Privacy and Personal Data **Protection in Ethiopia**

September 2018

CIPESA

Table of Contents

Privacy and Personal Data Protection in Ethiopia
Berhan Taye and Roman Teshome

Executive Summary

Ethiopia is currently undergoing political reforms under the leadership of Prime minister Abiy Ahmed who came into power in April 2018. Some of the reforms undertaken include among others, freeing thousands of political prisoners, lifting bans on social media outlets, unblocking 250 websites, privatising some government monopolised sections, embarked on revision and annulment of several repressive laws. Previous regimes has been criticised for its repressive laws and other measures that stifle fundamental human rights including the right to privacy.

This report presents finding from the study on the state of data protection and Privacy in Ethiopia. The study adopted a qualitative approach that included analysis and review of relevant literature on data and privacy issues including the legal and the policy framework in Ethiopia. The research reviewed reports of previous studies, media reports, academic works, government documents, and other literature. To assess the extent to which existing legal and policy frameworks support data protection and privacy in Ethiopia, the study further involved studying of local laws and policies on privacy and personal data protection.

Findings from the report reveal that privacy is a legal and practical concept that has not fully been conceptualised in Ethiopia. Despite the provision of privacy protection in the constitution and several subsidiary laws, the existence of similar laws limit the right to privacy. Findings further indicate that several Ethiopians have little regard to personal privacy or its protection. This has a lot to do with the social, economic and political state of the country. Findings also indicate that social and cultural factors coupled with the lack of awareness about privacy protection contribute to the poor state of data protection and privacy in Ethiopia. This is worsened with the massive collection of personal data by both government organs and non-governmental actors without adequate legal, regulatory and policy frameworks.

The report draws recommendations to government, private institutions and civil society organisations. It calls upon government to among others; enact a comprehensive data protection and privacy law that sufficiently defines the duties of data controllers and processors and the rights of data subjects; ensure that the data protection law development process is consultative, transparent, and participatory, involving all concerned actors including data subjects and the private sector; review and redraft all legislations that infringe on the right to privacy to ensure they adequately protect all citizens including the Anti-Terrorism Proclamation, Computer Crime Proclamation, the Anti-Corruption Proclamation and others. Private institutions are encouraged to adopt data protection guidelines, policies and regulations that spell out the terms and conditions for the users of their services and build capacity of their officers in data protection and privacy compliance. Other entities are encouraged to advocate for data protection and privacy protection through creating awareness about the need to respect this right.

1 Introduction

Privacy is a legal and practical concept that has not fully been conceptualised in Ethiopia. Some scholars contend that Ethiopian society is not concerned with privacy or its protection. They attribute this to the social, economic and political realities of the country.[1] Yilma argues that "demarcating one's private sphere has a lot to do with one's economic capacity." [2] Further, that the increase in economic freedom and independence leads to increase in the quest for privacy. Hence, the lack of financial ability and poverty are among the main factors behind the diminished concern for privacy and personal data protection in Ethiopia.

The social and cultural factors, particularly the communal life of the Ethiopian society, coupled with the lack awareness about privacy protection, contribute to the poor state of data protection and privacy in the country. Further, the dominance of authoritarian and totalitarian regimes, which had little regard for privacy and other human rights, throughout the country's political history and the infant democratic practice account for the current state of affairs in data protection and privacy.[3] However, with the advent of electronic media and smartphones in the country, the concern for privacy and personal data protection has gained momentum in recent years.[4]

Like most African countries, Ethiopia faces contemporary challenges that threaten data protection and privacy. One of these threats is the collection of a large amount of personal data by government organs, without adequate legal, regulatory and policy frameworks.[5] For instance, the Registration of Vital Events and National Identity Card Proclamation allows the collection of personal data and the transfer of this data to various institutions including intelligence authorities without the consent of the data subjects.[6] This law authorises the storage of sensitive data in the 'central database' without regulatory safeguards.[7] Similarly, Ethio-Telecom, the sole telecommunication service provider in Ethiopia, requires a lot of personal information to register SIM cards. For instance, a customer is required to provide a name, address, a relative's phone number, a photo ID, a photograph, and a signature before an individual can buy a SIM card.[8] Moreover, several respondents in the study indicated that with as little as 1,000 birr ($35), one could access private call records of Ethio-Telecom's customers. Undoubtedly, this unregulated personal data collection and use of personal data has an impact on privacy protection in Ethiopia.

In addition to amassing personal data, the government including law enforcement agencies, continue to use surveillance technologies without the appropriate regulatory mechanisms, thus posing a threat to privacy and data protection.[9] Moreover, the lack of transparency and procedural guarantees of access to information, including

1 *Kinfe Micheal Yilma, Data privacy law and practice in Ethiopia, International Data Privacy Law, 2015, Vol. 5, No. 3, p.177; see also Alebachew Birhanu Enyew, Towards Data Protection Law in Ethiopia, in Alex B. Makulilo (ed.), African Data Privacy Laws, 2016, p.147.*
2 *Yilma, supra note 1, p.178*
3 *Ibid, p.178 & 179; see also Enyew, supra note, p.148.*
4 *Ibid, p.179.*
5 *Ibid, p.183.*
6 *Proclamation No.760/2012, Article 63(1)*
7 *Ibid, Article 57(2).*
8 *Ethiopia government in mobile phone registration drive to curb smuggling, fraud, available at https://aptantech.com/2017/09/ethiopia-government-in-mobile-phone-registration-drive-to-curb-smuggling-fraud/ last accessed 24 July 2018.*
9 *Yilma, supra note 1, p.183.*

personal information of individuals, escalates the situation and makes it prone to abuse.[10] For instance, in 2011, Ethio-Telecom introduced Deep Packet Inspection (DPI),[11] a technology that allows internet service providers to monitor internet traffic of users. Despite the initial plan for the commercial use of DPI technology, it was abused to track personal communication.[12]

