyber Activities in Ethiopia: Appraisal of Computer Crime Proclamation in Light of Freedom of Expression and Right to Data Privacy" is my original work and that it has not been submitted for any degree or examination in any other University. Whenever other sources are used or quoted, they have been duly acknowledged.

Dagne Jenbere Terefe

Signature: _____

Date_____

Approval

The undersigned certify that they have read and hereby recommend to the Jimma University to accept the Thesis submitted by Dagne Jenbere entitled "Regulation of Cyber Activities in Ethiopia: Appraisal of Computer Crime Proclamation in Light of Freedom of Expression and Right to Data Privacy "in partial fulfillment for the award of Master of Laws (LL.M) degree in Human Rights and Criminal Law.

By: Dagne Jenbere

Approved by Board of Examiners

Advisor: _____ Signature: _____

Date:_____

Examiner: _____ Signature: _____

Date:_____

Head of College: _____ Signature: _____

Date:_____

Head of Department: _____ Signature: _____

Date:_____

Acknowledgement

First and foremost, praise is to my almighty God for without whom I would not have accomplished this work. I would like to express my sincere gratitude to my advisor Dr. Alemu Miheretu for his guidance and support in developing the thesis in a more sensible way. I have immensely benefited from his selfless and tireless commitments at all stages of the research work. Without him, it would have been very difficult to complete this thesis like it appears here. Finally, I would like to thank my family and friends who have been keeping me strong.

Thank you all!

Glossary of Abbreviations

ACHPR	African Charter of Human and Peoples' Rights or African Commission of Human and Peoples' Rights or African Court of Human and Peoples' Rights *mutatis mutandis*
UNESCO	United Nations Educational, Scientific and Cultural Organization
ETC	EthioTelecom
FDRE	Federal Democratic Republic of Ethiopia
HRW	Human Rights Watch
INSA	Information Network Security Agency
ISP	Internet Service Providers
ITU	International Telecommunication Union
MCIT	Ministry of Communication and Information Technology
OECD	Organization for Economic Co-operation and Development
UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Committee or United Nations Human Rights Council *Mutatis Mutandis*
USA	United States of America

Table of Contents

Abstract

Before promulgation of the Computer Crime Proclamation, Ethiopia did not have comprehensive computer crime law that could regulate computer abuse except six articles of the Ethiopian Criminal Code that tried to regulate few aspects of computer abuse; Anti-terrorism Proclamation that regulated cyber terrorism and Telecom Fraud Offence Proclamation that deals with frauds committed through the use of telecom networks and service. The Computer Crime Proclamation entered into force as of July 7, 2016 by repealing the computer crime provisions of the code but leaving the provisions of the proclamations intact.

Although it provides important provisions to protect individuals' rights and cyber security that the code lacks, the proclamation created new controversial cybercrimes such as criminalization of online defamation and criminal liability of ISP that negatively affect freedom of expression and right to data privacy. It regulates cyberstalking and cyber security by vague provisions. It also provides wide discretion to investigative authorities to carry out warrantless sudden searches for real-time collection of evidence for preventive purposes without requiring them to establish whether the process is necessary and proportionate before an independent organ; order retention and collection of communication without warrant and extend the scope of a search warrant in some cases. Though the proclamations is not yet practically tested, this thesis exposes it to strict scrutiny under the standards of limitation of freedom of expression and right to data privacy. Though freedom of expression and right to privacy can be limited under limitation clauses provided in the FDRE Constitution and Human Rights Instruments that Ethiopia has ratified, by applying a normative legal research methods, this research found that Articles 13, 14, 16, 25(3), 30 and 32 of the Computer Crime Proclamation have irrationally, illegitimately and unnecessarily restricted freedom of expression and right to data privacy.

CHAPTER ONE

INTRODUCTION

1.1. Background to the Study

Computer is one of the fruits of scientific developments which has invaluable role in modern world, *inter alia*, in facilitating swift and simplified communication among persons in different corners of the world through Internet. Internet has evolved from a closed network called the Advanced Research Projects Agency Network (ARPANET)[1] which was available to a limited number of United States' officials and universities to a worldwide network almost available to anybody, through the World Wide Web.[2] The huge and complicated communications created by computer systems not only facilitated easy communications in today's world but also paved the way for culprits to commit crime with intricate systems in which it is difficult to apprehend them. Therefore, legislation of computer crime law is important, though not the sole measure, to protect cyber security and individuals' rights on internet.

There is no universally agreed definition for "cybercrime". But, in a general sense, cybercrime is an act that covers the entire range of crimes which involve computer, computer network, cell phones, etc., either as its target or as an instrumentality or associate.[3] Thus, broadly speaking, any kind of criminal activity that takes place with the help of or against these electronic devices in the given cyber space comes under the purview of the cybercrime. On the other hand, some authors argue that it is data and not the computer system *per se* that is the target of cybercrime.[4]

However, technically speaking, a computer abuse can be one of the three different types in which computer is involved in a crime.[5] In the first type, computer is the direct object of the illegal act. This typifies computer abuse against the computer hardware. In the second type, the computer is used as the instrument of the offense. These are offenses in which electronic

[1] http://www.livinginternet.com/i/ii_arpanet.htm accessed on January 2, 2017.
[2] Xavier Amadei, *Standards of Liability for Internet Service Providers: A Comparative Study of France and the United States with a Specific Focus on Copyright, Defamation, and Illicit Content,* 35 Cornell International Law Journal 1 (2002).
[3] Pramod Kr. Singh, *Laws on Cybercrimes*, 6 (2007).
[4] Peter Stephenson, *Investigating Computer-related Crime: Handbook for Corporate Investigators* 4 (2000).
[5] https://www.coursehero.com/file/p2fomsb/Computer-Crimes-The-term-computer-crime-refers-broadly-to-any-wrongful-act-that/ accessed on January 2, 2017.

data processing equipment is used to commit other offenses that in the past could not have been committed without physically removing something or entering the premises of the victim. It is this type of computer crime that presents virtually all the unique legal questions. In the new "paperless office,"[6] proprietary information stored in a computer memory or on an electronic medium can be accessed, altered, stolen, and sabotaged without the perpetrator's being physically present or resorting to the use of force. The third type is when a computer is used as the subject of the offense. This typifies an offense in which computer is used to commit traditional crimes like child pornography, copyright infringement, identity theft etc.

Among all types of computer crimes, it is the intangible electronic impulse nature of computerized information that has caused the greatest concern in the legal community over possible loopholes in criminal law. Because, it cannot be regulated under the traditional substantive and procedural criminal laws. Accordingly, the large scale use of internet and computer network in the day-to-day human lives has made the subject of computer crimes a matter of interest, popularity and, sometimes, points of debate.

Ethiopian cybercrime jurisprudence seems under developed because of the country's short history of computer and internet penetration.[7] The 2016 World Internet Stats shows that there are about 4.2 million internet users in Ethiopia and that is only 4.2% out of the current total population of Ethiopia.[8] The pace of regulation of cyber activities in the country hadn't been as quick as the development of computer systems in the country. Internet started to be used in the country as of 1997.[9] The 1957 Penal Code, the then incumbent criminal law, had no computer specific provisions to deal with computer misuse conducts.

The FDRE Criminal Code that came up in 2004, *inter alia*, to protect cyber security has provided short list of computer crimes which are short of regulating the complicated cybercrime as far as their scopes and substance are concerned. For one thing, the code provides

[6]Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 criminology 101,111 (1988).
[7]Kinfe Micheal, *Development in Cybercrime law and practice in Ethiopia*, 30 Computer Law and Security Review 720 (2014).
[8]http://www.internetlivestats.com/internet-users-by-country/accessed on December 21, 2016.
[9]Kinfe Micheal & Halefom Hailu, *The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media,* 9MLR 108, 129 (2015).

limited cybercrimes (only computer hacking, spreading malware and denial of service)[10] accordingly, wrongful cyber activities like computer-related forgery, fraud and identity theft, child pornography and spamming were not criminalized. Given the nature, type, impact, and targets of cybercrimes and criminals, it is possible to conclude that computer abuses were not carefully and sufficiently criminalized under the code according to their unique nature, impacts, and the provided punishments are disproportionally lenient.[11] The code treated cybercrime as property crime and provided lenient punishment if they are committed.[12] On the other hand, the old Ethiopian Criminal Procedure Code, doesn't provide for the procedures and the evidence rules which are capable to investigate and prosecute cybercrimes.[13]

In response to the under regulation of cyber activities, Ethiopia has been taking some policy and legislative measures. Ethiopia has come up with the National Information and Communication Technology Policy and Strategy in 2009 (ICT Policy) and Criminal Justice Policy of 2011. The main objectives of the ICT policy are: to address the national security implications arising from widespread application of ICT within the economy and the society; to secure and safeguard the national electric communication system and protect both data and network integrity; and to prevent, detect and respond to cybercrime and abuse of ICT so as to contribute to fight against national, regional and international crimes.[14] More importantly, the full implementation of the Criminal Justice Administration Policy requires many changes and additions to the existing law, in particular the criminal code, the criminal procedure code, and existing law concerning criminal evidence.[15] In addition to the main changes explicitly required by the new policy, it has a great concern about computer and cybercrimes. The objective of the policy concerning cyber activities may be summarized as securing the

[10] Ethiopian Criminal Code, Federal *Negarit Gazeta*, Proclamation No. 414/2004 Articles, 706, 707 and 708 respectively.
[11]Molalign Asmare, *Computer Crimes in Ethiopia: An Appraisal of the Legal Framework*, 3 ISSN 92,103 (2015).
[12]Halefom Hailu, *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*.
[13]Kinfe *supra* note 7 at 721.
[14] See the Ethiopia National Information and Communication Technology Policy and Strategy, (2009).
[15] See the Federal Democratic Republic of Ethiopian Criminal Justice Administration Policy, Ministry of Justice, (2011).

government and the society from computer crimes and to prevent computer crimes proactively and take appropriate measures if once committed.[16]

In response to the need of new legislation, on July 7th of 2016, Ethiopian parliament has promulgated computer specific law, Computer Crime Proclamation No. 958/2016. However, the proclamation had been encountering many challenges at its draft stage. The challenges include its overlapping provisions with the Anti-terrorism and Telecom Offence proclamations and its provision regarding prohibition of uploading and dissemination of information that incites fear on Internet. The part of the draft that criminalizes disseminating information that incites fear, that faced strong challenge at the draft stage, is dropped from the promulgated version of the proclamation. That part of the draft had been viewed as sandwiching the thorny provisions of the controversial anti-terrorism proclamation that has been criticized for having chilling effect on individuals' freedom of expression and lead to suppression of speeches that have contents of opinions of persons and criticisms or expressing one's dissent on the governing party.[17] The proclamation also repealed the cybercrime provisions of the criminal code and provided too much different provisions from the computer crime provisions of the code, different conditions for liability of wrongdoers by computers or computer systems and rules for procedure and evidence in computer crime proceeding. The proclamation left overlapping provisions that exist in Anti-terrorism and Telecom Offence proclamations intact.

Concerning the nomenclature, Ethiopian legislature chose "computer crime" instead of "cybercrime" or any other nomenclature given to computer abuse. This may be due to the fact that the nomenclature "cybercrime" focuses on the involvement of computer network[18] whereas "computer crime" seems broader and includes all crimes that involve computers in the process, even elicit acts in relation to stand-alone machines. [19]

[16] Molalign *supra* at 98.
[17] See http://allafrica.com/stories/201604261343.html Accessed on January 9, 2017.
[18] Lawrence F. Young, *United States Computer Crime Laws, Criminals and Deterrence*, 9 International Review of Law, Computers & Technology 1, 16 (1995).
[19]Gercke M, *Understand Cybercrime: A guide for developing countries* 2 (2011).

1.2. Literature Review

As far as literature on cyber regulation in Ethiopia is concerned, the works of Kinfe Mecheal are important. He has published many articles related to this study individually and with his co-authors, in different journals. In the article titled as *Developments in Cybercrime law and Practice in Ethiopia*[20] he commented on the draft of the current computer proclamation and argued that it should unify cybercrime provisions scattered in other Ethiopian laws like, Telecom Fraud Offense Proclamation, Advertisement Proclamation and Anti-terrorism proclamation.[21] Additionally, he required the draft to regulate revenge porn which was not considered in the draft.[22] He affirmatively argued that the draft of the proclamation under study respected right to privacy as it allows warrantless investigation only in exceptional circumstances.[23] Differently, the concern of this this study is to search if there is any guarantee in the proclamation that protects the authority from encroaching to individuals' righto privacy. Hence, the study wants to inquire validity of such arguments. Even, the above mentioned author himself, under the article he wrote with Alebachew which is titled as *Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices*, has argued that the 'sudden search' may pose a threat to the constitutional right to privacy and recommended that such a search should be conducted upon judicial authorization.[24] As oppose to the author's idea in the first article, the researcher wants to study whether outlawing the warrant requirement in real-time collection of computer data is sound and in line with standards of limitation of right to privacy of the suspect in investigation of crime.

Concerning liability of ISPs such as search engines, websites, ISPs, and hosting services providers, Kinfe and Hailefom in their common article, titled as *The Internet and Ethiopia's IP Law, Internet Governance and Legal Education: An Overview*, argued that the issue falls under different legal regimes with the potential risk of unnecessary overlaps and redundancies

[20] Kinfe Mecheal, *Developments in Cybercrime law and Practice in Ethiopia*, 30 Computer Law and Security Review 720, 735 (2014). The same Article with significant changes but with similar author was also published under Hawassa University Annual Research Review Workshop. See Kinfe Micheal, *Developments in Cybercrime Law and Practice in Ethiopia*, Hawassa University, Annual Research Review Workshop, College of Law & Gov. 94, 128 (2015).
[21] *Ibid* at 733.
[22] *Ibid*.
[23] *Ibid*.
[24] Kinfe Micheal & Alebachew Birhanu, *Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices*, 26 JEL 94, 152 (2013).

between laws that regulate the matter.[25] They feared such case will increase risk of 'over legislation' and bring the problems of interpretation, administration and enforcement of the laws.[26] Thus, their fear was over legislation but the problem that the researcher wants to study in this research, regarding ISP, is whether imposing criminal liability on them indirectly affects freedom of expression and right to privacy.

After promulgation of the proclamation, Kinfe has written an article called, *Some Remarks on Ethiopia's New Cybercrime Legislation*.[27] In that article he has discussed those human rights that are threatened by the proclamation in few paragraphs.[28] Though the article raises some provisions of the proclamation which are also focus of this study because they seem to contradict with human rights of individuals, unlike the article, this study wants to enter into detail assessment of the provisions in light of the human rights obligations Ethiopia bears and standard of limitation of those human rights.

Molalign Asmare has also written an article titled as *Computer Crimes in Ethiopia: An Appraisal of the Legal Framework*.[29] The article addressed issues of computer crime provisions of the Criminal Code, the 2009 ICT Policy and the 2011 Criminal Justice Policy of Ethiopia. Though what he recommended in the article had been positively addressed in the draft of the computer crime proclamation two years before publication of the article, parts of the article that deal with historical development of computer crime regulation in Ethiopia are important. This study is assessment of the computer crime proclamation which was not touched by Molalign.

1.3. Statement of the Problem

Though criminal law is often perceived as most relevant law to regulate cyber security, possible legal responses also include the use of civil law and administrative law. Despite the important developments at international, regional and national levels to regulate cyber activities, debates continue to exist on as to compatibility of the legislations with human rights. On one hand, no

[25] Kinfe Micheal & Halefom Hailu, *The Internet and Ethiopia's IP Law, Internet Governance and Legal Education: An Overview*, 9 MLR, 154, 160 (2015).
[26] *Ibid*.
[27] See Kinfe Micheal, *Some Remarks on Ethiopia's New Cybercrime Legislation*, 10 MLR, 448, (2016).
[28] *Ibid*.
[29] Molalign, *Computer Crimes in Ethiopia: An Appraisal of the Legal Framework supra*.

country can remain a silent when the very existence, peace, law and order, etc., of such countries is under threat. On the other hand, individuals' human rights and contribution of computer system to the every aspect of development in the state should not be undermined by inappropriate and irrational laws.

Computer crime laws are often justified on the basis of protecting individuals' reputations, national security or countering terrorism. But in practice, it is seen while governments use them to censor content that the government and other powerful entities do not like or agree with.[30] On the other hand, criminal law comes to picture as a last resort due to its strong impact on human rights.[31] Accordingly, not all misbehavior in cyber activities require criminal law. Particularly, the range of cyber activities that the state may wish to regulate will not always require the use of intrusive criminal law measures because, minor infringements can be regulated under civil or administrative law.[32] In regulating cyber activities by criminal law, criminalization of certain conduct is controversial. Where a strong justification for the criminalization of a particular conduct does not exist, a risk of over criminalization arises. This seeks internal and external standards against which the process of criminalization should be checked.

Despite its effort to overcome various problems, the computer crime proclamation encountered many challenges from human rights scholars and NGOs since its promulgation. Article 19, a British human rights NGO that defends freedom of expression and opinion,[33] found the proclamation as human rights unfriendly as it doesn't observe standards of limitation of the right to freedom of expression and data privacy.[34] Legitimate standards of limitation of freedom of expression and opinion according to Article 19(2&3) of ICCPR and *Siracusa* principles[35] require that the prescription of limitations shall be provided by a law, to achieve legitimate aim and necessary in a democratic society. The United Nations Human Rights

[30] 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.
[31] Nils Jareborg, *Criminalization as Last Resort (Ultima Ratio)*, 2 Ohio St. J. Crim. L. 521 (2005)
[32] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* 52 (2013).
[33] https://www.article19.org/ accessed on January 4, 2017.
[34] https://www.article19.org/resources.php/resource/38450/en/ethiopia:-computer-crime-proclamation accessed on December 21, 2016.
[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).

Committee under its General Comment 34 stated that any restriction on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as ISPs or search engines, are only permissible to the extent that they are compatible with paragraph 3 of Article 19 of ICCPR.[36] The committee also commented that defamation laws must be crafted with care to ensure that they comply with paragraph 3, and that they do not serve, in practice, to stifle freedom of expression.[37] The committee insisted that all such laws, in particular penal defamation laws, should include such defenses as the defense of truth and they should not be applied with regard to those forms of expression that are not, of their nature, subject to verification.[38] In order to check whether the proclamation has limited freedom of expression and right to data privacy validly, this study assesses some provisions of the proclamation in light of these criteria.

The computer crime proclamation, like any legislation relevant to cybercrime, addresses a wide range of issues, including: criminalization of particular conduct; power of investigative powers; issues of criminal jurisdiction; admissibility of electronic evidence; data protection responsibilities of electronic service providers; and mechanisms of international cooperation in criminal matters involving cybercrime. Although it provides important provisions to protect cyber security that the code lacks, the proclamation created new controversial computer crimes (such as incrimination of online defamation and criminal liability of ISPs) that seem to have chilling effect on freedom of expression online and procedural rules that affect right to data privacy.

Some provisions of computer crime proclamation seem to take away the remaining breathing space for most Ethiopians, online freedom of expression, as the offline one is diminished by the recent proclamations.[39] The glimpse of some provisions of the proclamation, especially, that are sought to regulate online data content seem vague as a result may criminalize legitimate

[36] UNHRC, *Article 19: Freedoms of opinion and expression, General comment No. 34,* 102nd session**,** Geneva, 11-29 July 2011.
[37] UNHRC, *concluding observations on the United Kingdom of Great Britain and Northern Ireland*, (CCPR/C/GBR/CO/6) (2008).
[38] *Ibid*.
[39] See section 2.1.3.2 of this thesis *infra*.

dissent of a person or his/her opinion against someone without requiring intent to harm.[40] The proclamation makes ISPs criminally responsible if they directly involve in dissemination of the prohibited conducts.[41] It also obliges them to take measures against illegal content data that are uploaded by Internet users.[42] By doing so, it gives power to determine legality or illegality of content data to ISPs and administrative authorities. It is important to check the effect of these legislative measures on Internet user's freedom of expression. Why we should oblige ISP, most of the times, which are private entities, to decide over legality or otherwise of data content? After all, are ISPs or administrative authorities appropriate organ to decide over legality or otherwise of a content data? This study exposes Article 16 of the proclamation to these questions and test whether it passes scrutiny under the standards of limitation of freedom of expression and right to data privacy.