Ethio-Telecom's customer information system uses ZSmart, a privacy-invasive technology that combines surveillance and customer management. According to the Human Rights Watch, ZSmart was installed in 2009 by the Chinese telecom company ZTE and is used to manage all customer information and automatically records and updates personal information, such as location, SMS texts and all calls made using Ethio-telecom networks.[13] The same report also identified another privacy-invasive technology used by Ethio-telecom, ZXMT. The technology was also installed by ZTE in 2009, and it is capable of monitoring internet traffic and intercepting web browsing, and other similar communications.[14]

Furthermore, some reports have detailed how the Ethiopian Government has used intrusive technologies to surveil political opposition, journalists, and bloggers. According to a report published by Citizen Lab in 2013, the Ethiopian government injected malware on to the pictures of prominent opposition members and tricked users to download the images with malware.[15] In another report released the following year, Citizen Lab also stated that the Ethiopian government used an intrusive spyware, Remote Control System (RCS), to steal files and passwords, intercept Skype calls and instant messages of the Ethiopian Satellite Television (ESAT), a critical and independent media station operated by some Ethiopians living in the diaspora.[16] In February 2014, a similar allegation was raised in a lawsuit against the Ethiopian government by the Electronic Frontier Foundation (EFF) on behalf of an American citizen of Ethiopian origin before the US Federal District Court in the District of Columbia. The applicants claimed infringement of privacy through the use of FinSpy spyware technology.[17] In the same year, another related complaint emerged in the UK which alleged that the Ethiopian government used the same technique to intrude electronic communications of an Ethiopian political refugee in the UK.[18]

Over the past decade, the Ethiopian government has procured and deployed numerous surveillance and intrusive technologies in Ethiopia. Whether in the name of customer management or national security, these technologies have instilled fear and paranoia in many people. The deployment of these pervasive tools continues unchallenged due to the lack of robust data and privacy protection laws, proliferation of laws that disregard privacy, and the absence of judicial and legislative oversight to provide the appropriate checks and balances.

10 *Ibid.*
11 *R Sandvik, 'Ethiopia Introduces Deep Packet Inspection' (2012) Tor Project Blog, available at https://blog.torproject.org/ethiopia-introduces-deep-packet-inspection last accessed 24 July 2018.*
12 *Yilma, supra note 1, p.183.*
13 *Human Rights Watch, "They know everything we do": Telecom and Internet Surveillance in Ethiopia, 2014, available at https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia, accessed 25 July 2018, p. 36 & 37.*
14 *Ibid, p.62.*
15 *By Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, 'You Only Click Twice: FinFisher's Global Proliferation', March 13, 2013, The Citizen Lab Research Brief, available at https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/, accessed 25 July 2018, p.7-9.*
16 *Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, 'Hacking Team and the Targeting of Ethiopian Journalists', February 12, 2014, Citizen Lab Research Brief, available at https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/, accessed 25 July 2018, p. 1–12; see also Bill Marczak, John Scott-Railton, and Sarah McKune, 'Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware, March 9, 2015, available at https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/, accessed 24 July 2018.*
17 *Electronic Frontier Foundation, Kidane v. Ethiopia available at https://www.eff.org/cases/kidane-v-ethiopia, accessed 24 July 2018.*
18 *Privacy International Seeking Investigation into Computer Spying on Refugee in UK, Press Release, 17 February 2014, https://ecadforum.com/2014/02/19/ethiopian-refugee-illegally-spied-on-using-british-software/, last accessed 24 July 2018..*

2 Methodology

The study adopted a qualitative approach that included analysis and review of relevant literature on data and privacy issues including the legal and the policy framework. The research reviewed reports of previous studies, media reports, academic works, government documents, and other literature. The analysis also involved studying of local laws and policies on privacy and personal data protection. This was important for assessing the extent to which the existing legal and policy framework supports or protects the enjoyment of the right to privacy.

Key informant interviews with purposively selected respondents were also conducted. Purposively selected respondents were drawn from staff of private companies, government ministries, semi-autonomous bodies, telecoms regulators, media houses, social media users, human rights defenders and activists, consumers' associations, academics, lawyers, and select individuals from the general public who were conversant with the issues at hand.

3 Country context

3.1 Political Economy

The Ethiopia population is estimated to stand at 107 million people. This is the second largest population in Africa after Nigeria. More than 80% of the population lives in rural areas.[19] The country has a Gross Domestic Product (GDP) per Capita (PPP) of USD 1,899 according to the World Bank.[20] It ranks at a low position of 173 out of 189 countries, under the United Nations Development Programme (UNDP) Human Development Indicator.[21]

3.2 ICT Status

Ethiopia has the lowest percentage of internet penetration in Africa. According to the International Telecommunication Union (ITU), only 15.4% of Ethiopians have access to the internet. Further, there are 0.5 fixed (wired) broadband subscribers per 100 inhabitants and only 7.2% mobile broadband subscribers.[22] The country has one of the most expensive broadband internet services in the world.[23] The cost of 1-megabyte speed unlimited broadband subscription was approximately USD 40 per month which is quite expensive compared to average income. However, on August 22, 2018, Ethio-Telecom announced a discount on its services, reducing the cost of broadband internet by 54%.[24]

Most internet users in the country access the internet from their mobile phones, whose use has considerably increased in recent years. Statistics from ITU indicate that Ethiopia has 59.7 mobile-cellular subscriptions per 100 persons,[25] which is a significant increase compared to 23.7 subscriptions per 100 individuals in 2014.[26] However, mobile data subscription remains expensive, and this was particularly before the significant discount announced last August. The cost of 500-megabyte mobile data bundle was around USD 3; but after August 22, 2018, this decreased by 43%.[27]

19 *Ethiopia Population 2018 http://worldpopulationreview.com/countries/ethiopia-population/*
20 *GDP per capita, PPP (current international $), World Bank https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?locations=ET*
21 *Human Development Indices and Indicators: 2018 Statistical Update http://hdr.undp.org/sites/all/themes/hdr_theme/country-notes/ETH.pdf*
22 *Data from ITU's Ethiopia country profile available at https://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx accessed 27 July 2018.*
23 *Human Rights Watch report, supra note 13, p.22.*
24 *Tariff Discount http://www.ethiotelecom.et/tariff-discount/*
25 *ITU data, supra note 20.*
27 *Human Rights Watch report, supra note 13, p.22.*
28 *Tariff Discount http://www.ethiotelecom.et/tariff-discount/*

Ethio-Telecom, a state-owned telecommunication company, is the sole provider of telecommunication services in Ethiopia. It has also been responsible for implementing a number of internet shutdowns in the country. According to Shutdown Tracker Optimization Project, Ethiopia in 2018, shut down the internet at least three times.[28] In June 2018, the new government announced its decision to privatise Ethio-Telecom in two years and to allow other telecommunication service providers to operate in Ethiopia.[29]

3.3 Political Environment

The Ethiopian People's Revolutionary Democratic Front (EPRDF), the ruling regime since 1991, adopted an ethnic-based federalism. This party, which has ruled the country for more than 27 years, has severally been criticised for its repressive laws and other restrictive measures that stifle political opposition and curtail fundamental freedoms. The government has extensively restricted freedom of expression, freedom of association, and the right to privacy and other principal rights, particularly since the controversial 2005 election.[30]

However, following the change of leadership, the country has since April 2018 been going through commendable political reforms under the leadership of the new Prime Minister Abiy Ahmed. Since then, the new Prime Minister has freed thousands of political prisoners,[31] lifted bans on some media outlets, unblocked more than 250 websites,[32] decided to privatise some government monopolised sectors, and made peace with neighbour Eritrea.[33] The new administration has also commenced the revision and potential annulment of some of the repressive laws in the country. Nevertheless, the overall result of this reform and its implication to the democratic space in the country is yet to be fully seen.

28 *Berhan Taye, Old habits die hard: Ethiopia blocks internet in the eastern part of the country, again! Available at https://www.accessnow.org/ethiopia-blocks-internet-in-eastern-part-of-country-again/, last accessed 07 September 2018*
29 *Aaron Maasho, Ethiopia opens up telecoms, airline to private, foreign investors, available at https://www.reuters.com/article/us-ethiopia-privatisation/ethiopia-opens-up-telecoms-airline-to-private-foreign-investors-idUSKCN1J12JJ, last accessed 25 July 2018.*
30 *Human Rights Watch Report, supra note 13, p.12.*
31 *Aljazeera, Ethiopia to free thousands of Oromo Political Detainees, available at https://www.aljazeera.com/news/2018/01/ethiopia-free-thousands-oromo-political-detainees-180127111131976.html, last accessed 07 September 2018*
32 *Berhan Taye, Ethiopia: Verifying the unblocking of Websites. Available at https://www.accessnow.org/ethiopia-verifying-the-unblocking-of-websites, last accessed 07 September 2018*
33 *Jason Burke, 'These changes are unprecedented': how Abiy is upending Ethiopian politics, the Guardian, * July 2018, available at https://www.theguardian.com/world/2018/jul/08/abiy-ahmed-upending-ethiopian-politics, accessed 24 August 2018.*

4. Laws and Policies Affecting Privacy and Personal Data Protection

Ethiopia does not have a comprehensive data protection and privacy law. However, the constitution and various laws mention privacy or data protection

4.1 International Human Rights Instruments

Ethiopia has ratified a number of international and regional human rights instruments that provide for the right to privacy. These include the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), Convention on the Rights of the Child (CRC), and the African Charter on the Rights and Welfare of the Child. According to Article 9 of the Ethiopian constitution, these and other human rights instruments ratified by Ethiopia form an 'integral part' of the laws of the country.[34]

Furthermore, the constitution declares that the interpretation of fundamental rights and freedoms enshrined in the constitution shall conform to the human rights instruments the country has ratified.[35] In other words, whenever there is an ambiguity, or the specifics are not clear, human rights instruments shall inform the interpretation of the human rights provisions in the constitution.

Similarly, the privacy guarantees enshrined in the constitution should be interpreted in accordance with international and regional human rights instruments Ethiopia is a party to. The United Nations Human Rights Council resolution passed in 2016 stresses that "the same rights that people have offline must be protected online" especially as it relates to the protection of the freedom of expression as indicated in the UDHR and the ICCPR, both of which Ethiopia has ratified.[36]

4.2 The Constitution of the Federal Democratic Republic of Ethiopia

The 1995 Ethiopian Constitution introduced a range of privacy safeguards, which were informed by the privacy provisions found in international human rights instruments to which Ethiopia is party. Under article 26 of the constitution, the right to privacy includes a guarantee not to be subjected to search of one's home, person and property and to the seizure of any personal property. More importantly, the same article also provides that:[37] "Everyone has the right to inviolability of his notes and correspondence including postal letters, and communications made using a telephone, telecommunications, and electronic devices."[38] This provision protects personal data in the digital space since it extends privacy protection to all electronic communications. Therefore, privacy rights guaranteed offline are also protected online.