The proclamation also introduced procedural rules for the investigation and prosecution of cybercrimes that have potential to harm freedom of expression and right to data privacy as it allows the investigatory organ to carry out warrantless 'sudden searches' and surveillance of suspected computers for preventive purposes without requiring them to establish whether the process is necessary and proportionate.[43] Search without warrant could be allowed in some exceptional cases to avoid delay that may result in impediment of justice[44] but it is equally essential to guarantee protection of innocent individuals' privacy. The proclamation also empowers the investigatory organ to extend the scope of the warrant obtained for searching and seizing computer and computer system in some cases.[45] In these cases, the proclamation empowers the executive organ with a wide discretion and this needs evaluation of the law against the right to privacy guaranteed in human rights instruments ratified by Ethiopia and the FDRE constitution. Hence, this research inquires whether the proclamation has provided

[40] Computer Crime Proclamation, Federal *Negarit Gazeta*, Proclamation No.958/20 I6, Article 2(14), 13, 14 and 16.
[41] *Ibid* Article 16 (1).
[42] *Ibid* Article 16 (2)
[43] *Ibid* Article 25(3).
[44] Fisaha Getachew, *The Respect For Human Rights In Pre-Trial Criminal Investigation (The Case of Oromia Special Zone Surrounding Finfine)*, A Thesis Submitted to Addis Ababa University, School of Graduate Studies in Partial Fulfilment of the Requirement of the Degree of Masters in Human Rights, 14 (2015) (*unpublished*).
[45] Computer Crime Proclamation *supra*, Article 32.

safeguards to protect right to data privacy while the investigatory organ undertakes the computer forensics.

Generally, although the proclamations is not yet practically tested, its provisions that regulate online content data, criminal liability of ISP and digital forensic as they provide rules that restrict freedom of expression and right to data privacy need to be exposed to strict scrutiny alongside the standards of limitation of the human rights. Though human rights are not absolute and can be legally limited under necessary conditions, the glimpse of the provisions of the proclamation created my curiosity to know the reasons and justification of having such criminal provisions.

1.4. Objectives of the Study

The general objective of the study is to evaluate provisions of the computer crime proclamation in light of freedom of expression and right to data privacy.

The specific objectives of the study are:

1. To assess provisions of the proclamation that regulate online content data in light of freedom of expression.
2. To assess the propriety of making ISPs criminally responsible for the acts of the third parties through their services.
3. To assess provisions of the proclamation that regulate digital forensic in light of right to data privacy.

1.5. Scope of the Study

This study is primarily concerned with assessment of substantive provisions of the proclamation in light of freedom of expression and the procedural rules of the proclamation, especially, provisions that regulate digital forensic. Accordingly, the relationship between the proclamation and other laws and provisions that deal with computer crimes that are prohibited in every jurisdictions what I call “conventional computer crimes” for the purpose of this study, and other procedural matters are excluded as they are, although at the draft stage of the proclamation, dealt with in the works cited in this study or irrelevant to the topic of this study.

1.6. Significance of the Study

First and for most, this study identifies gaps that call for intervention by the law or policy makers. Secondly, it plays important role in prevention of computer crime by discussing prohibited cyber activities and thus inform the potential cyber criminals. Thirdly, it helps judges on how to interpret provisions of the proclamation, public prosecutors on how to undertake legitimate investigation and prosecution of cybercrimes under the proclamation and advocators on how to argue for their clients' human rights when accused of violation of the provisions of the computer crime proclamation. Finally, it contributes a lot to further studies on the cyber regulation in Ethiopia, the area which is least studied but is necessary due to proliferation of computer use and abuse.

1.7. Research Methodology

This research is a normative legal research. Given its doctrinal nature, it uses library sources. It utilizes comparative legal research since its very purpose is to appraise the computer crime proclamation in comparison with legislative texts of states, jurisprudences and legal doctrines of the international and regional human rights systems so as to demonstrate possible friction they tested between human rights and cybercrime laws and way outs they used. The researcher has collected relevant and appropriate books, journal articles, decisions, general comments, recommendations, concluding observations and resolutions of international and regional human rights bodies and reports of the special rapporteurs regarding freedom of expression and right to data privacy to instill the existing human rights concerns against computer crime laws. To assess the concerns and arguments during the preparatory works of the proclamation, the researcher has collected the Explanatory Note of the proclamation that show the intension behind provisions of the law.

1.8. Limitations of the Study

Even though the study strives to appraise the provisions of the proclamation in light of standards of limitations of human rights, it has tried to compare and contrast the issue under study with its counterpart in another jurisdictions. In this process, the study is limited to countries that publishes their laws in English. However, the utmost effort is taken to access research and articles written in English to minimize such limitation. Another awful limitation

to this study is shortage of relevant and appropriate reading materials that give bounteous picture of the issue under study in other jurisdictions save free online materials. Another problem of the study that limits it only to evaluations of the words and sprit of the provisions of the proclamation is the fact that the proclamation is newfangled.

1.9. Overview of Chapters

This thesis is divided into six chapters. The first chapter presents introduction. The second chapter presents role of internet in enhancing and exercising freedom of expression and right to data privacy. It also presents the status of the rights at international level and in Ethiopia along with the standards of limitation of the rights provided in the human rights instruments and FDRE Constitution. Chapter three deals with the status of internet access in Ethiopia and the reason behind that low internet penetration of the country. It also evaluates provisions of the proclamation that regulate cyberstalking and online defamation in light of freedom of expression and right to privacy. Chapter four challenges criminalization of ISP for third party's illegal content. It argues against empowerment ISP and administrative authorities to decide legality and illegality of content data. Chapter five assesses provisions of the proclamation that regulate digital forensic in light of right to data privacy. It questions validity warrantless sudden searches provided in the proclamation and wide discretion entrusted to the investigatory organ to extend the scope of search warrant obtained to get access to, search and seizure computers and computer systems. Finally, chapter six provides conclusion and recommendations that largely call for amendment and repeal of the thorny provisions of the proclamation that affect freedom of expression and right to data privacy.

CHAPTER TWO

FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY ON THE INTERNET

Introduction

Internet was originated just few years before the adoption of ICCPR that recognized freedom of expression and right to privacy at international level. Introduction of internet has boosted the exercise and protection of freedom of expression and right to data privacy. Internet plays important role to achieve the promised human rights protections by amplifying voices of human rights defenders and helping to expose abuses. Freedom of expression which is vital in a democratic system is enhanced by the opportunities computer system bestowed our world. Internet has also helped protection and exercise of right to privacy by providing security mechanisms such as anonymity, encryption, pass word etc.

All human rights instruments that deal with civil and political rights, to which Ethiopia is a party, and the FDRE Constitution recognized freedom of expression and right to privacy. Both rights are not limited to offline communications rather, they apply fully to communications, ideas and information distributed through the Internet.[46] For the reason that it has central role in exercise of human rights in general[47] and freedom of expression in particular, the UNHRC has recently passed a resolution condemning countries that intentionally disrupt citizens' internet access.[48] More than 70 states supported the resolution as cosponsors.[49] But, Ethiopia and few other countries voted against the resolution.[50]

Ethiopia has ratified human rights instruments that recognized freedom of expression and right to privacy and incorporated them under chapter three of the FDRE Constitution. However, the

---

[46] UNHRC, *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/20/L.13. (2012) Para. 1. Available at: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280 accessed on April 19, 2017.
[47] Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression *supra* at Para. 61.
[48] UNHRC, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, A/HRC/32/L.20, 27 June 2016.
[49] See https://www.article19.org/resources.php/resource/38429/en/unhrc:-significant-resolution-reaffirming-human-rights-online-adopted accessed on February 24, 2017.
[50] *Ibid*.

Computer Crime Proclamation has provisions that restricted online exercise of these rights. Given the importance of internet in enhancing the exercise and protection of human rights, the computer crime proclamation should be scrutinized against the standards of limitation of the rights. This chapter provides the general over view of relationship between internet and freedom of expression and right to privacy. To foster the assessment of the proclamation in the following chapters, it also discusses the standards of limitation of the rights.

2.1. Internet and Freedom of Expression

Freedom of expression is important for individual's dignity.[51] It constitutes essential foundations for democracy, rule of law, peace, stability, sustainable development and participation in public affairs. Generally speaking, freedom of speech is justified for our special need of protection for search for truth, individual autonomy, democracy and self-government and tolerance.[52] Internet has created new opportunities for individuals to disseminate information to a mass audience and have an important impact on the participation and contribution of citizens in decision-making processes. In contemporary world, Internet is becoming the preferred mode of political participation, education, employment, commerce or personal activities. It has become indispensable tool for normal social functioning thus, deprivation of internet access could entail social exclusion and arguably amount to a human rights violation. The UNHRC considered that electronic and Internet-based modes of expressions are protected like freedom of expression offline.[53] Accordingly, it called states to adopt all necessary steps to ensure every individuals' access to the Internet.[54] The office of UN rapporteur on freedom of expression has been consistently urging states to promote universal Internet access and be cautions against rules that limit data content on Internet.[55]

In contemporary world, Internet is used for bottom-up agenda setting and empowering citizens to speak up in a networked public sphere. Particularly, social media has changed the nature of political campaigning and playing important role in elections and political campaigns around

[51] *General comment No. 34 supra at* para.1.
[52] Wojciech Sadurski, *Freedom of Speech And Its Limits*, 8-35 (1999).
[53] General Comment No 34: *supra* at para. 12.
[54] *Ibid* at para.15.
[55]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.

the world.[56] For instance, social media played pivotal role in Arab Spring,[57] in shaping political debates,[58] by which societies struggled to knock down repressive governments.[59] 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 democratic values. But, in some instances, technologies on internet can also be misused to enflame conflicts and malicious agitation by populists that do not believe in a healthy democratic discourse.[60] In such cases, Internet can play extraordinary role in intensifying violence and chaos with in the society. These issues necessitate cyber laws of which criminal law may be one.

2.1.1. Elements of Freedom of Expression: Overview

2.1.1.1. The Right to Seek and Receive Information

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.[61] 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. Any restriction that prevents the flow of information online must be in line with permissible limitations as set out in international human rights law.

2.1.1.2. The Right to Impart Information and Ideas of all Kinds Through any Media and Regardless of Frontiers

Freedom of expression also includes 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

---

[56] 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.
[57] See 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).
[58] See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595096&download=yes accessed on March 21, 2017.
[59] 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/
[60] *Ibid*.
[61] General Comment 34, *supra*.

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. This includes, according to UNHRC, political discourse,[62] commentary on one's own[63] or on public affairs,[64] canvassing,[65] discussion on human rights,[66] journalism,[67] scientific research, expression of ethnic, cultural artistic expression,[68] teaching,[69] linguistic and religious identity and, advertising. Means of expression can include books, newspapers, pamphlets, posters and banners as well as all forms of audio-visual, electronic and internet-based modes of expression.

2.1.2. International Standards on Limitation of Freedom of Expression

Many of the rights guaranteed to the individuals must be limited or qualified or their scope may be narrowed in order to prevent conflicts with other rights or with certain general interests. Freedom of expression has to be balanced against other human rights and public interests. Limiting freedom of expression requires strictly defined parameters. The ICCPR and the ACHPR[70] provide three-part-test for limitation of the right.

Freedom of expression is one of the most frequently violated rights in the world.[71] It has always been the object of tension, struggle and contest between the state and the citizens and within society itself.[72] Due to this, different international and regional human rights bodies have been taking measures which are developed to standards of limitation of freedom of expression. From the limitation clauses of ICCPR and jurisprudences of international and regional human rights bodies, the International Commission of Jurists have drawn principles of limitation of human rights called "*Siracusa* Principles" which can be equally applied to freedom of expression and

[62] See UNHRC, *Mika Miha v. Equatorial Guinea*, Communication No. 414/1990,
[63] See UNHRC, *Fernando v. Sri Lanka*, Communication No. 1189/2003, Views adopted on 31 March 2005.
[64] See UNHRC, *Coleman v. Australia*, Communication No. 1157/2003, Views adopted on 17 July 2006
[65] See UNHRC, *Concluding observations on Japan,* (CCPR/C/JPN/CO/5).
[66] See UNHRC, *Velichkin v. Belarus*, Communication No. 1022/2001, , Views adopted on 20 October 2005.
[67] See UNHRC, *Mavlonov and Sa'di v. Uzbekistan*, Communication No. 1334/2004, , Views adopted on 19 March 2009.
[68] See UNHRC, *Shin v. Republic of Korea*, Communication No. 926/2000, , Views adopted on 16 March 2004.
[69] See UNHRC, *Ross v. Canada*, Communication No. 736/97, , Views adopted on 18 October 2000.
[70] See the Commentary of ACHPR on Article 9 (2) of the charter *infra*.
[71] 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 No 34*, 12 Human Rights Law Review 627,632 (2012),
[72] *Ibid*. at 633.

right to privacy.[73] These principles explained limitation clauses to restrict the rights in the human rights instrument. Accordingly, certain limitation imposed on freedom of expression has to fulfill the following three cumulative requirements.

2.1.2.1. The Limitation must be prescribed by Law

Arbitrary limitation of freedom of expression is impermissible. The government must follow a written law that is clear and unambiguous to limit freedom of expression. The UNHRC defined in a relatively precise manner the concept of "law" as 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. The law cannot give persons who are in charge of its application unlimited powers of decision on the restriction of freedom of expression. Laws must contain rules which are sufficiently precise to allow persons in charge of their application to know what forms of expression are legitimately restricted and what forms of expression are unduly restricted."[74]

Thus, clarity of the law is strictly required especially when the legislation is criminal law.[75] 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. Accordingly, vaguely worded edicts, whose scope is unclear, will not meet this standard and are therefore not legitimate.[76]

2.1.2.2. The Limitation should aim at Legitimate Purpose

For a restriction to be acceptable, it must also sought to serve a legitimate purpose. The covenant provides that the objective of the prescription consists of respecting the rights and reputation of others or the protection of national security, public order, public health or public morality.[77] These are the only legitimate grounds of restriction of a speech. The list provided in the Article 19 of the covenant is a complete list,[78] and not a list that states can add to. When they impose restrictions, states should remember that the restriction may not put the right in

[73] See Siracusa principles *supra*.
[74] UNHRC, *Keun-Tae Kim v. The Republic of Korea*, Communication No. 574/1994, CCPR/C/64/D/574/1994, 4 January 1999, para 25
[75] See Gary Slapper, *Clarity and the Criminal Law*, 71The Journal of Criminal Law, 475, 477 (2016).
[76] https://www.article19.org/pages/en/limitations.html accessed on April 4, 2017.
[77] See ICCPR *supra* Article 19(3).
[78] General Comment No. 34 *supra* at Para. 21.

jeopardy.[79] The relation between right and restriction and between norm and exception must not also be reversed.[80]

2.1.2.3. Limitation must be Necessary in a Democratic Society

Freedom of expression is a building block of democratic society thus, the later cannot exist or survive without true implementation of the former. 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. This requires that, for instance, punishments provided by limiting freedom of expression must be proportionate. If not, they will create a fear of speaking up which backlashes the basic tenets of democracy. As one can see in the following chapters of this study, in the great majority of cases where human rights bodies have ruled national laws to be impermissible limitations on the right to freedom of expression, it was because they were not deemed to be 'necessary.'

2.1.3. Status of Freedom of Expression in Ethiopian Laws

2.1.3.1. The FDRE Constitution

Freedom of Expression has got constitutional recognition in Ethiopia. Article 29 of the FDRE Constitution guarantees freedom of expression. Both elements of freedom of expression which are discussed in previous sections of this chapter are recognized under the Constitution.[81] The Constitution rules that the limitations of the right has to be made through law. It provides that, in principle, freedom of expression cannot be limited on account of the content or effect of the point of view expressed.[82] Generally, according to the Constitution, limitation of freedom of expression is permissible only: 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.[83]

---

[79] *Ibid*.
[80] *Ibid*.
[81] See Constitution of the Federal Democratic Republic of Ethiopia, Federal *Negarit Gazeta*, Proclamation No. 1/1995the FDRE Constitution Article 29 (2).
[82] *Ibid* at Article 29 (6).
[83] *Ibid*.

But, limitation according to Article 29(6) of the Constitution imposes dilemma. On one hand, the clause "public expression of opinion which is intended to injure human dignity" that is provided as a ground of limitation to freedom of expression under the Constitution is not clear, therefore, may be abused. On the other hand, the Constitution fails to provide for the third standard of limitation of freedom of expression i.e. necessity of the limitation in a democratic society, although it sought to establish democratic government. However, Article 13 (2) which states that the human rights provisions of the Constitution shall be interpreted in conformity with the human rights instruments which Ethiopia has ratified will help in this case. Accordingly, Article 29 of the Constitution should be interpreted in conformity with the Article 19(3) of the ICCPR.[84]

2.1.3.2. Subsidiary Laws

The Proclamation on Freedom of Mass Media (press law) and Access to Information was promulgated in 2008 aiming at realization of freedom of expression by facilitating establishment of free media and guaranteeing individuals' right to access to information.[85] It provides that all persons have the right to seek, obtain and communicate any information held by public bodies, except when such information is exempted.[86] This proclamation has a lot contribution in enhancing the right to access to information. But, in practice, the proclamation has chilling effect on freedom of expression by paving the way for implicit political intervention that increases self-censorship.[87]

Recent Ethiopian proclamations have been criticized for their alarming effect on freedom of expression.[88] The Freedom of Mass Media and Access to Information Proclamation[89] discouraged private media from engaging actively in several topics including human rights, through its restrictive provisions on defamation, excessive fine and cumbersome registration

[84] FDRE Constitution *supra*, Article 13 (2).
[85] See Freedom of Mass Media and Access to Information Proclamation, Federal *Negarit Gazeta* Proclamation No.590/2008, preamble.
[86] *Ibid* at Articless 12(1) and 15.
[87] See 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 for Partial Fulfillment of the Requirements for the Degree of Master of Arts in Journalism and Communication (2013) *(unpublished).*
[88]Gedion Timothewos, *Freedom of Expression in Ethiopia: The Jurisprudential Dearth*, 4 MLR 201, 231 (2010).
[89] See Freedom of the Mass Media and Access to Information Proclamation *supra* note 85.

system.[90] Prosecutions of political speeches and the repeated prosecution of persons running private newspapers by Ethiopian government shows that there is incongruence between what the FDRE Constitution provides about freedom of expression and the reality on the ground.[91]

Charities and Societies proclamation also affected human rights advocacy by placing excessive restrictions on the Non-Governmental Organizations that advocate human rights.[92] Due to this, many of them have changed their mandate and those human rights organizations who survived have significantly scaled down their activities due to the major impacts of fund restriction.[93] Because of this restrictive regulation by the proclamation, robust NGOs that advocates human rights in Ethiopia is lacking.[94]

The Ethiopian anti-terrorism proclamation contains human rights unfriendly provisions that may be abused to suppress any dissent or movement which the government doesn't like. As far as this proclamation is concerned, the United Nations Human Rights Committee (UNHRC) in its concluding observation against Ethiopian initial report stated that there are unclear definition of certain offences in proclamation.[95] The committee has given the Ethiopian government to ensure observance of the country's human rights obligations under the ICCPR by the law. Most of the prisoners, suspects and convicted persons under the proclamation are journalists and persons from opposing parties.[96] This implies that the government is using the proclamation to control dissenters and whistle blowers against lack of good governance, corruption, poverty, political and economic inequality and the absence of fair and free elections.

[90] Shimelis Hailu, *Ethiopian Anti-Terrorism Law and Human Rights Nexus: An Appraisal*, A Thesis Submitted to the School of Graduate Studies of Addis Ababa University 39 (2014) (*Unpublished*).
[91]Gedion Temothewos, *An Apologetic for Constitutionalism and Fundamental Rights: Freedom of Expression in Ethiopia*, CEU Collection 122 (2009).
[92] See Charities and Societies Proclamation, *Federal Negarit Gazeta*, Proclamation No.621/2009, Article 77, 85, 88,
[93] Shemelis *supra* at 42.
[94] Mizanie Abate, *Transnational Corporate Liability for Human Rights Abuses: A Cursory Review of the Ethiopian Legal Framework*, 4 Mekelle University Law Journal 34, 70 (2016).
[95] UNHRC, *Concluding observations of the Human Rights Committee on Ethiopia*, 102nd session Geneva, 11-29 July 2011, para. 15.
[96] Shimelis *supra* at 81.

2.2. Internet and Right to Data Privacy: Overview

In general terms, privacy has been defined as the right to be let alone.[97] Right to privacy is guaranteed in all human rights instruments to which Ethiopia is a party that provide for civil and political rights.[98] As state party to the instruments, Ethiopia must respect the privacy of individuals and ensure that third parties do not act in a way that could arbitrarily affect it. Computer and computer system have made protection of right to data privacy better by providing security systems through which persons keep their information secretively out of reach of others. Internet provides for passwords, encryption, anonymity and digital algorism options that highly protect data from unwarranted access from unauthorized organs including repressive government agencies. In the contemporary world, a new boundary, made up of the screens and passwords that separate the virtual world from the real world of atoms, emerged with the advent of internet.[99] Digital storage of personal information, arguably, can be more secure than traditional one. Thus, internet plays a lot in protection of right to privacy.

2.2.1. Elements of Right to Data Privacy

Unfortunately, right to privacy is mentioned both under the UDHR and ICCPR in more general provisions or in the form of principle. Meaning, the instruments do not provide details of the right. This was done as such to compromise the demands of several states during drafting stages of the two instruments.[100] The right to privacy is formulated in general phrases. Hence, the technical details and limitations to be imposed are left opened for state parties. Due to this, rights which could be termed as 'subsets' to the classic right to privacy such as the right to anonymity, right to encryption and right to algorithm are not expressly regulated within the human rights instruments or are only implicit in them.[101] But, privacy on internet is unthinkable without recognizing these security mechanisms that are developed to maintain the security of internet users. Despite the absence of binding laws that guarantee digital rights at international

[97] Samuel D. Warren & Louis D. Brandeis, *The right to privacy*, 4 Harvard Law Review 2303, 2305 (1890).
[98] See for example, Universal Declaration on Human Rights; Article 12, International Covenant on Civil and Political Rights: Article 17, Convention on the Rights of the Child: Article 16.
[99] David R. Johnson & David Post, *Law and Borders- The Rise of Law in Cyberspace*, 48 Stanford Law Review, 1367 (1996).
[100] Kinfe Micheal, *Digital privacy and virtues of multilateral digital constitutionalism—preliminary thoughts*, 00 International Journal of Law and Information Technology, 1, 15 (2017)
[101] *Ibid* at 12.

level, there is a promising move to recognize the digital bills of rights that gives protection to these security mechanisms.[102]

On June 17, 2015, the United Nations Special Rapporteur on Freedom of Expression presented report[103] on the use of encryption (the transformation of data by the use of cryptography to produce unintelligible data to ensure its confidentiality[104]) and anonymity (the fact of not being identified[105]) in digital communication to the UN Human Rights Council. The special rapporteur recognized that encryption and anonymity, as leading instruments for online security, enable people to exercise their rights to freedom of opinion and expression and the right to privacy in the digital age. Accordingly, imposing blanket prohibitions on encryption and anonymity is neither necessary nor proportionate to the interest they protect.

2.2.2. Status of Right to Data Privacy at International Level

Just following the petition of about 500 writers to the UN to create an international bill of digital rights which all governments should adhere to,[106] in December 2013, the UNGA adopted resolution 68/167, which expressed the UNGA's deep concern at the negative impact that surveillance and interception of communications may have on human rights.[107] Affirming that the right to privacy should be protected online, the UNGA called all states to respect and protect the right to privacy in digital communication. It also called on all states to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view of upholding the right to privacy by ensuring the full and effective implementation of all of their obligations under international human rights law.[108] The UNGA has also recently adopted its third resolution on digital privacy[109] which urges states to restrain from requiring businesses to take steps that have impacts on privacy while at the same time

[102] *Ibid*.
[103] http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx accessed on April 18, 2017.
[104] UNESCO, *Human rights and encryption*, 9 (2016).
[105] Ian J. Lloyd, *Information Technology Law* (6th Ed.), 5 (2011)
[106] Kinfe Micheal, *Digital privacy and virtues of multilateral digital constitutionalism-preliminary thoughts*, *supra* at 6.
[107] See UNGA, The Right to Privacy in the Digital Age, GA Res 68/167 (18 December 2013)
[108] See UNGA, The Right to Privacy in the Digital Age, GA Res 69/166 (18 December 2014).
[109] See UNGA, The Right to Privacy in the Digital Age, UN Doc A/C.3/71/L.39/Rev.1 (16 November 2016).

calls upon businesses to work towards enabling communications and to develop technical solutions to safeguard users' privacy.[110]

Recalling the first two resolutions of the UNGA on digital privacy, in 2015, the UNHRC decided to appoint, for a period of three years, a Special Rapporteur on the Right to Privacy to work up on protection of the right.[111] The UNHRC is deeply concerned about the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.[112] The UNHRC has also considered the effects of surveillance in its concluding observations.[113] It had also adopted the General Comment 16 as early as 1988 which provides that the right to privacy of correspondence must be protected *de jure* and *de facto*, and any form of surveillance, including electronic surveillance or interception is prohibited under Article 17 of the ICCPR.[114] The African Union Convention on Cybersecurity and Personal Data Protection, to which Ethiopia will, hopefully, be a member in future, apportioned many Articles to protect data privacy.[115] Generally, right to data privacy (right to privacy online) is recognized equally with right to privacy offline in international human rights system and arbitrary intrusion is impermissible.

2.2.3. Right to Data Privacy in Ethiopia

2.2.3.1. The FDRE Constitution

The Constitution stipulates right to privacy under its Article 26(1) broadly and illustratively so as to allow one to invoke protection of personal data. The Constitution puts the right to privacy in a more detailed manner than the two international bills of rights (UDHR and ICCPR).[116] The provisions of the Constitution that guaranteed right to privacy are framed illustratively so

[110] *Ibid* at paras 5(i), 7.
[111] See UNHRC, Right to Privacy in the Digital Age, Human Rights Council Res 28/16 (26 March 2015).
[112] *Ibid*.
[113] See, for instance, Comments of the Human Rights Committee: Russian Federation, 26 July 1995, para 19; Observations of the Human Rights Committee: Jamaica, 19 November 1997, para 20; Concluding Observations of the Human Rights Committee: Poland, 29 July 1999, para 22.
[114] UNHC, *General Comment 16: Art 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, para 8.
[115]The African Union Convention on Cybersecurity and Personal Data Protection, AU Doc. EX.CL/846(XXV), 27 June 2014, Chapter II, Articles 8–23.
[116] See the FDRE Constitution *supra*, Article 26.

that all forms of intrusion into private spheres are prohibited. The Constitution requires public officials not only to refrain themselves from interferences with individual privacy but also to protect against invasions of privacy by others.[117] It puts limitation clause under Article 26(3) to protect other competing and compelling interests. Accordingly, limitation to the right to privacy is allowed only when three cumulative conditions are satisfied: (1) whether there is a compelling circumstance to restrict the right, (2) where the restriction is based on specific law and (3) where the restriction is made for one of the purposes of the six legitimate objectives enumerated under the provision i.e, national security, public peace, the prevention of crimes, the protection of health, public morality, and the rights and freedoms of others. Accordingly, these are the important tests to assess the justifiability of any limitation to the right to privacy in the proclamation.

2.2.3.2. Subsidiary Laws

There are many civil and criminal law provisions that are devoted to protect right to privacy in Ethiopia. There are many Articles of civil code that protect individuals' right to privacy.[118] The press law provides rules for protection of private information from disclosure when the interest of such individual requires.[119] This law is the only legislation in Ethiopia that contains a comprehensive and lengthy definition of personal information.[120] The Law on the Registration of National Identity Cards is another law that contains rules that are protective of privacy.[121] The Criminal Code[122] and Criminal Procedure Code[123] also provide provisions that are aimed to protect privacy.

On the other hand, based on the limitation clause provided in the Constitution, some specific laws including the Criminal Procedure Code[124] (though promulgated before the Constitution),

[117] Kinfe Micheal, *Data privacy law and practice in Ethiopia*, 5 International Data Privacy Law, 177, 180 (2015).
[118] Civil Code of The Empire of Ethiopia, *Federal Negarit Gazeta*, Proclamation No. 165/J960. Articles 10, 11, 13, 31, 20-23, 27–30 , 2044–2052 and 2055.
[119] The Proclamation on Freedom of Mass Media and Access to Information *supra* at Article 16.
[120] Kinfe, *Data privacy law and practice in Ethiopia supra* note 85.
[121] Registration of Vital Events and National Identity Card Proclamation, Federal *Negarit Gazeta*, Proclamation No. 760/2012. Article 64(3 and 4),
[122]See Ethiopian Criminal Code, Federal *Negarit Gazeta*, Proclamation No. 414/2004. Article 601, Article 604-606.
[123] Criminal Procedure Code, *Negarit Gazeta*, Proclamation No. 185/1961. Article 32 and 33
[124] Ibid, Article 32 (1) and (2).

the Anti-Corruption Proclamation[125] and the Anti-Terrorism Proclamation[126] put restrictions on the right to privacy for the said objectives. But, their fitness to the sought requirements in the Constitution is quarrelsome.[127]

2.3. The Computer Crime Proclamation

The advent of internet is not only boon but bane as well. Because it has created complex systems in which culprits commit crimes and escape. The fact that computer and computer system may be used to commit crime through internet requires that the internet should be policed. In the history of regulation of cyber activities, the law has been crawling behind newly invented computer abuses.[128] In Ethiopia too, some hazard computer abuses could not be punished due to lack of appropriate laws capable of regulating such behavior. Because, the provisions of criminal code which were set to punish ordinary crimes, as any ordinary criminal law of every state,[129] and few provisions of the code which are computer specific were inadequate to regulate the cases of computer crimes. [130] Due to stealthy nature of computer crime, stipulation of cybercrime law requires deep and up-to-date knowledge of the subject matter on one hand and cautious stipulations concerning the effect of the provisions on human rights.

On June 7, 2016 Ethiopian legislature introduced the Computer Crime Proclamation. It had been under draft since 2013. It is claimed by the drafters of the proclamation that the proclamation was prepared in harmony with various model laws existing at regional and international levels.[131] The proclamation has got comprehensive provisions for both substantive and procedural matters connected with cybercrime. It also has got unique controversial provisions like criminalization of defamation, criminal liability of ISPs for illegal

[125] Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation, Federal *Negarit Gazeta*, Proclamation No. 434/2005 as amended by Proclamation No. 882/2015. Article 46. Provides that where it is necessary for the investigation of corruption offence, head of the Federal Ethics and Anti-corruption Commission organ may order the interception of correspondence by telephone, telecommunications and electronic devices as well as by postal letters. (Emphasis added).
[126] Anti-Terrorism Proclamation, Federal *Negarit Gazeta*, Proclamation No. 652/2009 Article 16.
[127] See Kinfe & Alebachew *supra*.
[128] Thomas Welch, *Computer Crime Investigation and Computer Forensics*, 6 Information Systems Security, 56, (1997).
[129] Lawrence F. Young, *United States computer crime laws, criminals and deterrence*, 9 International Review of Law, Computers & Technology 1, 4 (1995).
[130] Kinfe & Halefom *supra* at 128.
[131] See the Explanatory Notes of the Computer Crime Proclamation *Supra* at 3&4.

content data of third party and procedural rules which deviate from the rules of criminal procedure code that triggered this study. Because, when such limitation comes to Internet, it is crucial to evaluate the limitations based on the unique and special characteristics of human rights on the internet in line with the yardsticks set in the human right law. Thus for example, when establishing the proportionality of a particular restriction, it is crucial to assess the impact of that restriction not only from the point of view of the private parties directly affected by the measure, but also from the perspective of the impact on the functioning of the Internet.

Conclusion

The advent of internet enhanced the protection and exercise of human rights especially, freedom of expression and right to privacy. These rights are worthy of protection online. In both of the international and regional human rights instruments to which Ethiopia is a party and the FDRE Constitution, there are standards against which limitation of these rights may be acceptable. Commonly, to limit the rights, there should be a clear law made by the authoritative organ, the limitation should be sought to protect the identified legitimate interest and the limitation should be necessary in democratic society. These yardsticks are drawn from the provisions of the human rights instruments, the Constitution and jurisprudence of human rights bodies. The Computer Crime Proclamation has restricted both the freedom of expression and right to data privacy by providing some special provisions on content of data, responsibility of ISPs and digital forensic. Therefore, the following chapters assess provisions of the proclamation in light of the standards discussed in this chapter.

CHAPTER THREE

REGULATION OF CONTENT DATA IN COMPUTER SYSTEMS

Introduction

Section three of the computer crime proclamation provides provisions that prohibit computer data that contain child pornography,[132] affect liberty and reputation of persons[133] disturbs the public[134] and spamming.[135] It also provides criminal liabilities of ISPs for the illegal contents produced by their users.[136] These provisions directly impose restrictions on freedom of expression. Limitation to online freedom of expression by itself is not wrong for computer networks provide ample opportunity for propagating scurrilous material about others[137] and some online conducts that are hazardous for the wellbeing of the society and disturb peace and security of the public, therefore, certain legal limitations should be there to protect the rights of individuals and security of the public. However, neither imposing general restrictions on freedom of expression nor unnecessary restriction is permissible under human rights instruments and the FDRE Constitution. This chapter examines Article 13 and 14 of the computer crime proclamation in light of the standards of limitation of freedom of expression and right to data privacy.

3.1. Right to Access Internet in Ethiopia

Right to access Internet could be an integer of freedom of expression.[138] The conclusion to be drawn from obligation of a state under Article 19 of ICCPR is that freedom of expression imposes a positive obligation upon states to promote and facilitate universal Internet access.[139] As a state party to ICCPR, Ethiopia must ensure that all of its citizens are afforded equal

[132] Computer crime proclamation, Federal *Negarit Gazeta*, proclamation No. 958/2016 Article 12.
[133] *Ibid* Article 13.
[134] *Ibid* Article 14.
[135] *Ibid* Article 15.
[136] *Ibid* Article 16.
[137] Diane Rowland & Elizabeth Macdonald, *Information Technology Law* (2nd ed.), (2000).
[138] Stephen Tully, *A Human Right to Access the Internet? Problems and Prospects*, 14 Human Rights Law Review, 175 (2014).
[139] The United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration On Freedom Of Expression And The Internet*, (2011) at par. 6.

opportunities to receive, seek and impart information by any means of communication without any discrimination.[140] It is also duty bound to clear any barrier which hinders universal accessibility of internet facilities.

As far as internet penetration rate is concerned, Ethiopia is crawling behind most countries in Africa save 11 countries.[141] Due to the government's monopoly which has stifled innovation, restricted network expansion and the scope of services, telecom sector in Ethiopia provides private consumers with few options. Accordingly, access to ICT services remains prohibitively expensive in Ethiopia. The investment proclamation provides that private investors cannot invest in telecommunication service privately but jointly with the government.[142] The use of any telecom technology that could bypass the local network is also strictly prohibited.[143] Prices of using Internet are set by the state-controlled ETC[144] and kept exaggeratedly high.[145] According to the research conducted by Alliance for Affordable Internet very recently, Ethiopia is ranked 55 out of 58 countries the study is conducted up on in terms of supplying internet with affordable cost.[146]

Ethiopian government has been defending government monopolization of telecom service provision under two reasons: First, one of the fundamental concerns for governments is the issue of universal access. The government wants to retain telecom service in its hands to supply universal access of telecom service to every Ethiopians.[147] Considering telecom service as a public service by government or through government intervention, policy-makers believe that a public monopoly operator would be in the best position to build telecommunication networks effectively and that only such operators could make services available to citizens at equitable prices without siphoning off undue profits. For developed economies, this argument holds

[140] See ICCPR *supra* Article 19.
[141] http://www.internetworldstats.com/africa.htm accessed on April 19, 2017.
[142] Investment proclamation, Federal *Negarit Gazeta*, Proclamation No. 769/2012 Article 6 (2) (b).
[143] Telecom Fraud Proclamation, Federal *Negarit Gazeta*, Proclamation No. 761/2012 Article 9(2).
[144] International Telecommunication Union, *Internet from the Horn of Africa: Ethiopia Case Study*, 11 (2002).
[145] Ethiopia – Telecoms, Mobile, Broadband and Forecasts, Paul Budde Communication Pty Ltd.: June 2014, http://bit.ly/1ji15Rn
[146] Alliance for Affordable Internet available at at http://a4ai.org/affordability-report/report/2017/ accessed on May 12, 2017.
[147] Minyahel Desta, *Liberalization of telecommunication in Ethiopia challenges and prospects: citizens' view and opinion*, Research paper submitted to trade policy training center in Afric (trapca) for the 2012 annual conference (unpublished) 18 (2012).

water as they have already developed telecom services in position and their economy is solvent to subsidize basic services.[148] But in the case of less developed countries' like Ethiopia, according to ITU's Universal Access/Service Report, the scenario of cross-subsidization worked less well and monopoly operators had difficulties in providing both basic and new services and in keeping up with technological changes.[149] Likewise, in response to similar arguments forwarded by most of developing countries' policy makers, OECD report of the 2007 and other several studies found from empirical evidence that very few countries have achieved universal access solely through monopoly operators.[150] If properly planned within government and agreed with market entrants, most countries can attract private investment in infrastructure that benefits the economy and society as a whole, including rural and low income areas.[151] Thus, such argument by the government is thin and doesn't show practical realities.

Second, Ethiopian government wants to retain huge capital gained from investing in telecom service as it is lucrative source of income by which the government funds mega projects.[152] The huge capital produced by ETC may be due to the monopolization. Despite repeated international pressure to liberalize telecom service in Ethiopia, the government refuses to release its grip on the sector. Due to the lack of liberalization of telecom service by the Ethiopian government, Ethiopia remained a country with mono telecom service provider that has significantly hindered the expansion of digital media in the country.[153] As a result, Ethiopia has one of the lowest rates of internet and mobile-telephone penetration in the Africa.[154]

In addition to the above reasons, some people argue that the fact that all connections to the international Internet are completely centralized via ETC enabled the government to cut off the internet at will.[155] From this fact, it is possible to argue that the government wants to retain

---

[148] ITU, Universal Access/Service: Assessment Report, 3 (2013).
[149] *Ibid*.
[150] See OECD Annual Report of 2007.
[151] *Ibid*.
[152] http://www.reuters.com/article/us-ethiopia-economy-insight idUSKBN0LC0C320150208 accessed on April 3, 2017.
[153] See http://www.ethioconstruction.net/?q=news/telecoms-slow-down-development-ethiopian-tech-scene-%E2%80%93-iceaddis accessed on April 4, 2017.
[154] *Freedom House (2016) available at* https://www.justice.gov/eoir/page/file/916611/download accessed on April 6, 2017.
[155] Freedom House (2015) available at https://www.justice.gov/eoir/page/file/917171/download *and Freedom House 2016 supra*.

the monopoly to effectively administer the internet. Fortunately, this helps the government to control every communication via ETC by installing devices that can trample free speech.

3.2. Regulation of Content Data under the Computer Crime Proclamation

3.2.1. Protection of Individuals Rights and Public Security Online

The first two Sub Articles of Article 13 of the proclamation seem to regulate cyberstalking. "Cyberstalking" is the use of Internet or other electronic means to stalk or harass an individual, group, or organization.[156] Cyberstalking is a wrongful act in which the stalker harasses a victim using electronic communication, such as e-mail or instant messaging or messages posted to a Web site or a discussion group. Basically, the nature of cyberspace is such that it is seen to encourage stalking. Usually, a cyberstalker acts anonymously or pseudonymously afforded by the Internet to allow them to stalk their victim without being detected. The proliferation of the Internet has brought about an abundance of means by which cyberstalkers can target upon their victims. 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.[157] Thus, the response of a state through crafting anti-cyberstalking laws or amending traditional anti-stalking laws to account for technological advances in the Internet and electronic communications is right. Nevertheless, anytime speech is regulated, there exists the possibility that the law may infringe the right to free speech.[158] Expressive speech on the Internet is generally afforded robust protection, similar to that of books, newspapers, and magazines. Therefore, an anti-cyberstalking 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.[159]

Article 13 (1&2) of the proclamation seems to regulate cyberstalking because it prohibits disseminating online data whose content offend, intimidates or threatens another person or his

[156] http://searchsecurity.techtarget.com/definition/cyberstalking accessed on March 22, 2017.
[157] Basu, S. and Jones, R.P., *Regulating Cyber stalking*, 2 JILT 1, 16 (2007).
[158] https://www.rctlj.org/2012/10/anti-cyberstalking-laws-misuse-and-the-first-amendment-right-to-free-speech/ accessed on March 22, 2017.
[159] *Ibid*.

families[160] and sending to a person or disseminating data whose content causes fear, threat or impose psychological strain on another person.[161] Though regulating cyberstalking is important, these provisions of the proclamation have to be scrutinized in light of the standards of limitation of freedom of expression because they restrict freedom of expression. The provisions are too general to capture as many conducts as possible. There is neither legal nor practical definition of "intimidation," "threatening" and "causing fear." These stipulations are against the standard of limitation of the right that requires clear law. Lack of clarity of these provisions has repercussion on free speech. Because, in normal course of things, people make rash comments in the heat of emotion with no intention of causing a harm but may be, he/she is simply exasperated or angry by certain condition.[162] 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.