34 *Ibid, article 9 (4).*
35 *Ibid, article 13(2).*
36 *Independent, UN Declares Online Freedom to be a Human Rights that Must be Protected, available at https://www.independent.co.uk/life-style/gadgets-and-tech/un-declares-online-freedom-to-be-a-human-right-that-must-be-protected-a7120186.html, last accessed 07 September 2018*
37 *Constitution of the Federal Democratic Republic of Ethiopia, 21 August 1995, article 26 (1).*
38 *Ibid, article 26 (2).*

However, the right to privacy is not absolute as it can be limited to protect other competing interests provided in subsidiary laws if the necessary conditions are met. Under article 26(3), there are three grounds upon which the right to privacy can be restricted. Firstly, there needs to be a compelling circumstance that necessitates the encroachment on privacy rights. Secondly, the proposed restrictions must be explicitly provided in a specific law; and thirdly, the limitation must be imposed to protect specific legitimate interests that are specifically enumerated in the constitution, such as national security or the public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others.[39]

4.3 Recognition of Privacy and Personal Data Protection in Statutes

Apart from the constitution and the human rights treaties the country has ratified, there are also some subsidiary laws that provide for privacy rights and data protection in Ethiopia.

4.3.1 Civil Code of Ethiopia

Some of the provisions of Section 2 of the Ethiopian Civil Code are dedicated to the protection of privacy under the theme of 'rights of personality'. The privacy related rights recognised under this general theme include a right not to be subjected to search except in cases provided by law, and inviolability of domicile.[40] Article 11 on the restriction on freedom and search provides that, "No persons may have his freedom restricted, or be subjected to a search, except in the cases provided by law." Further, article 13 on inviolability of domicile, provides that:

(i) The domicile of a physical person is inviolable;
(ii) No one may enter the domicile of another against the will of such persons, neither may a search be effected therein, except in the cases provided by law.

These guarantees are also reiterated in the constitution, as described above, and in the criminal procedure code.

4.3.2 Freedom of Mass Media and Access to Information Proclamation

The Freedom of the Mass Media and Access to Information Proclamation enacted in 2008, has some guarantees that directly or indirectly protect privacy and personal data. It particularly seeks to find a balance between access to information and privacy protection. However, although the proclamation guarantees the right of all persons to seek and access any information held by public bodies, it also enumerates exceptions that restrict this right.[41] One of these exceptions is aimed at protecting personal information. Public agencies are required to reject requests to access records, if the concerned records relate to personal information of third parties, including a deceased individual who has passed away for less than 20 years.[42]

39 *Ibid, article 26 (3).*
40 *Civil Code of Ethiopia, Proclamation No. 165 OF 1960, Article 11 & 13.*
41 *Freedom of the Mass Media and Access to Information Proclamation, Proclamation No. 590/2008 of 2008, 4 December 2008, article 12. https://chilot.me/2011/11/freedom-of-the-mass-media-and-access-to-information-proclamation-no-5902008/*
42 *Ibid, article 16.*

Moreover, the proclamation defines personal information by providing an open-ended (exemplary) list of information regarded as private, which include:[43]

> (a) information relating to the medical or educational or the academic, employment, professional or criminal history, of the individual or information relating to financial transactions in which the individual has been involved;
> (b) information relating to the ethnic, national or social origin, age, pregnancy, marital status, colour, sexual orientation, physical or mental health, wellbeing, disability, religion, belief, conscience, culture, language or birth of the individual;
> (c) information relating to any identifying number, symbol or other particular assigned to the individual, the address, fingerprints or blood type of the individual;
> (d) the personal opinions, views or preferences of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
> (e) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual;
> (f) the views or opinions of another individual; or
> (h) the name of the individuals where it appears with other personal information relating to the individual or where the disclosing of the name itself would reveal information about the individual;

Thus, the proclamation protects these and other personal information and access to public records in such cases depending on other related factors. In addition, commercial information like trade secrets and other business related information are exempted from disclosure if they could potentially harm the financial interests of the person concerned.[44] Apart from these, a request for access to public records can be rejected if it relates to confidential information of a third party or if it would potentially prejudice the supply of similar information in the future when public interest demands so.[45] On the other hand, the Proclamation further protects personal data by incorporating a notification and intervention procedure. According to article 19 of the Proclamation, a third party whose information is requested for disclosure will be notified of such request and given an opportunity to protest against the disclosure of the information requested.[46] However, the law is silent on whether such a person will be notified of the request for disclosure if the request is lodged by a government entity.

Despite the Proclamation embodying commendable safeguards for privacy and data protection, it is not without limitation. One of the shortcomings of the proclamation is that it gives discretion to public bodies to disclose personal information through informal channels. Article 19 of the law provides that "nothing in this proclamation shall be understood as limiting the power of public bodies to provide access to information on an informal basis." [47] This backdoor access can threaten the protection of personal data, and it can be easily abused.[48] It is common practice in Ethiopia to access personal information of other people through payment of bribes or at the discretion of the concerned authority.

43 *Ibid, article 2(8).*
44 *Ibid, article 17.*
45 *Ibid, article 18.*
46 *Ibid, article 19.*
47 *Ibid, article 19.*
48 *Kinfe Micheal Yilma, Sources of Ethiopian Privacy Law, 20 July 2015, available at http://www.abyssinialaw.com/blog-posts/item/1544-sources-of-ethiopian-privacy-law, accessed 23 July 2018.*

The lack of a centralised organ within government to deal with access to information requests, the lack of awareness within government agencies, and the lack of policy guidelines for the implementation of this proclamation are major challenges to the full implementation of this law.