Both the human rights instruments to which Ethiopia is a party and the FDRE Constitution provides public security as a legitimate ground to limit freedom of expression because content data that can disturb the public security can be easily and swiftly disseminated on the internet. Thus, it is important to take a legislative measure to ensure peace and security of the society. Article 14 of the proclamation is designed to defend public peace and security on internet. 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, Halefom recommended that provisions of Article 14 need to be narrowly interpreted.[163] He further expressed his fear that the law enforcement authorities may interpret these provisions malevolently to deny discussions of matters of public concern unless strict requirements are followed.[164] Similarly, Ethiopian civil societies have been voicing their concern that the law would be used to crackdown critical commentary, political

[160] Computer Proclamation *Supra* Article 13 (1).
[161] *Ibid* 13 (2).
[162] Chuck Easttom & Det. Jeff Taylor, *Computer Crime, Investigation, and the Law*, 415 (2011).
[163] Halefom *supra* 21.
[164] *Ibid*.

opposition, and social unrest.[165] They feared that the phrases like "incites violence, chaos or conflict among people" could be abused to suppress digital campaigns.[166]

Practically, Ethiopian government has been claiming that social media platforms are disturbing security of the country. This accusation is primarily pointed to Facebook. In Ethiopia, Facebook seems almost synonymous to internet.[167] Ethiopia ranks 7th of the top 10 African countries with the most Facebook users.[168] Facebook is an online social network/networking service that was launched in 2004 and became available worldwide in 2006.[169] It 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.[170] It also heightened protests in Oromia and Amhara states that forced the government of Ethiopia to declare state of emergency.[171] Exasperated by these challenges at home, the Ethiopian Prime Minister told to the UNGA 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.[172] In support of this, some persons also argued that social media have despoiled civility in Ethiopia.[173] But, these assertions were debunked by the empirical research conducted jointly by scholars of Addis Ababa University and University of Oxford as there are practically insignificant number of hate speech communicated between Ethiopians through Facebook.[174]

---

[165] 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.

[166] *Ibid*.

[167] Gagliardone, I. et al. *Mechachal: Online debates and elections in Ethiopia. From hate speech to engagement in social media* 16 (2016). and see See Leo Mirani, *Millions of Facebook Users Have No Idea They're Using the Internet*, accessed April 4, 2017, available at http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet

[168] http://www.ethiocyberlaws.com accessed on April 4, 2017.

[169] Facebook was initially available to American university students only. In 2006 it was opened to everybody that had a valid email address.

[170] Gagliardone, I. et al, *supra*.

[171] Ezana Sehay How Social Media Is Despoiling Civility In Ethiopia, available at http://www.ethiocyberlaws.com/

[172] See http://www.un.org/apps/news/story.asp?NewsID=55022#.WN0vDmdlDIW accessed on April 5, 2017.

[173] Ezana Sehay *supra*.

[174] See Gagliardone, I. et al *supra*.

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 stating that such language allows the provisions to be applied to both current and future technologies in regulation of cybercrime.[175] Nevertheless, UNHRC commented that a norm, to be characterized as a "law," must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[176] As the words of Articles 13 (1) & (2) and 14 are vague, they give no clear notice to regulate prohibited and permissible speeches.

3.2.2. Regulation of Online Defamation

Defamation can be defined as the intentional infringement of another's right to his/her good name, or, more comprehensively, the wrongful, intentional publication or communication of words or behavior concerning another which has the tendency to undermine his status, good name or reputation.[177] For a statement to be accounted 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.[178] The term "defamation" tends to be used as a generic descriptor for actions in which it is alleged that the making of untrue and unwarranted comments about an individual have tended to lower that person's standing in the eyes of right-thinking members of society.[179] Defamation is considered both under civil and criminal laws in Ethiopian legal system. Civil code regulates it under fault based liability.[180] Accordingly, civil remedies will be sought from a person made liable under the code which may include; compensation, apology, injunction etc. Similar remedies are there in the press law.[181]

3.2.2.1. Criminalization of Online Defamation

As far as regulation of internet defamation is concerned, one has to address whether criminal law is appropriate to regulate online defamation and justifiable under standards of limitation

[175]The Explanatory note of Computer crime Proclamation, page 5.
[176] See, General Comment 34 *supra* at para. 25.
[177] Sanette Nel, *Defamation on the Internet and other computer networks*, 30 The Comparative and International Law Journal of Southern Africa, 154, 155 (1997).
[178] Ter Kah Leng, *Internet defamation and the online intermediary*, 31Computer Law and Security Reviews 68 (2015).
[179] Lloyd, *infra* at 547.
[180] Civil Code of The Empire of Ethiopia *supra* Article 2044.
[181] Freedom of Mass Media and Access to Information Proclamation, Federal *Negarit Gazeta,* Proclamation No.590/2008, Article 41(2).

of freedom of expression. Criminalizing defamation in general and internet defamation in particular cannot be validly justified because criminal defamation laws negatively affects free expression. They 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, criminal defamation law still cast 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 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. This is not to say that defamation should not be outlawed; but in accordance with the necessity test, the means used to discourage it should be carefully targeted to prevent the stifling of legitimate criticism.

Some authors argue that due to availability of self-help mechanism on internet 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.[182]This argument was developed before invention of social networking platforms like Facebook[183] and tweeter[184] that came up with appropriate systems to reply to any statement of users instantaneously. This shows that the argument hold water better in the current communications on internet. However, for this argument to function, the plaintiff has to get access to the media through which the defamation is posted. In contrast, a person who neither owns nor has access to a computer, who has never used a computer or has no idea how a computer functions, or who could not reasonably afford the cost to access, has no access to counter speech. Thus, the argument holds water as long as there is reasonable expectation that the plaintiff is able to respond to the defamatory statement. Such person can use tort law as a last resort against the defamation. But, the undeniable fact is that the ability to remedy the defamation by counter

[182] Jeremy Stone Weber, *Defining Cyberlibel: A First Amendment Limit for Libel Suits against Individuals Arising from Computer Bulletin Board Speech*, 46 Cas. W. Res. L. Rev. 235,261 (1995).
[183]http://www.knowyourmobile.com/apps/facebook/21807/history-facebook-all-major-updates-changes-2004-2016 accessed on March 21, 2017.
[184] https://www.lifewire.com/history-of-twitter-3288854, accessed on March 21, 2017.

speech allows the person defamed by online defamation to keep his or her name intact than any other legal remedy.[185]

Therefore, criminalization of online defamation is futile and unnecessary because of the chilling effect that the criminal sanctions can impose on freedom of expression. The current social media platforms provided ample mechanisms to reply to a data content disseminated on Internet having messages about certain person. If the statement or video or audio or image disseminated on Internet containing messages about him/her is false, the person against whom the it is made can falsify by giving true information about himself/herself on the point. If this doesn't satisfy him/her, he or she can enter the civil proceeding by claiming civil remedies.

Criminal sanctions have the potential to frighten the persons due to which persons may abstain from communicating about the important issues which will benefit the public at large. In this manner, criminalization of defamation affects freedom of expression negatively. And, in cases of online defamation of individuals, stipulating criminal sanctions that are applied to offline defamation may be unnecessary or disproportionate.[186] Because, Internet facilitates discussions and debates between individuals in which individuals take a self-help measures to show falsity of statements made against them. Defamation laws may lead to strong self-censorship to avoid the fear of being subject to severe criminal sanctions. As criminalization of defamation cannot pass the test of standard of necessity of the measure in democratic society, criminalization of Internet defamation is unjustifiable under the three-part-test.

3.2.2.2. Position of Human Rights Bodies on Criminalization of Online Defamation

Jurisprudence of International and regional human rights bodies makes it clear that the three-part-test present a high standard which any interference with freedom of expression must overcome. Throughout their jurisprudence, international and regional human rights bodies have recognized the threat posed by criminal defamation laws on freedom of expression and recommended that defamation should be decriminalized.

[185] *Ibid* at 265.
[186] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* at para. 27.

3.2.2.2.1. The UN Human Rights System

On his 2011 report, the United Nations Special Rapporteur on the Promotion and Protection of freedom of opinion and expression called all states to decriminalize defamation.[187] Similarly, considering its chilling effect on freedom of expression, UNHRC called state parties to ICCPR to consider the decriminalization of defamation and stated that, in any case, the application of criminal law should only be tolerated in the most serious cases and imprisonment is never an appropriate penalty.[188] These serious cases can be hate speech or incitement to violence but not mere defamation. Accordingly, it is impermissible for a state party to indict a person for criminal defamation.[189]

3.2.2.2.2. The African Commission of Human and Peoples' Rights

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.[190] Article 2(2) of the Declaration states that any restriction on freedom of expression shall be provided by law, serve a legitimate interest and must be necessary in a democratic society.[191] In deciding on communication brought before it, the Commission, while interpreting Article 9 (2) of the charter that provides conditions under which freedom of expression may be limited, stated that:

> "According to Article 9 (2) of the Charter, dissemination of opinions may be restricted by law. This does not however mean that national law can set aside the right to express and disseminate one's opinions guaranteed at the international level; this would make the protection of the right to express one's opinion ineffective. To permit national law to take precedence over international law would defeat the purpose of codifying certain rights in international law and indeed, the whole essence of treaty making."[192]

By similar understanding, the Commission adopted a resolution that called up on all African states to decriminalize defamation.[193] The commission stated that criminal defamation laws constitute a serious interference with freedom of expression and impedes the role of the media

---

[187] *Ibid* at 73.
[188] General Comment 34 *supra* at Para 47
[189] *Ibid*.
[190] *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.
[191] *Declaration of Principles on Freedom of Expression in Africa*, *Supra* Article 2(2).
[192] ACHPR, *Civil Liberties Organization and Media Rights Agenda v. Nigeria*, Comm. Nos. 140/94, 141/94, 145/95 (1999), para. 40.
[193] ACHPR, *Resolution on Repealing Criminal Defamation Laws in Africa*, Res 169(XLVIII) (2010).

as a watchdog, prevent journalists and media practitioners to practice their profession without fear and in good faith.[194] It is vivid that criminal defamation laws impose similar threat on bloggers, whistle blowers and human rights defenders on Internet.

3.2.2.2.3. The African Court of Human and People's Rights

African Court of Human and People's Rights has also ruled out criminalization of defamation in *Konate* V. *Burkina Faso case*.[195] Lohé Issa Konaté had written three articles which were published that the Burkina Faso's Courts found to be defamatory and punished him to serve the imprisonment of one year and pay fine of 1.5 Million CFA Francs (an equivalent of 3000USD). The courts ordered him to pay the damages of 4.5 Million CFA Francs (an equivalent of 9000 USD) and court costs of 250,000 CFA Francs (an equivalent of 500USD). Kenote petitioned to the ACHPR that the sentence to a term of imprisonment, the huge fine and damages as well as the court costs violate his right to freedom of expression protected by various human rights treaties to which the Burkina Faso is a party.[196] The court evaluated the decision of Burkina Faso's courts in light of the three-part-test. 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.[197]

3.2.3. Regulation of Online Defamation in Ethiopia

Under the age-old but binding Ethiopian civil code, defamation is ruled under fault based liability.[198] Accordingly, a private party, in order to establish liability must prove that the defendant acted intentionally or negligently in making a damaging false statement. On the other hand, defamation is also criminalized under the criminal Code. Article 613 of the code provides that whoever, addressing a third party, imputes to another, with the intent to injure his honor or reputation, an act, a fact or a conduct, where the allegation accords with the truth, is punishable, up on complaint, with simple imprisonment not exceeding six months or fine. If the defamation is made deliberately against public servant, the punishment will be increased

[194] *Ibid*.
[195] ACHPR, *Lohé Issa Konaté v. The Republic of Burkina Faso*, App. No. 004/2013, 5 December (2014).
[196] *Ibid* at para. 116.
[197] *Ibid*.
[198] See *supra* note 118.

to one year.[199] But, this is against the best practice in democratic states. Let alone increment of punishment for the defamation of public figures, standard of proof of such allegation in civil cases is high out there.[200]

Article 13 (3) of the Computer Crime Proclamation provides that *whosoever disseminates any writing, video, audio or any other image through a computer system that is defamatory to the honor or reputation of another person shall be punishable, upon complaint, with simple imprisonment not exceeding three years or fine not exceeding Birr 30,000or both.* This Article criminalizes Internet defamation and provides for increased number of years of imprisonment and amount of fine compared with the offline defamation regulated under the criminal code.

One may argue that the regulation of online defamation is right due to the nature of transmission of the defamatory word, video or image on the internet. Because, Internet has capacity to disseminate them to the every corner of the world in fraction of seconds. To stand against this, one may suggest criminal punishment to deter potential offenders and hit back the wrong doer. But, such argument doesn't hold water because of two things. First, as the nature of internet can facilitate swift dissemination of defamatory statement, equally, it has also a self-help mechanism for a person in similar capacity to do battle with the statement made against him or her. Second, stipulation of criminal laws may terrify individuals therefore, they may refrain from giving their important comments and suggestions about other individuals. This makes the essence of online freedom of expression to diminish. Due to this, the works and behaviors of individuals, especially, of government officials will not be scrutinized by the public. As a result, there will be lack of public control on the government officials and wrong behavior or conduct of persons may not be criticized. This shows that, criminalization of defamation in general and online defamation in particular is unnecessary as it attacks the very

[199]The Criminal Code of the Federal Democratic Republic of Ethiopia, Federal *Negarit Gazeta* Proclamation No. 414/2004 Article 618 (1) (b).

[200] U. S. Supreme Court, New York Times Co. v. Sullivan, 376 U.S. 254 (1964), this case was a landmark case that established the actual malice standard, which has to be met before press reports about public officials can be considered to be defamation and libel. See also Mark Tushnet, *New York Times V. Sullivan around the World*, 66 Alabama Law Review 337 (2014).

essence of freedom of expression for one thing and there is a civil remedy with less threat to free speech to correct the online defamation as a last resort.

Conclusion

Internet access which is the core for exercise of freedom of expression online is low in Ethiopia. This problem might have been curbed by privatizing telecom service and allowing as many competitive private ISPs as possible. But, both Ethiopian investment law and policy remained rigid by prohibiting private entities from delivering independent internet service. Given the duty of the government to facilitate universal access to information and a system through which opinions will be freely shared, entangling Internet access by laws and policies amount to systematic violation of freedom of expression and need to be corrected.

As it has been starkly discussed in this chapter, provisions of the proclamation that are intended to protect individuals' reputation and liberty employed vague words. The law limiting a right should be clear so as to notify the individual which behavior is prohibited and which is not. The computer crime proclamation couldn't provide for unambiguous words that identify the shield from the sword. The absence of clarity of words that say "intimidate" and "threat," and phrases that states "causes fear" and "causes psychological strain" under Article 13 (1&2) of the proclamation indicate that they fail to fulfill standard of limitation of freedom of expression which requires clear law. Lack of clarity of the words employed under Article 13 (1&2) makes them clumsy thus, cannot fulfill the standard of limitation of freedom of expression.

Article 14 which is aimed to protect public security also provided surreptitious phrases that have higher probability to be abused by government authorities to irritate journalists, bloggers, human rights defenders and the civilians as a whole. They may be interpreted to prohibit any dissent against the government or well-founded criticisms against the government's decisions or government officials. Thus, Article 14 can't pass the scrutiny under Article 19 (3) of ICCPR.

The proclamation criminalized online defamation under its Article 13 (3). Nevertheless, given the repercussion of criminal sanctions on freedom of expression, criminal law is not appropriate tool to regulate online defamation in democratic society. Because, for one thing, internet has provided a self-help mechanism through which defamed persons can sustain their

good name. If that is not enough to correct the wrong behavior, civil remedies can help to address the problem of defamation as the civil defamation laws provide sufficient redress for all those who claim to have been defamed. On the other hand, international standards require that any interference with freedom of expression must meet the three-part-test. Criminalization of defamation constitutes unnecessary and disproportionate measures on the exercise of freedom of expression with regard to matters of public interest, given its silencing effect that is unsuited to a democratic society.

CHAPER FOUR

CRIMINAL LIABILITY OF INTERNET SERVICE PROVIDERS

Introduction

Internet, through systems provided by internet service providers, gives information on almost every aspect of life. Acts of communication through Internet, regardless of their content, pass through a complex technological infrastructure, consisting of very different physical and logical elements. These complex systems are provided by ISPs. ISP are a broad range of actors, mainly private ones, who act as intermediaries by providing a range of services such as access and interconnection, transmission, processing and routing of Internet traffic, hosting and providing access to material posted by others, searching or referencing materials on the Internet, financial transactions, and connecting users through social networks, among other things.[201]

One of the controversial issues in the regulation of cyber activities is about the responsibilities of ISP with regard to the content data that are originally provided by the users and which are made available on internet passing through services of ISP. 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 paly only passive role. But, in few internet services, managing and controlling ability over the Internet of the ISP plays a significant role in the management of the online information and the protection of the Internet security.

Ethiopia is connected to internet through the government controlled ETC. This doesn't mean that ETC is the only internet service provider in Ethiopia. The provisions of the computer crime proclamation that deal with ISP touch every domestic and international ISPs.[202] This chapter

[201] Bradley Mitchell, *ISP - Internet Service Providers*, October 17, 2016 available at https://www.lifewire.com/internet-service-providers-817781 accessed on May 11, 2017.
[202] See Computer crime Proclamation *supra*, Article 42. This provision adopted principle of internationality that helps to regulate cybercrimes from each corner of the world.

assesses the provisions of the proclamation that deal with the liability of ISP in light of freedom of expression and right to data privacy.

4.1. Types of Internet Service Providers

There are various kinds of services connected with the Internet which different types of ISP deliver. The liability of the service provider should depend on the role played by the ISPs as criminal liability presupposes participation of a person to the commission of the crime. ISPs are categorized to various types depending on the services they provide.

4.1.1. Internet Access Provider

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.[203] Access providers are structured hierarchically[204] to control the physical infrastructure needed to access the internet and make the infrastructure available to individual subscribers in return for payment.[205] They may or may not control content of the data that passes through their service depending on their purpose and terms of service.

4.1.2. Transit Provider

Internet is a network of networks. To get connected to the Internet, an entity must attach itself to another entity that is already connected to the Internet. A transit provider allows interaction between a computer and the access provider, and hosting providers, and its function is merely transmission of data, mere conduit role. It usually facilitates this connection by purchasing a service called Internet transit. Generally, Internet transit is the business relationship whereby an ISP provides, usually sells, access to the global Internet. Metaphorically, Internet transit can be imagined as a pipe in the wall that says "Internet this way". [206]

---

[203] http://searchmicroservices.techtarget.com/definition/IAP-Internet-access-provider accessed on March 27, 2017.
[204] Hossein Bidgoli, *The Internet Encyclopedia*, California State University Bakersfield, California, 199 (2004).
[205] Article 19, *Internet Intermediaries, Dilemma of Liability*.
[206] http://drpeering.net/core/ch2-Transit.html accessed on March 28, 2017.

4.1.3. Hosting Provider

Hosts 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.[207] 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.

4.1.4. Content Provider

The term content provider refers to persons who use the above infrastructure to make available to end users the most diverse information, including web pages, services, email, connection between different end users and as many other possibilities as the mind can conceive, by delivering content created by the provider itself or by intermediaries or third parties.

4.2. Criminal Liability of Internet Service Providers

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 fundamental rights.[208] Differently, skeptics of network neutrality tend to see more active network management as meeting consumers' demand[209] and traffic differentiation as the only way for ISPs to safeguard a return of investment into next-generation Internet architecture.[210]

---

[207] Article 19, Internet Intermediaries *supra*.
[208] See Barbara Van Schewick, *Towards an Economic Framework for Network Neutrality Regulation,* 5 Journal on Telecommunications and High Technology Law 329, 392 (2007).
[209] See 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)
[210] See Robert E. Litan & Hal J. Singer, Unintended Consequences of Net Neutrality Regulation) 5 Journal on Telecommunications and High Technology Law 533, 596 (2007).

In the modern world, regulation of cyber activities to achieve social, political and economic ends is vital. Regulating internet without the involvement of ISP is unthinkable. There is growing relationship between governments and online corporations to control internet.[211] But, gate keeping ISPs would have a negative effect on receiving and imparting information.[212] Concerning the regulation of cyber activities through ISPs, the UNHRC stated in its general comment 34 that any restrictions on the operation of internet service providers is only permissible to the extent that it is compatible with paragraph 3 of Article 19 of the ICCPR.[213] 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, which is disseminated using those services, as long as it doesn't specifically intervene in that content or refuse to obey a court order to remove that content, where it has the capacity to do so.[214]

Making ISPs liable under guise of protecting public security or individual's reputation or liberty may affect the free circulation of internet services which negatively affects freedom of expression.[215] But this doesn't mean that freedom of expression simply entails the irresponsibility or impunity of the ISPs. Here, it is noteworthy to remember 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 for it. Though all ISP may participate in some way in the transmission or diffusion of the information; however, 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.

As far as liability of ISP who participates in production and edition of the content data is concerned, the 'liable editor' regime which is well-known in press laws[216] impose itself.

---

[211] Tully *supra* at 181.
[212] See Jasper P. Sluijs, *From Competition to Freedom of Expression: Introducing Article10 ECHR in the European Network Neutrality Debate*,12 HRLR 509, 554 (2012).
[213] UNHRC, General Comment No. 34 *supra* at para. 43.
[214] 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
[215] Rowland & Macdonald *supra* at 499.
[216] See Freedom of the Mass Media and Access to Information Proclamation, Article 6 cum. Article 45.

However, most ISPs are mere distributors or can be considered as libraries. Current technology does not allow ISPs to effectively control the volume of information introduced by its users. Moreover, the information cannot be controlled effectively without incurring disproportionate expenses like right to data privacy. Therefore, for the purpose of making ISP that have participated in the wrongful conduct liable, it is important to discern between ISP which can/ should control content and those can't/shouldn't control the content produced by their users. Then, the former will be liable controller and the later will be mere conduit. The liable controller here refers to the effective control of the information. If an ISP has the technical capacity to control the information effectively and uses this capacity, it can be held liable and vice versa. Generally speaking, the ISP's capacity to control information and its effective knowledge of the offence determine its obligations.

On the other hand, some ISPs save third parties' data automatically. Such ISP have technical capacity to control this data, but consider that it is not their function to do so. If ISPs have an 'effective knowledge', in contrast to the mere automatic reception of the data, that certain information is illicit, they have a duty to inform the relevant authorities. If an ISP fails to report an offence, it becomes accessory after the fact.

Realistically, some ISP are mere conduits. 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. As just mentioned, in most cases, intermediaries do not have, and are not required to have, the operational/technical capacity to review content 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 requisite number of operators and attorneys to perform such an undertaking, as private actors, intermediaries are not necessarily going to consider 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 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. It would also jeopardize the right of all persons to use the media they deem appropriate for the transmission of ideas and opinions.[217]

The general position held by international treaties and most of the national legislations is that ISPs are immune from liability for contents uploaded by their users.[218] There is an international consensus appeared to develop around the notion that holding online intermediaries liable for third party content of which they lack knowledge or control over is prejudicial to the functioning of electronic commerce and the exercise of freedom of expression. [219] 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.[220] This kind of attributive liability introduces strict liability in regulation of cyber activities. Doing so seems to conflict with some broadly shared and deeply felt intuitions regarding the individuality of responsibility and the relationship between responsibility and guilt, requirement of blameworthiness.[221] Even though strict criminal liability can be justified under criminal law when we see the whole activities done to commit the crime elements of crime,[222] the consequence has the chilling effect on freedom of expression. If ISP are made liable for the contents provided by the third parties, they will employ strict systems by which they check against prohibited contents. This limits the freedom of expression of the users only to what the ISP thinks, not what the law provides.

On the other hand, right to privacy requires that the ISP have to be kept away from the personal information of internet users. But if ISP are made criminally responsible for the contents provided by third parties, they must access one's every information to block illegal ones. This also limits the right to privacy of internet users. Finally, instead of fighting an uphill battle in

[217] OAS Rapporteur's report *supra*, para 99.
[218] Catherine Seville, *EU Intellectual Property Law and Policy*, 47 (2009).
[219] Lisl Brunner, *The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia,* 16, Human Rights Law Review, 163, 174 (2016).
[220] Anton Vedder, *Accountability of Internet access and service providers – strict liability entering ethics?*, 3 Ethics and Information Technology 67, 73 (2001).
[221] *Ibid*.
[222] See Kenneth W. Simons, *When is Strict Criminal Liability Just*, 87 J. Crim. L. & Criminology 1075, 1137 (1997).

jurisdictions where ISP are made liable for contents provided by third parties, victims of hate speeches and violence may turn attention to Internet access providers. This may discourage ISP from providing internet service and this will indirectly affect human rights i.e. freedom of expression.

4.3. International Human Rights Law and Criminal Liability of ISPs

In its general comment No. 34, UN Human Rights Committee stated that any restriction imposed on ISP should be compatible with Article 19(3) of ICCPR.[223] Similarly, in the joint declaration they adopted in 2011, the four regional special rapporteurs for freedom of expression stated that online intermediaries should not be liable for third-party content as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so.[224] Subsequent reports of the UN Special Rapporteurs of 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.[225] 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.[226]

As the issue has been a prominent and recurrent feature of international debates on Internet governance, 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 liability.[227] Generally, there is international consensus on the fact that holding ISP liable for the content produced by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads

[223] General Comment No. 34 *supra* at para. 43.
[224] Joint Declaration on Freedom of Expression and the Internet *supra* at para 2.
[225] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* at para 102.
[226] Joint Declaration on Freedom of Expression and the Internet *Supra* at para 2(b);
[227] 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.

to self-protective and over-broad private censorship which also affects right to data privacy, often without transparency and the due process of the law.[228]

4.4. Liability of ISPs under the Computer Crime Proclamation

Before assessing the rules that provide for liability of ISPs, it is important to identify ISPs in Ethiopia. Article 2(13) of the proclamation states: "Service provider" means a person who provides technical data processing or communication service or alternative infrastructure to users by means of computer system."[229] This definition is broader and include every person or entity that provide internet access, transits service and hosting service. Though ETC is the sole ISP that controls everything regarding Internet service in the country, private sectors can provide value added services or act as a reseller by obtaining a license from the MCIT and signing service delivery agreement with ETC.[230] Accordingly, there are few internet cafes,[231] web hosts and blog owners in Ethiopia. Oversea ISPs like Facebook, Google, and Twitter are also subjected to the law[232] if the crime is committed in Ethiopia, against Ethiopia or Ethiopians.

In many national laws, international human rights laws and model laws, 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.[233] It is a widely recognized principle that 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 the well-established principle of immunity of the ISP for third party contents, the Computer Crime Proclamation made them criminally liable under various conditions under

[228] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* at Para. 40.
[229] Computer crime proclamation *supra* Art. 2(13).
[230] See Ministry of Communications and Information Technology, *License Directive for Resale and Telecenter in Telecommunication Services Directive*, Directive No. 1/2002.
[231] Ministry of Communication and Information Technology Federal Democratic Republic of Ethiopia, 1 Communication and Information Technology Statistical Bulletin 4 (2014).
[232] *Ibid* at Pag.30.
[233] Kinfe Micheal & Halefom Hailu, *The Internet and Ethiopia's IP Law, Internet Governance and Legal Education: An Overview*, 9MLR 154, 161 (2015).

its Article 16. To have the full picture of the article, it is important to see the conditions of liability of ISPs in the following sections.

4.4.1. Direct Involvement of ISP in the Dissemination of the Content Data

The first statement of Article 16 (1) makes ISP liable if it is directly involved in the dissemination of the illegal content. The proclamation doesn't provide for what does it mean by "direct involvement." It may mean direct participation in the dissemination of readymade content data. But from the general theory of criminal liability,[234] we may conclude that ISPs which play a role in providing access to third party content but that doesn't know the content of that data shall not be considered as content publishers and made liable. Most of the internet access providers merely facilitate internet access for persons and they may not know or are expected to know the content of the data. Similarly, web hosts which facilitate publication of Internet blogs and comments, though they involve in dissemination of the information, are not thereby become publishers of the blogs.[235] 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.[236] Nevertheless, according to Article 16(1) of the computer crime proclamation, if certain ISP directly involved in the dissemination of some illegal content data without having knowledge of its content, it is criminally responsible. Applying this rule to the internet access providers, hosts and transits that, by their very nature, do not contribute to the content or know or expected to know the content of data is awkward. However, according to the broad definition of the ISP under the proclamation,[237] dissemination of the illegal content data by ISP, who has no knowledge of the content produced by third party by itself is punishable. If this is the case, it

[234] See George P. Fletcher, *The Theory of Criminal Liability and International Criminal Law*, 10 JICJ 1029, 1044 (2012).
[235] Ter Kah Leng, *Internet defamation and the online intermediary*, 31 computer law & security review, 6 8, 7 7 (2015).
[236] *Ibid*.
[237] Computer Crime Proclamation *supra* Article 2(13).

is incompatible with basic theory of criminal liability and has a negative effect on freedom of expression and right to privacy as ISP will desist providing internet service in Ethiopia or if they prefer to provide, they censor each content of the data of their users that pass through their services that violates right to data privacy. This makes the provision short of passing the three-part-test. Because, criminalization of data disseminators without cognizance of its content is unnecessary in the modern society in which information is back bone of development in every aspect of life.

4.4.2. Direct Involvement in Edition of the Content Data

If an ISP involved in edition of content data, this presupposes that the ISP not only has knowledge but also contributed to the illegal content. In this case, the ISP is participated in producing the 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. For instance, they 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 to be posted on their pages. In such case, Facebook page can be compared to a noticeboard where third parties can post comments but the host has ultimate power to control content and the ability 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. The users also know that what they posted on the pages may be blocked or removed by the creator.

4.4.3. Upon Obtaining Actual Knowledge that the Content Data is Illegal, Failed to take any Measure to remove or Disable Access to the Content Data

Under Article 16 (2) of the proclamation, if ISP 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, it will be liable under Articles, 13, 14 and 15 of the proclamation. "Actual knowledge," which is provided under Article 16 (2) is not defined in the proclamation. By their very nature, some ISP are not in position to know the content of the data transmitted through their services. It seems that this provision is framed in line with the importance of ISP to do in cooperation with the government to facilitate full disclosure and discontinuing of illegal practices. But this can be fully addressed by the duty to notice which Article 27 of the proclamation provides. Even if the ISP have actual knowledge of the illegality of the data, it is unnecessary to make them liable for the crime. Because, such mechanism puts private ISPs in the position to make decisions about the lawfulness or otherwise of the content and to protect themselves from liability, apply their maximum effort to censor data of their users. ISPs, because of their strategic position in the communications networks, can employ a range of software solutions to reduce offending online data by employing robust security systems accompanied by sophisticated professional spam filters.[238] Because, 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.[239]

4.4.4. Failed to Take Appropriate Measure upon obtaining Notice from Competent Administrative Authorities

In most of the cases, ISP can argue successfully that they do not take an active part in the actual process of communication or they may be able to rely on the defense of innocent dissemination. The risk inherent in this approach is, of course, that if service providers are able to rely on this defense and the author of the illegal content data cannot be traced, a victim has no effective remedy against illegal Internet contents or a crime may not be effectively prevented. Article

[238] 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).
[239] *Ibid.*

16 (3) seems to dissolve such problem but it employed problematic provision that affects freedom of expression and right to data privacy.

Article, 16 (3) of the proclamation seems to adopt mechanism of notice and take down. According to mechanism of "notice and take down," in exchange for protection from liability, ISP are required to take down content that a third party, more or less qualified according to the respective judicial system, alleges to be unlawful. This mechanism is developed in USA jurisprudence and disseminated to other states. But, the proclamation doesn't require for qualified judicial organ to decide illegality of the content data. It clearly authorizes administrative authorities to decide the illegality and to order the ISP to remove or disable access to the data.

Though this mechanism is important in controlling cybercrime, it has its own repercussion on freedom of expression and right to data privacy thus, cannot pass scrutiny under the three-part-test. According to Article 16 (3) of the proclamation, if certain content of data posted in certain website is contested and declared illegal by the competent administrative authorities, the web master is duty bound, according to article 16(3) of the proclamation, to take down that data. But, the administrative authority is not right organ to decide legality or otherwise of data. In Ethiopia, it is a court which has inherent judicial power.[240] Such procedure cannot be fair and contents which are legal may be removed from the wrong appreciation of the administrative authority or due to their political sensitiveness. Furthermore, the proclamation doesn't provide for right to appeal against this decision. Therefore, such action may arbitrarily enmesh freedom of expression.

Mechanism of notice and take down has also its own pitfalls. Although it allows the order to take down after the appropriate judicial organ has decided the illegality of the content, 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,

[240] FDRE Constitution *Supra*, Article 78.

developed a human rights friendly system called "Notice and Notice."[241] The mechanism on Notice and Notice dictates that the intermediaries shall not take down what users uploaded, rather, getting notified by the competent judicial organ to decide the legality of the content of the data, they are duty bound to notify the person that uploaded the content. This system is also buttressed under Manila Principle. [242] Nevertheless, the proclamation failed to provide the minimum guarantee that the mechanism of notice and take down provides.

4.4.5. Duty to Report

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.[243] Accordingly, service providers are required to report to INSA and the police when they come to know of the commission of cybercrimes or circulation of illegal content on their computer systems. It is obvious that everyone shall support justice by reporting commission of crime. The proclamation imposes a specific duty to report commission of cybercrime on ISP depending on the technical position that they have as far as Internet is concerned, because they can detect when certain computer system is hacked or intercepted for instance. Actually, this provision was drafted on the assumption that every ISP has the knowledge of content data that passes through its service.[244] But, as it is discussed somewhere in this study, most of the internet service providers cannot 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.[245] In his effort to display challenges ahead of the computer crime proclamation, regarding the issue at hand, Kinfe feared that service providers could be prompted to employ algorithmic bots to automatically detect illegality which, as we know, could impact not just the right to privacy but also free expression online.[246]

---

[241] http://www.entertainmentmedialawsignal.com/online-infringement-canadian-notice-and-notice-vs-us-notice-and-takedown accessed on March 27, 2017.
[242] Manila Principles *supra.*
[243] Computer Crime Proclamation, *supra*, Art. 27.
[244] The Explanatory Notes of Computer crime Proclamation at 37.
[245] Kinfe Micheal, *Some Remarks on Ethiopia's New Cybercrime Legislation*, 10 MLR 448, 453 (2016).
[246] *Ibid*.

But, as it stands now, Article 27 of the Computer Crime Proclamation doesn't impose obligation that every ISP should know every crime committed through their services, but if they come to know the commission of the crime, they bear duty to report. Nothing is provided in the proclamation as to the punishment if an ISP fails to comply with the duty to report. It may be provided in the regulations to be made by the council of minister in line with the proclamation.[247]

Conclusion

Article 16 of the proclamation, makes ISP criminally liable in principal capacity when certain illegal content data is transmitted through their service. But, there is international consensus that ISP should not be liable for the content produced and uploaded by the users. According to the first statement of Article 16 (1) the proclamation, ISP may be criminally liable if they disseminate illegal content data. Article 16 (2) empowers ISP the power to decide on legality or illegality of a content data that may give rise to horizontal violation of freedom expression and right to data privacy. Article 16 (3) defectively adopted mechanism of notice and take down and authorizes the administrative authorities to decide over legality of content data. In general, provisions of Article 16 of the proclamation allow interference of private entities (ISPs) in the privacy of internet users and to block their free speech under the pain of prosecution. They also allow administrative authorities to rule over legality of content data and order their removal. Such system enhances obstruction of political sensitive speech. Generally, save the second statement of Articles 16 (1) and 27 of the proclamation that provide for criminal liability of ISP that directly involved in editing of the illegal content data and imposes duty to report on ISPs respectively, the remaining provisions of the proclamation; i.e, the first statement of Article 16(1), Article 16(2) and Article 16(3) provide unnecessary limit on the freedom of expression and right to data privacy.

[247] Computer Crime Proclamation *supra*, Article 44.

CHAPTER FIVE

REGULATION OF DIGITAL FORENSICS

Introduction

With the advancement in information technology, data privacy is no longer limited to paper information and has extended to various kinds of electronically stored information such as emails, faxes, instant messages, electronic word documents, voice mails, digital images, spreadsheets etc. These kinds of data have increasingly become the focus of investigation in criminal cases. Prevention and prosecution of computer crime require special procedural rules that guide how to screen out illegal acts and collect evidences of computer abuse. As they are privacy sensitive, these procedural rules must be evaluated against the standards of limitation of right to privacy. The computer crime proclamation has provided special procedural rules that regulate real-time collection of data, preservation of evidence, production of evidence and computer search and seizure that impose limitation on right to data privacy. Under this chapter, procedural rules of the proclamation that regulate digital forensic will be assessed in light of the standards of limitation of the right to privacy which require that the limitation should be prescribed by law, necessary in democratic society and only imposed to protect legitimate aim.

5.1. The Right to Privacy in Surveillance or Interception of Communication

Electronic surveillance is a type of search and seizure that uses of electronic devices to monitor a person's activities or whereabouts and can take various forms, such as wiretapping or bugging.[248] Access to a computer in a suspect's possession may require a search warrant. By contrast, a suspect's stored email can be obtained from a service provider by order. Similarly, basic customer or subscriber information may be obtained from a carrier or service provider through a court order. As far as digital forensic is concerned, while laws of some countries provide for general search warrants, others require great specificity regarding the premises to be searched, and the nature of the evidence sought.[249]

[248] Rolando V. del Carmen, *Criminal Procedure Law And Practice* (7th edit.) 257 (2007).
[249] United States Department of Justice, *Searching and seizing computers and obtaining electronic evidence in criminal investigations*, Washington, DC: US Department of Justice (2002). Accessed on February 27, 2017, from http://www.cybercrime.gov/s&smanual2002.htm.

The general assumption in digital forensic investigation is that the investigators have vested interest in users' information; because they are important in proving a computer crime case in a court. The nature of digital technology has complicated the challenge of search and seizure in Internet world.[250] Though evidentiary data may be dispersed across a computer network and removed from the physical location of a search, it may be accessed through computers located on the search premises.[251] Governments can have legitimate reasons for undertaking surveillance of communications, for instance, to combat crime or protect national security. However, since surveillance highly interferes with the rights to privacy,[252] it must be done in accordance with strict requirements of the three-part-test that require a surveillance must be targeted, based on reasonable suspicion, undertaken in accordance with the law, necessary to meet a legitimate aim and be conducted in a manner that is proportionate to that aim, and non-discriminatory.

Digital forensic investigation may be effected through surveillance and interception of communication. Since its introduction to the field, digital forensics investigators have faced challenges in finding the balance between retrieving key evidences and infringing user privacy.[253] In response to this, surveillance and interception of communication must be clearly prescribed by law, necessary to achieve a legitimate aim, and proportional and narrowly tailored to achieving the aim.[254] On this point, the UN Special Rapporteur on Freedom of Expression has stated that:

> Communications' surveillance should be regarded as a highly intrusive act.… Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope, and duration of the possible measures, the grounds required for ordering them, the authorities competent to

[250] See Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, I9 International Journal of Cyber Criminology 55,119 (2015).
[251] Peter Grabosky, *Requirements of prosecution services to deal with cybercrime*, 47 Crime Law Soc. Change 201, 212 (2007).
[252] See Molalign Asmare, *Enhanced Forms of Criminal Investigation: Analysis on Its Potential Risks to Human Rights*, 7 Beijing Law Review, 33, 41 (2016).
[253] Asou Aminnezhad et al, *A Survey on Privacy Issues in Digital Forensics*, 1 International Journal of Cyber-Security and Digital Forensics (IJCSDF) 311 (2012).
[254] See UNHRC, Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, U.N. Doc. A/HRC/13/37, (December 28, 2009) paras. 17-18.

authorize, carry out and supervise them, and the kind of remedy provided by the national law.[255]

It is important to remember that when the human rights instruments require that limitation of right to privacy must be prescribed by law, they mean that it must meet a standard of clarity and precision which is sufficient to ensure that individuals have advance notice of and can foresee their applications. And, the proportionality requirement is a primary criterion in determining whether human rights interference can be considered necessary in a democratic society,[256] accordingly, any surveillance measure must not be employed when less invasive techniques are available,[257] and must be proportionate to the interest to be protected.