4.3.3 Registration of Vital Events and National Identification Cards Proclamation

Pursuant to article 64 of this Proclamation, information obtained in relation to vital events and national identification cards may be disclosed to other organs for specified purposes. These purposes include national intelligence and security, crime prevention and investigation, tax collection, administrative and social services, implementation of financial risk management and other purposes promulgated by law.[49] This is an open-ended list, which leaves room for authorities to disclose information for a range of reasons provided in other laws as well.

Under article 64(2), an organ that obtains information through these disclosure procedures is not at liberty to disclose the information to other organs or third parties.[50] However, the law does not stipulate any sanction for failure to comply with this rule. Further, article 64(3) stipulates that information specific to an individual may not be disclosed to any other person unless the authority has obtained the consent of the concerned individual or has been ordered to disclose the information by a competent court.[51] Moreover, even if the person has consented to the disclosure of the information, it may not be dispensed with if it harms the public interest.[52]

4.3.4 Income Tax Proclamation

The Income Tax Proclamation has specific provisions that spell out the duty of confidentiality. According to article 39(1) of the Proclamation, the tax authority is obliged not to disclose the tax information of a third party without the written consent of the person or organisation concerned. However, article 39(1(b)) also provides an exception in as far as it requires the authority to disclose such confidential information to law enforcement agencies in prosecution of tax related offences. Further, article 39(1(c)) provides that courts may request the authority to gain access to confidential information for other crimes as well and the latter is obliged to comply.[53]

4.3.5 Electronic Signature Proclamation

The Electronic Signature Proclamation, enacted in 2018, aims to promote electronic commerce and electronic government services and provides some form of protection of users' data. Specifically, article 4 provides for privacy protection of digital signatures while article 2 provides for use of encryption in the management of digital signatures.

49 *Registration of Vital Events and National Identity Card Proclamation, Proclamation No.760/2012, article 64 (1). Available at: https://chilot.me/wp-content/uploads/2017/04/proclamation-no-902-2015-registration-of-vital-events-and-national-identity-card.pdf*
50 *Ibid, article 64 (2).*
51 *Ibid, article 64 (3).*
52 *Ibid, article 64 (5).*
53 *Income Tax Proclamation, Proclamation No. 286/2002, Article 39. Available at: http://www.erca.gov.et/images/Documents/Proclamation/Income_tax/55.pdf*

Article 29(2) provides some safeguards for users' personal data and bars data collectors from disclosing personal data anyhow, stating that; "unless otherwise clearly expressed, each certificate provider shall keep personal information confidential." [54]

4.3.6 Criminal Code

Articles 604 to 606 of the Criminal Code are also relevant for the protection of privacy and personal data. These provisions criminalise the violation of privacy safeguards guaranteed in the constitution, such as violation of privacy of domicile or restricted area and violation of privacy of correspondence. The latter violation includes intrusion of one's letter, telegram, telephone, and other electronic correspondence, among others.[55]

4.3.7 The Criminal Procedure Code

The Criminal Procedure Code also has provisions that indirectly protect privacy. For instance, article 32 provides that no person or premises shall be searched without a court warrant except for some narrow exceptions. Moreover, the code enumerates circumstances under which a search warrant can be issued and stipulates the conditions of search and seizure.[56] The law requires that search warrants specify the properties to be searched and seized, but it does not have a specific provision about electronic materials.

4.4 Laws that Limit or Threaten Protection of Privacy and Personal Data in Ethiopia

Although the constitution and subsidiary laws have provisions on privacy and data protection, there are various legislation that threaten the enjoyment of the right to privacy in Ethiopia. They are explored below.

The 2009 Anti-Terrorism Proclamation

Article 22 of the law obliges institutions that collect personal data, such as banks, tax authorities, and medical institutions, to disclose such information whenever it is needed for investigation of terrorism cases. Moreover, the provision gives broad discretion to the police to make such requests, if law enforcement agencies "reasonably" believe that such disclosure is essential in the investigation process without any judicial oversight.[57] As Yilma rightly contended, "the danger is that such discretion is likely to be misused in practice, since orders for disclosure are not mandated to be made by an independent judicial tribunal." [58] The proclamation has other highly problematic provisions. One such example is article 16, which authorises the police to conduct "sudden search and seizures" only with the permission of the Director General of the Federal Police.[59] Given its provisions, the proclamation has been used to target the political opposition, journalists and bloggers.

54 *Electronic Signature Proclamation No. 1072/2018, Article 29. Available at: http://www.flslegalservices.com/wp-content/uploads/2018/12/1072-2018-electronic-signature-law.pdf*
55 *The Criminal Code of the Federal Democratic Republic of Ethiopia 2004, Proclamation No.414/2004, article 604-606.*
56 *The Criminal Procedure Code of Ethiopia, Proclamation No. 185 of 1961, article 32 & 33.*
57 *Anti-Terrorism Proclamation, Federal Negarit Gazeta, Proclamation No. 652/2009, article 22. Available at: https://chilot.me/2011/01/a-proclamation-on-anti-terrorism-proclamation-no-6522009/*
58 *Yilma, supra note 1, p.185.*
59 *Anti-Terrorism Proclamation, supra note 49, article 16.*

The 2005 Corruption Crimes Proclamation

This law limits the right to privacy by introducing special rules of investigation. Article 46, for instance, permits the interception of correspondences and letters without judicial warrant. This can be done with only the authorisation of the Commissioner of the Anti-Corruption Commission.[60]

The 2013 National Intelligence and Security Service Re-establishment Proclamation