In normal course of things, there are several digital forensic investigations that do not violate a person's reasonable expectation of privacy, and thus allow computers to be searched without a warrant. These conditions can be justified in any jurisdiction because, from the very definition of right to privacy, it is clear that the subject of the right may waive it by his or her publicizing his/her personal information. For instance, if the person has made the computer openly available, such as making the boot-up password visible, there is no reasonable expectation of privacy since he/she did not guard access ability. Likewise, if the information to be examined has been transmitted via the internet or received by someone via e-mail, there is no reasonable expectation of privacy since the individual relinquished that expectation when he/she transmitted it. Lastly, if a computer has been handed over to a third party, such as a repair shop, it is assumed that the person relinquished his/her reasonable expectation of privacy by granting computer access to a third party. Therefore, in order for a computer owner to preserve his/her reasonable expectation of privacy, and thus eliminate possibilities of a warrantless search, he/she should limit third party's access to the computer in all ways possible.

Consent of the user may also relieve the investigators from applying for warrant. Investigators may search a place or object without a warrant, or even probable cause, if a person with authority has voluntarily consented to the search. This also applies if there are several people

[255] Report of the special rapporteur on surveillance *supra* para. 81.
[256] Toon Moonen, *Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights*, 9 Peace Int' l L. Rev. Online Companion, 97, 105 (2010).
[257] Carmen *supra*.

who share a computer, and any person who has authority over the computer consents to a search. Spousal consent searches are often valid as well, as long as the consenting spouse has access to the computer. Consent from parents in regard to a minor's computer is also valid. Similarly, if the computer to be searched is a stolen one, it is assumed that there is no expectation of privacy, since the computer does not belong to the person.

5.2. Regulation of Digital Forensics under the Computer Crime Proclamation

Part three of the proclamation provides procedural rules, *inter alia*, that regulate digital forensic investigation. It provides the principle that dictates rules provided to regulate digital forensics investigation shall be implemented and applied in a manner to ensure protection for human and democratic rights guaranteed under the FDRE Constitution and all international agreements ratified by the country.[258] Though this principle notifies the investigatory organ that it should respect human rights of the suspect, the proclamation doesn't give full guarantee to human rights as the specific provisions that regulate special measures to be taken to prevent cybercrime and collect digital evidences do not provide necessary safeguards to right to privacy of internet users. The proclamation provides four procedural rules that are privacy sensitive.

5.2.1. Real-time Collection of Computer Evidence

Article 25 of the proclamation provides that the investigatory organ (INSA) can intercept in real-time or conduct surveillance on computer data, data processing service, or internet and other related communications of suspects with or without warrant depending on the urgency of the need to prevent and investigate cybercrime. This investigative power, in principle, is subject to independent judicial review.[259] The proclamation also allows real-time collection of computer evidence as a last resort, only when there is no other means readily available for collecting the data.[260] However, Article 25(3) of the proclamation allows interception or surveillance of a communication on internet without warrant where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is or to be committed. "critical infrastructure," according to Article 2(11) of the proclamation is a computer system, network or data where any of the crimes prohibited under

[258] Computer Crime Proclamation *supra* Article 21.
[259] Ibid Article 25(1).
[260] *Ibid* Article 25 (2).

Articles 3 to 6 of the proclamation, meaning, crime of illegal access, illegal interception**,** interference with computer system and causing damage to computer data, is committed against, would have a considerable damage on public safety and the national interest. This infrastructure, according to the Explanatory Notes of the proclamation[261] may be:

1. The controlling system of defense force or
2. Information networks and secret data of peace, security and justice institutions or
3. Information networks and secret data of financial institutions or
4. Computer systems that control basic public services like: water, power and communication services or
5. Transportation systems, especially air and rail transportation systems or
6. Media and communication systems or
7. Education, health and higher research institutions systems etc.

It is important to understand from the outset that such interception and surveillance allowed under article 23(3) is impermissible for other crimes provided under other provisions of the proclamation save those that are prohibited under Articles 3 to 6 of the proclamation. But this doesn't mean interception and surveillance of communications conducted without warrant to prevent these crimes doesn't strengthen the government's surveillance capabilities by enabling real-time monitoring or interception of communications and affects right to privacy. There are some practical set ups in Ethiopia that are threat to privacy beside authorization of interception and surveillance without warrants by the proclamation.

5.2.1.1. Proliferation of Collection of Personal Data

Now a days, the government of Ethiopia is highly concerned with the collection of personal data. The National Identification Card law requires collection of sensitive personal data and permits cross-organizational transfer of the data to other institutions including intelligence authorities without requiring the consent of the subject of the data.[262] Accordingly, the data can be handed over to security organs and may be used to target on certain persons whom the government want to control and privacy of such individuals may be intruded arbitrarily.

[261] Explanatory Notes of the Computer Crime Proclamation Page 8.
[262] Registration of Vital Events and National Identity Card Proclamation, Federal *Negarit Gazeta*, Proclamation No. 760/2012, Articles 63 &64.

Similarly, ETC enforced registration of mobile SIM cards with the names and address of registrants. These data are expected to be archived in databases which need robust security mechanisms.[263] With easy and seamless cross-organizational personal data transfer practices already in place in Ethiopia, the rise of SIM card registration is a troublesome practice that makes exercise of legitimate anonymity difficult.[264] The Ethiopian government is ostensibly motivated by the belief that forcing customers to register SIM cards will reduce the opportunities for malevolent actors to use mobile devices anonymously to undertake unlawful or socially harmful activities.[265] Because, governments fear that in markets in which SIM cards are not registered with personally identifiable information, users have the opportunity to communicate without attribution and are thus outside the immediate reach of the police.

SIM registration complicates the much lauded developmental and emancipatory influences of anonymity. These identification mandates may bring modest security benefits, although most of the times, the evidence for such claims remains inconclusive.[266] The right to privacy and the right to freedom of expression entail a corollary right to communicate anonymously. Allowing people to speak anonymously has long been recognized as worthy of protection in order to encourage communication that might otherwise invite reprisal or stigmatization, from political pamphleteering, to anonymous tips for journalists, to blowing the whistle on improprieties in the workplace or government.

Anonymity, of course, may also be sought by persons engaged in criminal activity, so it is not an absolute right. But neither may the freedom to communicate anonymously be subject to such restrictions as would eliminate the right a *priori*. The special rapporteur on freedom of expression has addressed the legality of real-name registration policies and offensive intrusion tactics that is, secretly infiltrating a computer to steal files or monitor activity and has called on governments to ensure individuals can express themselves anonymously online and to refrain from adopting real-name registration systems.[267] He further stated that, in order not to

[263] Kinfe Micheal, *Data privacy law and practice in Ethiopia*, supra at 183.
[264] *Ibid*.
[265] Donovan, K. and Martin, A., *The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change*. 21, (2014). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820 .
[266] *Ibid* at 23.
[267] Report of the special rapporteur on the Internet, para. 84.

hamper individuals' rights to data privacy, governments should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés, or mobile telephone.[268] In light of the practical repercussion that such measures may create, SIM card registration has negative effect on freedom of expression as persons cannot freely communicate on Internet as they are under control and will be devoid of their right to privacy on Internet as their secret information can be accessed through by ETC. The monopoly of the government over the ETC ensures that the government can effectively limit individuals' access to internet. This has the effect of curtailing freedom of expression and right to data privacy as there is no independent organ which can ensure that the surveillance practice is not abused in Ethiopia. This system makes the government omnipresent to actually control individuals' online activities by their mobile phones.

5.2.1.2. Proliferation of Surveillance Technologies in Ethiopia

The Ethiopian government is increasingly embracing technology in all of its activities including law enforcement purposes, and is reportedly acquiring the most advanced surveillance technologies.[269] Some human rights reports about the country indicate that there are violations of the right to privacy, including warrantless search of private property, illegal surveillance, monitoring of telephone conversations, and interference with e-mail by using surveillance technologies.[270]

Deep Packet Inspection technology that helps to examine the content of electronic communications such as e-mail or web queries and capable of monitoring private communications of users and enables filtering content[271] is installed by ETC and has been in use.[272] This technology would practically enable ETC to intercept and follow almost every

[268] Report of the special rapporteur on surveillance, para 88.
[269] Kinfe Micheal, *Data privacy law and practice in Ethiopia*, *supra* at 183.
[270] The Office of the UN High Commissioner for Human Rights (OHCHR), A Report on Ethiopian Human Rights Situations for Universal Periodic Review, A/HRC/WG.6/6/ETH/3, 22 September 2009, para 30. See also United States Department of State Bureau of Democracy, Human Rights and Labour, Country Report on Human Rights Practices for 2012, Ethiopia 2012 Human Rights Report, pp. 10, 11.
[271] See C Hangey, *Deep Packet Inspection and Your Online Privacy: Constitutional Concerns and the Shortcomings of Federal Statutory Protection*, University of San Francisco School of Law Working Paper Series, (2008) available at http://bit.ly/19cLkGp accessed on May 1, 2017.
[272] Human Rights Watch, *They Know Everything We Do*, Telecom and Internet Surveillance in Ethiopia 59 (2014).

communication over the net thus, it inevitably interferences with constitutionally guaranteed privacy of communications.[273] Similarly, ZSmart customer information system that is capable of recording data such as metadata, content of SMS texts, as well as location data and all phone calls made over ETC networks is also alleged to be in use by Ethiopian government.[274] ZXMT is another technology that is capable of scanning all Internet traffic and intercepting web-based e-mail, email accessed via client software such as Microsoft Outlook, and web browsing and chats that is in use by the Ethiopian government according to the HRW report.[275]

It is also indicated by findings of researchers from the University of Toronto that there are command and control servers for an offensive digital intrusion software called FinSpy in Ethiopia that controls online communication of some targeted Ethiopians abroad.[276] It is also found that Ethiopia has sought Chinese assistance in monitoring domestic communications and the Chinese telecommunications giant Huawei has moved from simply providing infrastructure to actively managing communications networks in Ethiopia.[277] In 2013, researchers at the Citizen Lab identified and analyzed a FinSpy sample that communicated with an active command and control server in Ethiopia that have been following the online communications of some Ethiopians overseas. The spyware is capable of stealthily transmitting chats, Web searches, files, e-mails, and Skype calls to a server somewhere in Ethiopia.

There are some foreign court cases in which Ethiopian government was sued for it allegedly intercepted and wiretapped the communication of some Ethiopians abroad. In 2014, Privacy International, a UK nongovernmental organization which is dedicated to investigations tackle what it perceives to be the unlawful use of surveillance, presented the case that alleging that Ethiopian government has employed FinSpy to control every communication *Teddese Kermiso* did by his computer being in UK. The result of the scan of the person showed that between 1.59am of 9th June 2012 and 10.49pm of 10th June 2012 FinSpy had been active on the

[273] Kinfe & Halefom *supra* at 28.
[274] *Ibid* 37.
[275] *Ibid* at 62.
[276] Morgan Marquis-Boire et al, *You Only Click Twice: FinFisher's Global Proliferation*, Citizen Lab, Research Brief No. 15, March 2013, available at https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2 accessed on May 4, 2017.
[277] Donovan & Martin *supra*.

computer of the victim being directed and controlled from Ethiopia.[278] But, Ethiopia has strongly denied the accusations. It was considered as a fabrication by groups bent to tarnish the image of Ethiopia by the spokesperson of Ethiopian Embassy in London.[279] The Privacy International submitted that the equipment used in Ethiopia by security forces was supplied illegally to the states by Gamma International in breach of export regulations applicable to that company in the U.K. thus, the organization took legal action against Gamma International.[280] The claim presented by the Privacy International representing Teddesse was that the Ethiopian government illegally intruded in to the privacy of the person and Gamma International refused to disclose information about the surveillance stating that it had no power to provide information about its investigations to Privacy International or to any third person, including victims of foreign regimes who used the company's products for surveillance purposes. The Privacy International took this case to the UK high court which decided that Gamma International should reconsider the application and restart the investigation.[281]

In *Kidane Vs Ethiopia* case, an American citizen living in Maryland sued the Ethiopian government for infecting his computer with secret spyware, wiretapping his private Skype calls, and monitoring his entire family's every use of computer for a period of months.[282] In the case, the Ethiopian government has never denied that it wiretapped Kidane's communication, but won dismissal of the lawsuit on the grounds that the digital attack was originated in Ethiopia and hence, the foreign court lacks jurisdiction over the case.[283] The case was taken to United States Court of Appeal for the District of Columbia Circuit and the appellate court confirmed the decision of the lower court for the very reason the lower court dismissed the case, lack of material jurisdiction.[284] The decision is extremely dangerous for right to privacy online. According to the decision, foreign state is free to intrude into privacy of individuals abroad in their own homes so long as it does so by remote control. Generally,

[278] *Ibid* para. 31.
[279] https://motherboard.vice.com/en_us/article/the-fight-to-uncover-spyware-exports-to-repressive-regimes accessed on May 4, 2017.
[280] See The High Court of Justice Queen's Bench Division, Administrative Court, (2014) 1475 (Admin).
[281] The High Court of Justice Queen's Bench Division, Administrative Court, (2014) 1475 (Admin). Para. 186.
[282] Morgan Marquis-Boire et al, *supra.*
[283] United States District Court for the District of Columbia Case No. 1:14–cv-00372, 2016.
[284] U.S. Court of Appeals for the District of Columbia Circuit, *Doe v. Federal Democratic Republic of Ethiopia*, Case No. 16-7081, March 14, 2017.

Ethiopian government has got sophisticated surveillance technologies that help to undertake a mass and targeted surveillance. Given the violent and secret nature of surveillance, strict regulation is expected from the computer crime proclamation but the proclamation leaves some spaces that leads to abuse of surveillance by the investigatory organ.

5.2.1.3. Lack of Transparent Interception and Surveillance

Transparency of surveillance is important for public oversight. It helps the public to get sufficient information to scrutinize how those laws that regulate surveillance are working in order to make informed decisions,[285] whether at the ballot box or by deliberating with others over matters of public policy.[286] Public oversight requires the government to release sufficient, clear, and precise information to the public to allow serious assessment of the necessity and proportionality of the use of surveillance by the investigatory organ in practice. Hence, transparency helps to hold investigators responsible for their behavior.[287]

The secret nature of surveillance poses a great challenge on individual's access to judicial review.[288] Revelations such as the Snowden leaks have shown that governments have in the past abused powers of surveillance, and the only way to prevent this is by transparency and providing redress to those affected. As far as surveillance of communication in Ethiopia is concerned, there has been no transparency on the extent of use of these technologies as well as the procedures through which law enforcement officers gain access to individuals' private matters.[289] The absence of transparency means that the use of surveillance technologies cannot be checked as there is no any other clear accountability or oversight mechanisms for them.[290] The fear in this scenario is that if abused, digital surveillance can enable governments that fail to uphold human rights to identify journalistic sources, government critics, or members of persecuted minority groups and expose such individuals to retaliation.

---

[285] Andrew T. Kenyon & Megan Richardson, *New Dimensions in Privacy Law*, 105 (2006).
[286] *See* ARTICLE 19, *The Public's Right to Know: Principles on Freedom of Information Legislation,* June 1999.
[287] Lorna Stefanick, *Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World*, 14 (2011).
[288] Molalign, *Enhanced Forms of Criminal Investigation supra* at 40.
[289] Kinfe, *Some Remarks on Ethiopia's New Cybercrime Legislation*, *supra* at 453.
[290] *Ibid*.

5.2.1.4. Absence of Sufficient Safeguards to protect Privacy

Merely legislating the law that authorizes surveillance of communication may give rise to a menace of surveillance that amounts to an interference with the privacy of all those to whom the legislation will be applied.[291] In view of this risk, there must be adequate and effective guarantees against abuse of what is laid down in the law.[292] However, the proclamation fails to provide for sufficient safeguards. The international human rights law requires safeguards that consist of requirements of legality, proportionality and necessity, as well as transparency, accountability and due process to prevent the abuse of power of surveillance. Though investigation normally focuses on the collection of information that is related to a specific crime, there may be a chance that the investigator will come across private information which is not related to the case. When it comes to the digital world, thousands upon thousands of digital files may be stored in a single digital storage medium. This greatly increases the risk of information disclosure and there are instances in where private data can be disclosed upon a loss of physical digital storage media like USB devices.

The jurisprudence on the legality of interception and secret surveillance in other jurisdictions offers valuable insight in this regard. For instance, the ECHR has held that the mere fact that there is a law authorizing interception does not validate the legality of the interception unless the law in question indicates, with reasonable clarity, the scope and manner of exercise of the relevant discretion conferred on the public authorities to give the individual adequate protection against arbitrary interference.[293] Similarly, the Council of Europe recommended that the special investigative techniques should be adequately defined in the national legislations about the circumstances under which the competent authorities are entitled to the use of those techniques.[294]

---

[291] See Richard Hunter, *World without Secrets*, (2002).
[292] Mooneh, T. *Special Investigation Techniques. Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights*, Pace Int'l L. Rev. Online Companion, 97, 106. (2010).
[293] ECtHR: Kruslin v France [1990] Application No. 11801/85.
[294] Council of Europe, Recommendation 10 of the Committee of Ministers to Member States on "Special Investigative Techniques" in Relation to Serious Crimes Including Acts of Terrorism, 2005, Para. 1.

One method that helps to protect the private data in the digital format is encryption, which helps to prevent unauthorized disclosure of individuals' innocent information.[295] Without the inclusion of data privacy protection into the digital forensics investigation technique, private information can only be protected through individual operating procedures which limits the search for evidence to the goal of investigation. It is important to design solutions in response to this demand. However, nothing is provided in the proclamation concerning measures to be taken by the investigators except the rubric provision which requires that the investigatory organ should respect human rights of suspected persons in general terms. However, this concern may be considered in the online computer crimes investigation system and technologies that INSA will establish to facilitate the investigation of cybercrimes.[296]

5.2.1.5. Absence of Independent Organ that Oversight Surveillance

International human rights law requires that the use of lawful surveillance powers by public officials must be attended by independently organ that monitors the strict safeguards against abuse. Judicial control offers the best guarantees of independence, impartiality and a proper procedure in surveillance of communication. The prior judicial authorization of surveillance powers is not merely desirable but essential in view of the effect that the interception and surveillance of communication have on right to data privacy. Neither of the other two branches of government is capable of providing the necessary degree of independence and objectivity to prevent the abuse of surveillance powers. Among its recent recommendations relating to Nation Security Agency surveillance, the UN Human Rights Committee recommended that the USA government should provide for judicial involvement in the authorization or monitoring of surveillance measures.[297] Similarly, the special rapporteur on human rights in counter terrorism straightforwardly argued that there must be no secret surveillance that is not

[295] Hou, S; Uehara *et al*, *Privacy preserving confidential forensic investigation for shared or remote servers*, The 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2011), Dalian, China, 14-16 October 2011. Available at http://hdl.handle.net/10722/152021
[296] Computer Crime Proclamation *supra* Article 39.
[297] UNHRC, Concluding Observations on the 4th U.S. report, 27 March 2014, available at: http://justsecurity.org/wp---content/uploads/2014/03/UN---ICCPR---Concluding---Observations---USA.pdf, para. 22

under the review of an effective oversight body and all interferences must be authorized through an independent body.[298]

Under Article 25 (3) of the proclamation, prior authorization by court is not required. Rather, the proclamation adopts mechanism of retroactive authorization by the president of federal high court.[299] The proclamation empowers the Federal General Attorney to give prior permission for interception and surveillance. However, independency and impartiality of the General Attorney remains under question. As the General Attorney is in charge of prosecution in criminal cases, it is difficult to expect impartiality from such organ in deciding whether surveillance has to be undertaken or not. Basically, the establishment of the office encounters certain paradox. Though one of the purposes behind establishment of the Federal General Attorney is to have an independent organ to oversee the general process of prosecution in the country,[300] there are many provisions in the establishment proclamation that have the effect of eroding its independency.