The Proclamation re-established the National Intelligence and Security Service (NISS) with a ministerial status as an autonomous federal government office. In article 27, it requires everyone including the major stakeholders, such as Ethio-Telecom, tax authorities and health institutions, to cooperate with NISS by providing information.[61] It is worth noting that whereas the law requires the NISS to obtain court warrants for surveillance and data interception, it does not require NISS to obtain court warrants to seek information from third-party data collectors. This lack of judicial oversight puts the protection of privacy and personal data in danger.[62]

The 2012 Telecom Fraud Offense Proclamation

Under Article 14, the law authorises the police to conduct secret surveillance upon a court order whenever they have "reasonably' suspected that telecom fraud has been committed or is likely to be committed.[63]

The 2016 Computer Crimes Proclamation

This law incorporates various provisions that threaten the protection of human rights. Under Article 24, service providers/data collectors are required to retain all computer data passing through its systems for at least one year and must disclose this on the order of a court or a public prosecutor. Specifically, Article 24 (2) states that; "data shall be kept in secret unless the court orders for its disclosure".

Article 25 provides that police and prosecutors may, by warrant of a court, intercept communications if this is deemed and when damage to critical infrastructure may occur as a result of computer crime, surveillance may be authorized by the President of the Federal High Court, on the recommendation of a minister, instead of a court.

Specifically, Article 25(3) states that; "Notwithstanding the provisions of subarticle (1) and (2) of this Article, the Attorney General may give permission to the investigatory organ to conduct interception or surveillance without court 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."

This deficit in judicial oversight and the very subjective wording of the law could pose challenges to the realisation of the right to privacy.

60 *Revised Anti-corruption Special Procedure and Rules of Evidence Proclamation, Federal Negarit Gazeta, Proclamation No. 434/2005, Article 46. Available at: https://chilot.files.wordpress.com/2017/04/proclamation-no-881-2015-corruption-crimes-proclamation.pdf*

61 *National Intelligence and Security Service Re-establishment Proclamation, Proclamation No. 804/2013, article 27; see also Yilma, supra note, p.187. Available at: http://library.stic.et/documents/30479/594148/Proclamation-no-804-2013-A+proclamation+to+re-establish+the+National+Intelligece+and+Security+Service.pdf/bf0f9a77-8181-43a7-9b87-997c8ec77243?version=1.0*

62 *Yilma, supra note 1, p.187.*

63 *Telecom Fraud Offense Proclamation, Federal Negarit Gazeta, Proclamation No. 761/2012, Article 14. Available at: https://chilot.me/2012/12/proclamation-no-7612012-telecom-fraud-offence-proclamation/*

The draft Data Protection Proclamation

The Ministry of Communication and Information Technology (MCIT) prepared a draft data protection Proclamation in 2009 and revised it in 2010. The draft was never adopted, although the Ministry is once again, preparing a new draft, whose future remains unknown.

> *"personal data" means data which relate to a living individual who can be identified: i. from those data, or ii. from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual"*[64]

This definition is broad and extends the scope of personal data to any information that can relate to an identified person. Further, the draft lists certain personal information as "sensitive personal data". This category of personal data includes information on racial or ethnic origin, political opinion, religious beliefs, membership to a trade union, physical and mental health condition, sexual life, genetic information, commission or alleged commission of a crime and legal proceeding against the subject.[65] The draft thus provides relatively heightened protection for sensitive personal data.

The draft further lists the following eight principles of data protection to govern the collection and processing of personal data.[66] These principles are regarded as the basic minimum to protect fundamental rights.[67]

i. Fairness: personal data should be obtained and processed fairly, which dictates that the data subject must be clearly informed of the purpose of data collection and processing.
ii. Purpose limitation: personal data can only be collected for certain specified lawful purposes and should only be processed in a manner that is compatible with those purposes.
iii. Data minimisation: the personal data sought to be collected must be "adequate, relevant and not excessive" in relation to the purposes they are collected and processed for.
iv. Accuracy: personal data shall be accurate or up-to-date.
v. Retention limitation: personal data should not be kept no longer than it is necessary for the purpose it is collected for.
vi. Rights of data subjects: personal data should only be processed by giving due regard to the rights of data subjects, which are provided in the proclamation.
vii. Data security: appropriate measures should be taken to protect personal data from unauthorised access and accidental loss or destruction.
viii. Interstate transfer of data: personal data should not transferred to a country where there is no adequate safeguards of data protection.

64 *The Draft Ethiopian Data Protection Proclamation, April 2010, part 1, Article 1(1)(F).*
65 *The draft proclamation, supra note 58, part 1, Article 2.*
66 *Ibid, schedule 1, part 1. (According to the draft proclamation, 'data processing' includes organization and alteration of the data; use of the information or data; disclosure, transmission and dissemination of the data; and alignment, combination, blocking, erasure or destruction of the information. The term 'data processing' used throughout this section also denotes this broader definition.)*
67 *Access Now; Creating A Data Protection Framework: A Do's And Don'ts Guide For Lawmakers, available at https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf; last accessed September 08 2108*

The draft also provides under article 7 for the rights of data subjects in relation to data processing. Accordingly, the data subject has a right to request information when their data is being processed and the purpose for the processing, and the data controller is obliged to comply.[68] Moreover, it provides for certain conditions that should be complied with before processing personal data, which include the consent of the data subject and the necessity of data processing to meet certain legitimate interests provided by law.[69]