Article 16 (1) of the Federal Attorney General Establishment Proclamation states that the Federal Attorney General discharges its powers and duties based on law being independent from any interference of any person or body. However, other provisions of the proclamation provide provisions that backlash the independence of the Attorney General. For instance, the Federal Attorney General is made accountable to the Prime Minister and the Council of Ministers.[301] In addition, the Attorney General and the Deputy Attorney Generals may be removed from their position by the decision of the Prime Minister.[302] Members of Ethiopian Legal Community voiced their concerns that the involvement of the executive, especially, the chief executive, in the day-to-day activities of the Attorney General affects the institutional and professional independence of the office.[303] Giving the role to authorize interception and

[298]Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, (2013) para. 62.
[299] Computer Crime Proclamation *supra* Article 25 (4).
[300] Federal Attorney General Establishment Proclamation, Federal *Negarit Gazeta*, Proclamation No. 943/2016, preamble para.3.
[301] *Ibid* Article 3(2).
[302] *Ibid* Article 10.
[303] Staff Reporter, *Establishing the Attorney-General: Reconstructing the justice system or heralding a new one?* Written on 26 Nov, 2015. Available at http://www.thereporterethiopia.com/content/establishing-attorney-general-reconstructing-justice-system-or-heralding-new-one accessed on May 3, 2017.

surveillance of online communication to this organ whose independence is not guaranteed would undermine the right to data privacy.

5.2.1.6. Absence of Effective Remedy and User Notification

Under international human rights law, the principles of user-notification and transparency are best understood not only under the right to privacy but also as part of the right to an effective remedy and fair trial.[304] User notification and transparency serve different interests: the former is concerned with the provision of sufficient information about a surveillance decision to enable the affected individual to effectively challenge it or seek remedies; the latter is aimed at ensuring that the general public has sufficient information to assess whether the laws governing surveillance are working effectively, including whether there are sufficient safeguards for an individual's right to privacy.

It is fundamental to any effective system of justice that where there is a right, there must be a remedy (*ubi jus ibiremedium*). Unfortunately, the proclamation doesn't provide for user notification in the context of data protection. The very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. There is the need for notification at the earliest possible opportunity unless the notification would seriously jeopardize the purpose for the surveillance or an imminent risk of danger to human life. But, the proclamation is silent on this point.

5.2.2. Preservation of Evidence

Article 30 (1) of the proclamation allows the investigatory authority to order a person to preserve specified computer data in that person's possession or control for up to three months and to keep such an order confidential. This provision lacks involvement of neutral organ that oversight the process. Two reasons are forwarded in the explanatory note of the proclamation

[304] See ICCPR supra Article 14 (1).

for following such trend:[305] First, due to the volatile nature of computer data, preservation orders must be given as quickly as possible without waiting the time-taking legal process. Secondly, the preservation order does not compel the disclosure of any computer data, and thus there are no privacy concerns.

The thorough scrutiny of human rights law, however, makes clear that the collection and retention of communications data amounts to an interference with the right to privacy,[306] whether or not the data is subsequently accessed or used by government officials. This position was supported by European Court of Human Rights. In S and Marper v. United Kingdom, for instance, the Grand Chamber of the ECHR held that "the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private interest of an individual concerned, irrespective of whether subsequent use is made of the data."[307]

Article 30 (1) provides the following cumulative requirements for an investigatory organ to exercise the power of a preservation order: the computer data must be necessary for cybercrime investigation, the computer data to be preserved must be for a specific case or computer data must be specified and the investigatory authority must have reasonable grounds to believe that specific data is vulnerable to loss or modification. It can be argued that these requirements are limitations on the investigatory authority and thereby play a balancing role between individual privacy and investigative powers.[308] But, pragmatically, this doesn't hold water because, for one thing, unlike other jurisdictions,[309] the proclamation doesn't put commencement of criminal prosecution as a pre-requisite, hence, the investigative organ may pass such order at any time. For another thing, there are much researches which show that if digital data is deleted

[305] Explanatory Note of Computer Crime Proclamation, page 40.
[306] See UNHC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, by David Kaye (2015).
[307] ECHR, S and Marper v. United Kingdom Applications nos. 30562/04 and 30566/04 (2008) at para 121.
[308] Halefom *supra* at 22.
[309] Alin Teodorus, *Procedural Aspects of Cybercrime Investigation*, 16 Journal of Legal Studies 55, 58 (2015).

by the user, it does not mean that the data is securely removed from the storage media[310] unless the information has been removed as a result of right to be forgotten.[311]

Furthermore, there is a major problem of preserving ones' privacy in Ethiopia because there is lack of knowledge and understanding as most of Ethiopians are newbies to technology.[312] Most of Ethiopian internet users do not know the technicalities of how networks and data storage are being managed, and their rights in their personal and private information being used by organizations. In view of the above facts, the target of ordering preservation of computer that intrudes into privacy of subjects of the data has to be scrutinized by independent organ. There should be *prima facia* evidence that necessitates such order that should be evaluated by court. Therefore, warrant is important to delve in to such order.

5.2.3. Production order

Article 31 of the proclamation provides how to order a person to submit the preserved computer data which is in that person's possession or control. Unlike the preservation order, this order requires the disclosure of data and is therefore more privacy sensitive. Therefore, this order is should be subjected to judicial warrant. Under this Article, the investigatory authority should prove that the data to be produced should reasonably wanted for the purposes of a computer crime investigation therefore, it want to get access to the data. The court may/may not order that access depending on the reason the investigative authority presents against such data. But, practically, Ethiopian courts couldn't show their independence from the executive branch of the government.[313] However, the proclamation rightly requires the investigator to obtain judicial warrant to produce a computer data as evidence.

---

[310] FrankY.W et al, *Protecting Digital Data Privacy in Computer Forensic Examination*, The 6th International Workshop on Systematic Approaches to Digital Forensic Engineering in conjunction with IEEE Security and Privacy Symposium (IEEE/SADFE 2011) 2 (2011).
[311] M. M. Vijfvinkel, *Technology and the Right to be Forgotten*, Master's Thesis Computing Science Radboud University Nijmegen (July, 2016 *unpublished*).
[312] Kinfe & Halefom *supra* at 130.
[313] The World Bank, *Ethiopia; Legal and Judicial Sector Assessment*, 21 (2004). See also Assefa Fiseha, *Some Reflections on the Role of the Judiciary in Ethiopia*, 3 Ethiopian Bar Review, 105, 110-11, (2009).

5.2.4. Computer Access, Search and Seizure

Article 32 of the cybercrime proclamation entrusts the investigatory authority with specific power to search or access computer systems, networks, and computer data or computer-data storage media. This investigative power refers to both physical and virtual search or access and is subject to prior judicial warrant. Critically speaking, to warrant computer search and seizure there should be probable cause to believe that the data to be seized exists, is evidence of a crime, and is presently located at the place to be searched and a reasonably detailed description of the place to be searched and the data to be seized. [314]

However, existence of intermingled personal information in a computer data creates a problem in computer search and seizure that would affect right to privacy unless properly regulated. Since it is not possible to physically separate information stored on a computer disk, searches of computers will almost inevitably involve the seizure of irrelevant information along with the relevant information. The important question to be asked to while framing the law that regulate computer search and seizer is: if the computer contains information subject to lawful search and seizure which is intermingled with other information that is not evidence of any crime, should the police be required to do any initial sorting to determine what files are within the scope of the warrant or simply go randomly looking through any and all files they may encounter?

The Computer Crime Proclamation tries to answers this question under its article 32(3) (a). But, there is apparent contradiction between the Amharic and English versions of the proclamation. The English version provides: *In the execution of search under Sub article (1) or (2) of this Article* (Article 32*), the investigatory organ may seize any computer system or computer data*. This version of the proclamation permits blanket seizure of computer and computer system without any on-site sorting for evidence relevant to the crime under investigation. But, the Amharic version of this Sub article provides different approach. It provides: *መርማሪ አካል በዚህ አንቀጽ ንኡስ አንቀጽ* (1) *እና* (2) *መሰረት የብርበራ ሥራውን ሲያከናውን* **ከወንጀሉ ጋር ግንኙነት ያለውን** *ማንኛውም የኮምፒዩተር ሥርዓት ወይም ዳታ መያዝ ይችላል (In the execution of search under sub article (1) or (2) of this Article* (Article 32*), the investigatory organ*

[314] Carmen *supra* at 266.

may seize any computer system or computer data ***that has connection with the crime****).* This provision allows seizure of a computer system or computer data that is only connected to the alleged crime. It is obvious that the Amharic version of the proclamation is binding in this case. But, this doesn't fully address the concern of privacy in the search and seizure. Let assume that certain personal computer is reasonably suspected to be connected with certain alleged computer crime. The investigator can, by obtaining warrant, seize the computer hardware according to Article 32 (3) (a) of the proclamation. According to the proclamation, after the seizure, the investigator is free under search every data in that computer. However, computers contain a large quantity and variety of information and the investigator must be warned to conduct searches carefully to prevent unwarranted intrusions in privacy.[315] The thorough understanding of article 32 of the proclamation shows that the law allows for wholesale seizure and search of the computer system or data that is connected with the alleged crime. This means that both relevant and irrelevant data of the suspected are going to be divulged. This leads to unnecessary intrusion of investigatory organ to one's privacy.

Under this issue, it is noteworthy to state the experience of USA, a country who has been encountering this problem in early 1980s. In 1980s, the country was following a system that allows wholesale seizure and search of computer as computer system was seen as analogy of closed container and it is possible to see in it after obtaining a warrant to defeat security measures.[316] But later, after the land mark case of *United States v. Tamura* in 1988,[317] the position of the US courts changed and they adopted *Tamura* rule which dictates that in cases of intermingled documents (computer data) search of a computer will be conducted according to certain procedures.[318] After seizing a computer or computer system that is connected with the alleged crime up on warrant, First, the police should be required to perform on-site sorting of computer data to isolate relevant from irrelevant possibly highly personal, data if at all possible. Second, if on-site sorting is not possible, the later sorting requires supervision from an independent magistrate and a showing of the practical considerations that prevented the on-site sorting. Thirdly, if the police feel that wholesale seizure of computer equipment

[315] Donald Resseguie, *Computer Searches and Seizure*, 48 Clev. St. L. Rev. 185, 205 (2000).
[316] *Ibid*, at 204.
[317] United States v. Tamura, 694 F.2d 591 (9th Cir. 1982).
[318] Resseguie *supra*.

will be required, approval for this should be obtained in advance at the time of warrant application. Nevertheless, the Computer Crime Proclamation doesn't provide for such procedures and simply ran the wholesale seizure of computers and computer systems. This highly affects right to privacy as the investigatory organ can freely look into every personal data in the seized computer or computer system which are irrelevant to the crime under investigation.

The proclamation also empowers the investigatory organ to extend a search or access to other computer system without requesting a separate search warrant if the computer data sought is stored in another computer system and can be obtained by same computer system.[319] In this case, the investigatory organ is relieved from proving conditions that establish computer search and seizure. This power may be abused. Because, the scope of the warrant may be broadened by the investigatory organ because it wanted to know data within that other computer or computer system. Extension of warrant in this case may create another threat to right to privacy.

Conclusion

Under its provisions that regulate digital forensic, the proclamation takes extreme measures trampling over right to data privacy as there is likelihood that they will be abused to raid the premises of independent media outlets or bloggers that are critical of the government, or political opponents. This problem has been rampant in Ethiopia even before the promulgation of the Computer Crime Proclamation.[320] Article 25 (3) of the proclamation legalizes the sudden searches and seizures without being authorized by a court. This part of the proclamation highly affects right to data privacy as there is: proliferation of collection of personal data in the country, the development of surveillance technologies in the country, lack of transparent interception and surveillance, no provision for sufficient safeguards to protect privacy under the Article, absence of independent organ for oversight, and absence of effective remedy and user notification requirements.

[319] Computer Crime Proclamation *supra*, Article 32 (2).
[320] See Biniam Abate, *Freedom of Expression & Digital Activism for Human Rights: An Evaluation of Online Participatory Politics in the Ethiopian Context*, A Thesis Submitted in Partial Fulfillment for the Requirements of the Degree of Master of Laws (LL.M) in Human Rights Law, Addis Ababa University, (2016 *unpublished*).

Article 30 and 32 of the proclamation provide a more general rule that allows warrantless collection and retention of communications on internet, a wholesale search and seizure of computers and empower the investigatory organ to extend the scope of the warrant provided for access, search and seizure of computer and computer system. These provisions are worrisome because they provide wide discretion for the investigatory organ. They allow the organ to access, search and seizure computer and computer system as it likes once it obtained a warrant. This highly threatens right to data privacy because the fate of individuals' right to privacy remains in the hands of the impartial investigatory organ.

Generally, offensive intrusion tactics that involve hacking into computers or networks by the government and wide discretion of the investigatory organ threaten the right to privacy and procedural fairness rights of Internet users. It may also result in considerable self-censorship of individuals refraining from openly communicating on a variety of topics across the telecom network.

CHAPTER SIX

CONCLUSION AND RECCOMMENDATIONS

6.1. Conclusion

The advent of internet enhanced the protection and exercise of human rights especially, freedom of expression and right to privacy. Nevertheless, Internet has also created various mechanisms for culprits to commit cybercrimes with the complex computer systems that causes huge damage to the persons and country. For this reason, both in the human rights instruments to which Ethiopia is a party and the FDRE Constitution, limitation clauses to human rights in both offline and online cases. Normally, to limit a right, there should be a clear law made by the authoritative organ; the limitation should be sought to protect the identified legitimate interest and be necessary in democratic society (three-part-test). The Computer Crime Proclamation comes up by providing some special provisions, *inter alia*, on content of data, responsibility of internet service providers and special procedural rules for digital forensic that affect the rights by violating the standards to limit the rights.

Basically, there is low Internet access in Ethiopia. The cause of this problem is highly attributable to monopolization of telecom service by the government. Despite the duty of the government to facilitate universal access to information and to make favorable conditions that enable the society to share opinions freely, there is little move by the government to solve this problem from the grassroots level. Rather, in Ethiopia, the laws and policies are designed denying privatization of telecom service. This doesn't hurt only access to internet but also pave the way for the government authorities to control, sometimes, arbitrarily, persons who have got access to the internet.

Secondly, Article 13 of the proclamation which is sought to protect individuals' reputation and liberty provides vague words that can impose a strict self-censorship. Similarly, Article 14 which is aimed to protect the public security on Internet also provides surreptitious phrases that have higher probability to be exploited by government authorities to irritate journalists, bloggers, human rights defenders and the civilians as a whole. This indicates that the

provisions fail to fulfill standard of limitation of freedom of expression which requires clear and reasonable law.

Thirdly, the proclamation has criminalized online defamation. However, given the silencing effects of 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. Beside, international standards on limitation of freedom of expression require that any interference with freedom of expression must meet the three-part-test. But, sanctions of criminal law constitute unnecessary and disproportionate measures on the exercise of freedom of expression with regard to matters of public interest. Therefore, criminalization of defamation cannot be justified under the Constitution and human rights law.

Fourthly, the proclamation makes ISP criminally liable in principal capacity when certain illegal content data is transmitted through their services. Nevertheless, there is international consensus that ISP should not be liable for the content produced and uploaded by their users. Provisions of Article 16 of the proclamation have a capacity to lead to interference of private entities (ISPs) in the privacy of internet users and allow them to block their free speech 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. Generally, except the second statement of article 16 (1) and Article 27 of the proclamation that provide for criminal liability of ISP that directly involved in editing of the illegal content data and imposes duty to report on ISPs respectively, the other provisions of the proclamation that impose criminal liability on ISP are unnecessary.

Fifthly, Article 25 (3) of the proclamation allows warrantless sudden searches that leads to offensive intrusion tactics that involve hacking into individuals' computers or networks by the government. It adopted extreme measures trampling over right to data privacy as there is likelihood when surveillance and interception of communication on Internet may be abused to raid the premises of independent media outlets or bloggers that are critical of the government, or political opponents. The provision may also lead to considerable self-censorship of many individuals fearing that they are under control by the investigatory organ.

Sixthly, Article 30 of the proclamation empowers the investigatory organ to pronounce order without obtaining warrant to this effect for data collection and retention whenever the organ thinks necessary. This may lead to surveillance of individuals' communications without warrant and create the sense of insecurity among internet users. It has the highest potential to lead to unnecessary surveillance and self-censorship that erode the right to data privacy online.

Finally, Article 32 of the proclamation gives wide discretion to the investigatory organ to extend scope of the warrant in computer search and seizure. This may lead to intrusion of one's privacy under the guise of warrant secured for other reasons. Article 32 also lacks necessary safeguards that protect right to privacy of the suspected person during the computer search, especially, in cases where data which is required for investigation is intermingled with the irrelevant private data.

6.2. Recommendations

As it is starkly discussed in this study, the Computer Crime Proclamation has many thorny provisions that limit freedom of expression and right to data privacy without valid justifications. Based on the fact that these two rights are to be respected on the internet, the following measures are recommended.

1. The Ethiopian government should privatize telecom service to realize universal affordable internet access in Ethiopia. The government should release its grip on the sector and hand over it to private entities to boost universal Internet access.
2. The Ethiopian Parliament should amend Article 13 (1) & (2) and Article 14 of the proclamation. The legislature should correct the vague provisions of the Articles that failed short of the requirement of clear stipulations provided by human rights instruments and the Constitution to limit freedom of expression. Until the amendment takes place, the Ethiopian courts should narrowly interpret the Articles because, as the provisions stand now, they beg many subjective meanings and government authorities may take arbitrary measures against individuals under the guise of the provisions. Thus, the courts should decide accusations under the provisions by interpreting the words narrowly.
3. Criminalization of online defamation should be abandoned in Ethiopia for it threatens and negatively affects freedom of expression. In view of that, the legislature should repeal

Article 13(3) of the Computer Crime Proclamation. The legislature gave deaf ear to the loud call of human rights bodies, *inter alia*, resolution of African Commission of Human and Peoples' Rights and decision of the African Court of Human Rights and criminalized online defamation. This deviation is unnecessary and enmeshes online freedom of expression in the country unless online defamation is decriminalized.

4. The legislature should amend Article 16(1) of the proclamation and delete the first statement of the Sub article that makes ISP criminally liable for their mere involvement in dissemination of illegal content data. For those ISPs that have played editing roles in preparation and dissemination of illegal content data, the second statement of the Sub article can effectively regulate.
5. The legislature should repeal Article 16 (2) of the proclamation that affect the right to data privacy by allowing inappropriate organs (ISP) to test the legality of a content data and remove it from computer systems. ISPs, due to their strategic position in communications on Internet, may enter into surveillance of every communication on Internet to discharge their duty and this destroys right to data privacy on Internet. Therefore, there should not be any provision which authorize ISP to remove or dismiss Internet user's data without the consent of the later.
6. The legislature should amend Article 16(3) of the proclamation that empowers administrative authorities to order removal of data content. Because, it goes against separation of power and leads to violation of right to privacy and online freedom of expression. Even, if a court decides illegality of a data, removing one's data without allowing him/her to defend it is against that individual's right to fair hearing. Thus, the provision has to be amended in line with the mechanism of "notice and notice" to facilitate prevention of cybercrime without compromising human rights of Internet users.
7. The legislature should amend Article 25(3) of the proclamation that can lead to arbitrary violation of right to privacy. Although surveillance may not be abandoned as a whole, the following corrections have to be taken to control its effects on right to data privacy.
    a. Reference to "Federal General Attorney" under article 25 (3) should be dropped and replaced by court and surveillance should only be allowed with warrant.
    b. The law should require periodic report on the number of surveillance undertaken to enforce transparency and its consequences.

c. The law should establish the mechanism through which individuals affected by illegal surveillance claim redress and the person who commits it be made accountable.