Moreover, the draft stipulates stringent conditions for the processing of "sensitive private data" (defined above). In such cases, the consent of the data subject must be explicit and the legitimate interests provided thereof are more restrictive. In the latter case, the consent of the data subject must be explicit and the legitimate aims provided herein are also relatively limited.[70] A data subject is also entitled to request the data controller not to begin, or to cease a data processing if it is likely to cause a substantial and unwarranted damage or distress to the data subject or to another person.[71] Furthermore, a court is empowered to undertake rectification, blocking, erasure and destruction of data that is proved to be inaccurate upon application by the data subject.[72]

Despite its commendable safeguards for the right to privacy, the draft also has some shortcomings. Firstly, it stipulates certain grounds where the collection and processing of personal data can be exempted from regulation under the data protection principles and rules enshrined in it. These grounds include national security; crime and taxation; health, education and social work; regulatory activities; journalism, literature and art; research, history and statistics; and information available to the public and when disclosure is required by law or for legal proceeding.[73] These grounds can be used as an exception to limit the application of the principles of data protection and rules on personal data processing.

Secondly, a number of its provisions are vague and generally inadequate and outdated, given the recent developments on data protection. A significant part of the text is borrowed largely from the UK Data Protection Act of 1998, which was recently revised, without sufficient contextualisation.[74] Moreover, the draft does not adequately address the data protection threats that have emerged with new technological advancements and globalisation which have significantly increased the scale of collection and sharing of personal data. For instance, in its definition of sensitive data that ought to be protected, it fails to include biometric data, whose collection is rampant in the country; fails to take into account online identifiers and location data to be personal data or identifiers; and does not incorporate concepts like profiling or other issues that have arisen in the advent of information technology.

68 *The draft proclamation, supra note 58, part 2, article 7.*
69 *Ibid, schedule 1, part 1, schedule 2.*
70 *Ibid, schedule 1, part 1, schedule 3.*
71 *Ibid, part 2, article 10.*
72 *Ibid, part 2 article 14.*
73 *Ibid, part 4, article 27-38.*
74 *UK Data Protection Act, available at: https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted*

Further, the draft does not provide special protection to children or minors. The draft envisages the establishment of a government organ to oversee the implementation of data protection without clearly stipulating the powers and duties of the organ or its institutional framework. A similar shortcoming is evident with the proposed Data Protection Tribunal, which is set to be established without a proper structure and adequate rules.[75] The draft also fails to provide robust enforcement mechanisms, such as complaint procedures and effective sanctions.

In addition, some of the rules provided in the draft are not adequately defined and elucidated. For instance, the manner in which consent is given prior to data processing, transparency requirements, and the conditions of data subjects' right to erase and rectify inaccurate personal information are not properly defined. Similarly, information that should be provided to the data subject before the collection, access and sharing of personal data, are not adequately addressed by the draft.

Last but not least, the draft does not adequately regulate information sharing between public and private bodies, as it only provides for a general framework of data processing. Another shortcoming relates to data security and integrity, by not requiring data protection by design and by default by companies to ensure users' information is protected by embracing data protection principles both in their technology and organisational policy.[76] The draft also lacks detailed rules on data breach prevention, remedial procedures when a breach occurs, and notification of victims of data breaches. Furthermore, the exemption provisions, which limit the application of data protection rules and principles, are broadly defined. This allows data processing without adequate safeguards for data protection in numerous circumstances, which opens the door to possible abuse.

75 *Ibid, part 1, article 6.*
76 *AccessNow, Creating a Data Protection Framework: a Do's and Don'ts Guide for Law Makers,available at https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf, accessed 13 August 2018, p.10.*

5. Results

5.1 General Overview

In Ethiopia, the public's awareness of privacy and data protection is limited. Some scholars have suggested that large sections of the society are not vigilant or sensitive about data protection issues because of economic, social and political factors. The research demonstrates that most people do not question the necessity and process of collection and handling of their sensitive private data. The term privacy does not have an equivalent terminology in most local languages including Amharic which suggests that the concept is not a daily concern for many Ethiopians. In Amharic, the closest term to privacy is 'Ye Gil Hiwote Ye'Mekeberna Yemetebeke Mebit', which means "the respect and protection of personal life."

This lack of awareness and concern is not limited to the public, but also extends to the government and private institutions who are key stakeholders in data protection and privacy. The low level of awareness is also evident among academics and legal professionals, as only very few have written works on privacy and data protection. One of the government officials interviewed working in this sector stated that "the main focus here is on using the technology rather than the privacy issues associated with it."

Furthermore, governmental and non-governmental organisations are not creating awareness about data protection. The exceptions are the TV and radio shows run by the Information Network Security Agency (INSA), which covers various cyber security and technology issues. It is important to note here that INSA, until very recently, was the leading perpetrator of surveillance and privacy breaches in the country.[77]

The use of targeted and indiscriminate communication, particularly unsolicited bulk SMS, is very much prevalent in Ethiopia, and has significantly increased in recent years.[78] For example, Ethio-Telecom regularly sends out unsolicited promotional SMS texts from itself or from the organisations (both public and private) it has partnered with.[79] Specifically, the number of bulk SMS marketing calling for lottery draws or demanding to offer information in return for a certain fee are on the increase. Many customers are discontent about these unsolicited communications and some have even tried to stop receiving SMS from some sources, to no avail. The common procedure to stop receiving the SMS marketing from private entities is to send an SMS saying "stop", but some of the providers continue sending the bulk SMS despite being stopped. Some customers have also called Ethio-Telecom and complained about the practice, to which the telecom corporation subsequently warned certain private entities that use bulk SMS marketing for misusing the system.