8. The legislature should amend Article 30 of the proclamation that empowers the investigatory organ to preserve one's data as it wills and require involvement of the court to examine the existence of grounds stated under Article 30 (1) of the proclamation before permitting order of preservation.
9. The legislature should amend Article 32 of the proclamation which gives a wide discretion to the investigatory organ to access, search and seize computers and computer systems and correct it by
   a. providing rules that warn the investigatory organ to protect privacy while investigating the required computer data intermingled with other private data and
   b. denying extension of a warrant by the investigatory organ to further protect the digital right to privacy under any circumstance.

Bibliography

A. Books

1. Andrew T. Kenyon & Megan Richardson, *New Dimensions in Privacy Law*, (2006).
2. Catherine Seville, *EU Intellectual Property Law and Policy*, (2009).
3. Chuck Easttom & Det. Jeff Taylor, *Computer Crime, Investigation, and the Law,* (2011).
4. Diane Rowland & Elizabeth Macdonald, *Information Technology Law* (2nd ed.), (2000).
5. Gercke M, *Understand Cybercrime: A guide for developing countries*, (2011).
6. Ian J. Lloyd, *Information Technology Law* (6th Ed.), (2011).
7. Lorna Stefanick, *Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World*, (2011).
8. Peter Stephenson, *Investigating Computer-related Crime: Handbook for Corporate Investigators*, (2000).
9. Pramod Kr. Singh, *Laws on Cybercrimes*, (2007).
10. Richard Hunter, *World without Secrets*, (2002).
11. Rolando V. del Carmen, *Criminal Procedure Law And Practice*, (7th edit.) (2007).
12. Uchenna Jerome, *Cybersecurity Law and Regulation*, (2012).
13. UNODOC (United Nations Office on Drugs and Crime), *Comprehensive Study on Cybercrime*, (2013).
14. Wojciech Sadurski, *Freedom of Speech and Its Limits*, (1999).

B. Articles in Journal and periodicals

1. Alin Teodorus, *Procedural Aspects of Cybercrime Investigation*, 16 Journal of Legal Studies 55 (2015).
2. Anton Vedder, *Accountability of Internet access and service providers – strict liability entering ethics?* 3 Ethics and Information Technology 67 (2001).
3. Assefa Fiseha, *Some Reflections on the Role of the Judiciary in Ethiopia*, 3 Ethiopian Bar Review, 105 (2009).
4. Asou Aminnezhad et al, *A Survey on Privacy Issues in Digital Forensics*, 1 IJCSDF 311 (2012).
5. Barbara Van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 JT&HTL 329 (2007).
6. Basu, S. & Jones, R.P., *Regulating Cyberstalking*, 2 JILT 1 (2007).
7. Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, I9 IJCC 55 (2015).
8. Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debat*e, 3 JT&HTL 23 (2004).
9. David R. Johnson & David Post, *Law And Borders- The Rise of Law in Cyberspace*, 48 SLR, 1367 (1996).
10. Donald Resseguie, *Computer Searches and Seizure*, 48 Clev . St. L. Rev . 185 (2000).

11. FrankY.W et al, *Protecting Digital Data Privacy in Computer Forensic Examination*, The 6th International Workshop on Systematic Approaches to Digital Forensic Engineering in conjunction with IEEE Security and Privacy Symposium (IEEE/SADFE 2011) 2 (2011).
12. Gary Slapper, *Clarity and the Criminal Law*, 71The Journal of Criminal Law, 475, 477 (2016).
13. Gedion Temothewos, *An Apologetic for Constitutionalism and Fundamental Rights: Freedom of Expression in Ethiopia*: *A Comparative Study*, CEU Collection 122 (2009).
14. Gedion Timothewos, *Freedom of Expression in Ethiopia: The Jurisprudential Dearth*, 4 MLR 201 (2010).
15. George P. Fletcher, *The Theory of Criminal Liability and International Criminal Law*, 10 JICJ 1029 (2012).
16. Hossein Bidgoli, *The Internet Encyclopedia*, California State University Bakersfield, California, 199 (2004).
17. Jasper P. Sluijs, *From Competition to Freedom of Expression: Introducing Article10 ECHR in the European Network Neutrality Debate*, 12 HRLR 509 (2012).
18. Jeremy Stone Weber, *Defining Cyberlibel: A First Amendment Limit for Libel Suits against Individuals Arising from Computer Bulletin Board Speech*, 46 Cas. W. Res. L. Rev. 235 (1995).
19. Kenneth W. Simons, *When is Strict Criminal Liability Just*, 87 J. Crim. L. & Criminology 1075 (1997).
20. Kinfe Mecheal, *Developments in Cybercrime law and Practice in Ethiopia*, 30 Computer Law and Security Review 720 (2014).
21. Kinfe Micheal & Halefom Hailu, *The Internet and Ethiopia's IP Law, Internet Governance and Legal Education: An Overview*, 9MLR 154 (2015).
22. Kinfe Micheal & Alebachew Birhanu, *Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices*, 26 JEL 94 (2013).
23. Kinfe Micheal & Halefom Hailu, *The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media*, 9MLR, 108 (2015).
24. Kinfe Micheal, *Data privacy law and practice in Ethiopia*, 5 International Data Privacy Law, 177 (2015).
25. Kinfe Micheal, *Digital privacy and virtues of multilateral digital constitutionalism—preliminary thoughts*, 00 International Journal of Law and Information Technology, 1 (2017).
26. Kinfe Micheal, *Some Remarks on Ethiopia's New Cybercrime Legislation*, 10 MLR 448 (2016).
27. Lawrence F. Young, *United States Computer Crime Laws, Criminals and Deterrence*, 9 International Review of Law, Computers & Technology, 1 (1995).
28. Lisl Brunner, *The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia*, 16, Human Rights Law Review 163 (2016).

29. Mark Tushnet, New York Times V. Sullivan around the World, 66 Alabama Law Review 337 (2014).
30. 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 No 34*, 12 Human Rights Law Review 627 (2012).
31. Mizanie Abate, *Transnational Corporate Liability for Human Rights Abuses: A Cursory Review of the Ethiopian Legal Framework*, 4 Mekelle University Law Journal 34 (2016).
32. Molalign Asmare, *Computer Crimes in Ethiopia: An Appraisal of the Legal Framework*, 3 ISSN 92 (2015).
33. Molalign Asmare, *Enhanced Forms of Criminal Investigation: Analysis on Its Potential Risks to Human Rights*, 7 Beijing Law Review, 33 (2016).
34. Mooneh, T. *Special Investigation Techniques. Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights*, Pace Int'l L. Rev. Online Companion, 97 (2010).
35. Nils Jareborg, *Criminalization as Last Resort (Ultima Ratio)*, 2 Ohio St. J. Crim. L. 521 (2005).
36. Peter Grabosky, *Requirements of prosecution services to deal with cybercrime*, 47 Crime Law Soc. Change 201 (2007).
37. Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 criminology 101 (1988).
38. Robert E. Litan & Hal J. Singer, *Unintended Consequences of Net Neutrality Regulation* 5 Journal on Telecommunications and High Technology Law 533 (2007).
39. Samuel D. Warren & Louis D. Brandeis, *The right to privacy*, 4 Harvard Law Review 2303 (1890).
40. Sanette Nel, *Defamation on the Internet and other computer networks*, 30The Comparative and International Law Journal of Southern Africa, 154 (1997).
41. Stephen Tully, *A Human Right to Access the Internet? Problems and Prospects*, 14 Human Rights Law Review, 175, (2014).
42. 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).
43. Ter Kah Leng, *Internet defamation and the online intermediary*, 31 computer law & security review 68 (2015).
44. Thomas Welch, *Computer Crime Investigation and Computer Forensics*, 6 Information Systems Security 56 (1997).
45. Toon Moonen, *Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights*, 9 Peace Int' l L. Rev. Online Companion, 97 (2010).

46. 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).
47. Xavier Amadei, *Standards of Liability for Internet Service Providers: A Comparative Study of France and the United States with a Specific Focus on Copyright, Defamation, and Illicit Content,* 35 Cornell International Law Journal 1 (2002).
48. Yinghua Guo & Jill Slay, *Computer Forensic Functions Testing: Media Preparation, Write Protection and Verification,* 5 Journal of Digital Forensics, Security and Law 1, (2010).

C. Dissertations and Working Papers

1. Biniam Abate, *Freedom of Expression & Digital Activism for Human Rights: An Evaluation of Online Participatory Politics in the Ethiopian Context,* A Thesis Submitted in Partial Fulfillment for the Requirements of the Degree of Master of Laws (LL.M) in Human Rights Law, Addis Ababa University, (2016 *unpublished*).
2. C. Hangey, *Deep Packet Inspection and Your Online Privacy: Constitutional Concerns and the Shortcomings of Federal Statutory Protection*, University of San Francisco School of Law Working Paper Series, (2008) available at http://bit.ly/19cLkGp accessed on May 1, 2017.
3. Fisaha Getachew, *The Respect For Human Rights In Pre-Trial Criminal Investigation (The Case of Oromia Special Zone Surrounding Finfine),* A Thesis Submitted to Addis Ababa University, School of Graduate Studies in Partial Fulfilment of the Requirement of the Degree of Masters in Human Rights, 14 (2015) (*unpublished*).
4. Gagliardone, I. et al. *MECHACHAL: Online debates and elections in Ethiopia. From hate speech to engagement in social media* 16 (2016).
5. 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 For Partial Fulfillment of the Requirements for the Degree of Master of Arts in Journalism and Communication (2013) *(unpublished).*
6. Hou, S; Uehara *et al, Privacy preserving confidential forensic investigation for shared or remote servers,* The 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2011), Dalian, China, 14-16 October 2011. Available at http://hdl.handle.net/10722/152021
7. International Telecommunication Union, *Internet from the Horn of Africa: Ethiopia Case Study*, 11 (2002).
8. Ministry of Communication and Information Technology Federal Democratic Republic of Ethiopia, 1 Communication and Information Technology Statistical Bulletin (2014).
9. Minyahel Desta, *Liberalization of telecommunication in Ethiopia challenges and prospects: citizens' view and opinion*, Research paper submitted to trade policy training center in Africa (trapca) for the 2012 annual conference (unpublished) 18 (2012).
10. Shimelis Hailu, *Ethiopian Anti-Terrorism Law and Human Rights Nexus: An Appraisal*, A Thesis Submitted to the School of Graduate Studies of Addis Ababa University 39 (2014) (*Unpublished*).
11. The World Bank, *Ethiopia; Legal and Judicial Sector Assessment,* (2004).

D. Internet Sources

1. Bradley Mitchell, *ISP - Internet Service Providers*, October 17, 2016 available at https://www.lifewire.com/internet-service-providers-817781 accessed on May 11, 2017.
2. Donovan, K. and Martin, A., *The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change*. 21, (2014). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820 accessed on May 11, 2017.
3. Ezana Sehay *How Social Media Is Despoiling Civility In Ethiopia*, available at http://www.ethiocyberlaws.com/ accessed on May 11, 2017.
4. Freedom House (2015) available at https://www.justice.gov/eoir/page/file/917171/download accessed on May 11, 2017.
5. Freedom House (2016) available at https://www.justice.gov/eoir/page/file/916611/download accessed on April 6, 2017.
6. Halefom Hailu, *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.
7. http://allafrica.com/stories/201604261343.html Accessed on January 9, 2017.
8. http://drpeering.net/core/ch2-Transit.html accessed on March 28, 2017.
9. http://searchmicroservices.techtarget.com/definition/IAP-Internet-access-provider accessed on March 27, 2017.
10. http://searchsecurity.techtarget.com/definition/cyberstalking accessed on March 22, 2017.
11. http://www.bbc.com/news/world-africa-36763572 accessed on April 5, 2017.
12. http://www.entertainmentmedialawsignal.com/online-infringement-canadian-notice-and-notice-vs-us-notice-and-takedown accessed on March 27, 2017.
13. http://www.ethioconstruction.net/?q=news/telecoms-slow-down-development-ethiopian-tech-scene-%E2%80%93-iceaddis accessed on April 4, 2017.
14. http://www.internetlivestats.com/internet-users/ accessed on December 21, 2016.
15. http://www.internetworldstats.com/africa.htm accessed on April 19, 2017.
16. http://www.knowyourmobile.com/apps/facebook/21807/history-facebook-all-major-updates-changes-2004-2016 accessed on March 21, 2017.
17. http://www.livinginternet.com/i/ii_arpanet.htm accessed on January 2, 2017.
18. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx accessed on April 18, 2017.
19. http://www.reuters.com/article/us-ethiopia-economy-insight idUSKBN0LC0C320150208 accessed on April 3, 2017.
20. http://www.un.org/apps/news/story.asp?NewsID=55022#.WN0vDmdlDIW accessed on April 5, 2017.
21. https://motherboard.vice.com/en_us/article/the-fight-to-uncover-spyware-exports-to-repressive-regimes accessed on May 4, 2017.
22. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595096&download=yes accessed on March 21, 2017.

23. https://www.article19.org/resources.php/resource/38429/en/unhrc:-significant-resolution-reaffirming-human-rights-online-adopted accessed on February 24, 2017.
24. https://www.coursehero.com/file/p2fomsb/Computer-Crimes-The-term-computer-crime-refers-broadly-to-any-wrongful-act-that/ accessed on January 2, 2017.
25. https://www.rctlj.org/2012/10/anti-cyberstalking-laws-misuse-and-the-first-amendment-right-to-free-speech/ accessed on March 22, 2017.
26. Leo Mirani, *Millions of Facebook Users Have No Idea They're Using the Internet*, accessed April 4, 2017, available at http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet accessed on May 11, 2017.
27. Morgan Marquis-Boire et al, *You Only Click Twice: FinFisher's Global Proliferation*, Citizen Lab, Research Brief No. 15, March 2013, available at https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2 accessed on May 4, 2017.
28. Paul Budde Communication Pty Ltd. *Ethiopia – Telecoms, Mobile, Broadband and Forecasts*, June 2014, http://bit.ly/1ji15Rn accessed on May 11, 2017.
29. 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/ accessed on May 11, 2017.
30. Staff Reporter, *Establishing the Attorney-General: Reconstructing the Justice System or Heralding a New One?* Written on 26 Nov, 2015. Available at http://www.thereporterethiopia.com/content/establishing-attorney-general-reconstructing-justice-system-or-heralding-new-one accessed on May 3, 2017
31. 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.

E. Hard Laws

1. African [Banjul] Charter on Human and Peoples' Rights, adopted June 27, 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force Oct. 21, 1986.
2. African Union Convention on Cyber Security and Personal Data Protection, Adopted by the 23rd Ordinary Session of the Assembly of the Union, Malabo, 27th June 2014.
3. Anti-Terrorism Proclamation, Federal *Negarit Gazeta*, Proclamation No. 652/2009.
4. Charities and Societies Proclamation, Federal *Negarit Gazeta*, Proclamation No.621/2009.
5. Civil Code of The Empire of Ethiopia, Federal *Negarit Gazeta*, Proclamation No. 165/J960.
6. Computer Crime Proclamation, Federal *Negarit Gazeta*, Proclamation No. 958/2016.
7. Constitution of the Federal Democratic Republic of Ethiopia, Federal Negarit Gazeta, Proclamation No. 1/1995.
8. Convention on Cybercrime, European Treaty Series - No. 185, Budapest, 23.XI.2001.
9. Covenant on Civil and Political Rights, adopted by the UN General Assembly in Resolution 2200 A (XXI) of 16 December 1966 at New York, entered into force on 23 March 1976.
10. Criminal Procedure Code, *Negarit Gazeta*, Proclamation No. 185/1961. Article 32 and 33
11. Federal Attorney General Establishment Proclamation, Federal *Negarit Gazeta*, Proclamation No. 943/2016.

12. Freedom of Mass Media and Access to Information Proclamation, Federal *Negarit Gazeta* Proclamation No.590/2008.
13. Investment proclamation, Federal *Negarit Gazeta*, Proclamation No. 769/2012 Article 6 (2) (b).
14. Ministry of Communications and Information Technology, *License Directive for Resale and Telecenter in Telecommunication Services Directive*, Directive No. 1/2002.
15. Registration of Vital Events and National Identity Card Proclamation, Federal *Negarit Gazeta*, Proclamation No. 760/2012.
16. Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation, Federal *Negarit Gazeta*, Proclamation No. 434/2005
17. Telecom Fraud Offense Proclamation, Federal *Negarit Gazeta* Proclamation No. 671/2012.
18. The Criminal Code of Federal Democratic Republic of Ethiopia, Proclamation No. 414/2004.

F. Policy Instruments

1. National Information security Policy of The Federal Democratic Republic of Ethiopia, September 2011.
2. The Federal Democratic Republic Of Ethiopia, The National Information And Communication Technology Policy And Strategy, Aug, 2009.
3. The Federal Democratic Republic of Ethiopian Criminal Justice Administration Policy, Ministry of Justice, (2011).

G. Soft Laws

1. ACHPR, *Declaration of Principles on Freedom of Expression in Africa*, 32nd Session, Banjul, Gambia, (2002).
2. ACHPR, *Resolution on Repealing Criminal Defamation Laws in Africa*, Res169 (XLVIII) (2010)
3. American Association for the International Commission of Jurists, *Sira cusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, (1985).
4. Council of Europe, *Recommendation 10 of the Committee of Ministers to Member States on "Special Investigative Techniques" in Relation to Serious Crimes Including Acts of Terrorism*, (2005).
5. Council of European Union, *EU Human Rights Guidelines on Freedom of Expression Online and Offline*, Brussels, (2014).
6. Manila Principles on Intermediary Liability, *Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation*, (2015).
7. The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR)

Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration On Freedom Of Expression And The Internet*, (2011).
8. UNESCO, *Human rights and encryption*, 9 (2016).
9. UNGA, The Right to Privacy in the Digital Age, GA Res 68/167 (2013).
10. UNGA, The Right to Privacy in the Digital Age, GA Res 69/166 (2014).
11. UNGA, The Right to Privacy in the Digital Age, UN Doc A/C.3/71/L.39/Rev.1 (2016).
12. UNHRC, *Concluding observations on Ethiopia*, 102nd session Geneva, (2011).
13. UNHRC, *General Comment 16: Art 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation'*, (1988).
14. UNHRC, *General comment No. 34 Article 19: Freedoms of opinion and expression*, 102nd session Geneva, (2011).
15. UNHRC, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, A/HRC/32/L.20, 27 (2016).
16. UNHRC, *Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, U.N. Doc. A/HRC/13/37, (2009)
17. 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).
18. UNHRC, Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, U.N. Doc. A/HRC/13/37, (2009).
19. UNHRC, *Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Special Rapporteur Abid Hussain, E/CN 4/2002/75, (2002).
20. UNHC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, by David Kaye (2015).
21. UNHRC, *Right to Privacy in the Digital Age*, Human Rights Council Res 28/16 (2015).
22. UNHRC, *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/20/L.13. (2012).

H. Jurisprudences/Case Laws/

1. ACHPR, *Civil Liberties Organization and Media Rights Agenda v. Nigeria*, Comm Nos. 140/94, 141/94, 145/95 (1999).
2. ACHPR, *Lohé Issa Konaté v. The Republic of Burkina Faso*, App. No. 004/2013, (2014).
3. ECHR, *Kruslin v France* Application No. 11801/85 (1990).
4. ECHR, *S and Marper v. United Kingdom*, Applications nos. 30562/04 and 30566/04 (2008).
5. U. S. Supreme Court, *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).
6. U.S. Court of Appeals for the District of Columbia Circuit, *Doe v. Federal Democratic Republic of Ethiopia*, Case No. 16-7081, (2017).
7. UNHRC, *Coleman v. Australia*, Communication No. 1157/2003, (2006).
8. UNHRC, *Concluding Observations of the Human Rights Committee on Poland*, (1999).

9. UNHRC, *concluding observations on the United Kingdom of Great Britain and Northern Ireland*, (CCPR/C/GBR/CO/6), (2008).
10. UNHRC, *Fernando v. Sri Lanka*, Communication No. 1189/2003, (2005).
11. UNHRC, *Keun-Tae Kim v. The Republic of Korea*, Communication No. 574/1994, CCPR/C/64/D/574/1994, (1999).
12. UNHRC, *Mavlonov and Sa'di v. Uzbekistan,* Communication No. 1334/2004, (2009).
13. UNHRC, *Ross v. Canada*, Communication No. 736/97, (2000).
14. UNHRC, *Shin v. Republic of Korea*, Communication No. 926/2000, (2004).
15. UNHRC, *Velichkin v. Belarus*, Communication No. 1022/2001, (2005).