77 *The Register, Hacking Team mulled stopping Ethiopia sales – because of idiot g-men https://www.theregister.co.uk/2015/08/17/hacking_team_ethiopia/*
78 *Hawi Abdisa, Addis Fortune, Bulk Short Message Service Business Thrives. 05 August, 2017, Available at https://addisfortune.net/articles/bulk-short-message-service-business-thrives/ last accessed 08 September 2018*
79 *Getachew T. Alemu, Ethio Telecom's Faulty Choice Theory, 12 April 2012, available at https://addisfortune.net/columns/ethio-telecoms-faulty-choice-theory/, accessed 14 August 2018.*

5.2 Governmental and Nongovernmental Organizations that Collect Data

There are a number of government and private entities that collect and process data, with the state owned telecom company, Ethio-Telecom, being one of the largest data processors. Ethio-Telecom implements a mandatory SIM-card registration system where users are obliged to register with their names, photo ID, signature, relatives' phone numbers, and addresses in order to obtain SIM-cards. Thus, users are required to show an identification card, allow the telecom to keep a scanned copy of the card, and take their photo in order to get the service.

Since 2017 Ethio-Telecom has been registering mobile phone devices in order to prevent illegal smuggling of new devices and unwarranted use of the network. The telecom monopoly uses the national Equipment Identity Registration System (EIRS), which enables it to automatically register every device that uses a SIM-card from Ethio-Telecom. An Ethio-Telecom official said the system was expected to match each mobile device with the SIM card of the particular user using IMEI, a unique number given automatically to identify GSM, WCDMA, and iDEN mobile phones, as well as some satellite phones.[80] On August 22, 2018, the telecom operator announced that it had stopped device registration.[81] There is still concern regarding the management of data collected so far. Ethio-Telecom also has the metadata of communications undertaken through its network. Moreover, the Corporation utilizes technologies installed by the Chinese company, ZTE, that enables it to automatically store all SMS and other related communications as well as record all phone calls made using its network on demand.[82]

The other big government organs that collect personal information are the Vital Events Registration Agency and City Administration offices.[83] These bodies collect for the purpose of registration especially when vital events, such as birth, marriage and death, occur. For instance, in case of a marriage the law requires the collection of the couples' full names, dates and places of birth, principal residences, citizenship, ethnic origins and religion to be registered.[84] The vital events legal provision does not require couples to provide their fingerprints to get a marriage licence, however, in practice the fingerprints of the couples are also taken.

Similarly, Kebele administration offices, the smallest administrative units in Ethiopia, also collect personal information for the purpose of providing National Identity Cards. The data collected for this purpose includes full name, address, occupation, parents' full name and citizenship, sex, marital status, ethnic origin, photograph, fingerprint and other necessary information determined by the concerned organ.[85] Most of this information is also displayed in the identity card itself. In practice, most Kebele administrations do not collect fingerprint for national identification, despite the law providing for the same under article 57 of the national identification proclamation.

80 *Aptantech, Ethiopia government in mobile phone registration drive to curb smuggling, fraud, September 26, 2017. available at https://aptantech.com/2017/09/ethiopia-government-in-mobile-phone-registration-drive-to-curb-smuggling-fraud/, accessed 16 August 2017.*

81 *Ethio Telecom, the state monopoly, announces abandoning of mobile phone apparatus registration and cutting of service fees for internet and mobile users by about half https://newbusinessethiopia.com/ethiopia-abandons-mobile-apparatus-registration-cut-service-rate/*

82 *Human Rights Watch Report, supra note 13, p. 36 & 37.*

83 *Vital Events Registration Agency http://www.vera.gov.et/Home/EnglishIndex*

84 *Vital Events and National ID Registration Proclamation, supra note 6, article 30.*

85 *Ibid, article 57(2).*

In August 2018, the Addis Ababa City Administration decided to launch biometric identification cards that residents could use for all administrative purposes. The city administration is expected to start collecting fingerprints, in addition to other personal information required. Once the city administration rolls out the biometric ID cards, residents of Addis Ababa will receive services from the city government using their fingerprints as a verification method.

Additional government organs that collect personal data include tax authorities, ministry of education, immigration and nationality affairs, and the police. Public and private health institutions, schools and entities that provide related services also collect and process vast amounts of data. Some of these entities, such as education institutions, immigration and nationality affairs and health facilities, collect data regarding children, but most require the parent to accompany the child and give consent on behalf the child. For instance, the immigration and nationality affairs office collects biometric data including fingerprints and photos both from adults and children. In case of children, the parent consents to the collection of the data, at least impliedly, and signs the required documents on behalf of the child. The same practice is also implemented in schools where registration is conducted with the consent of parents.

Apart from these, there are also various private institutions and businesses that collect and process personal data. The most common are the e-commerce firms that operate in the country which collect a lot of personal information. For instance, Deliver Addis,[86] a company that provides food delivery service in the capital Addis Ababa, collects names, emails and phone numbers of the users. Furthermore, their system also accesses the location data, IP address of the customers. Ride,[87] an online taxi hailing service, is also another good example, which uses a mobile application and phone lines to provide taxi services. Similarly, it collects names, emails, phone numbers, and location data of its users.

5.3 Challenges to Privacy and Data Protection in Ethiopia

Privacy and personal data protection in Ethiopia is grappling with a number of legal and practical challenges. The following are some of the major threats to privacy and data protection this study identified.

5.3.1 Lack of Adequate Legal and Policy Frameworks

As discussed in the preceding sections, Ethiopia does not have a comprehensive data protection and privacy law that fully defines the obligations of data controllers and processors as well as the rights of data subjects. Even though provisions that can be used to this effect can be found in the rather fragmented legal framework, these legislations are still not adequate nor are they up to date to deal with the emerging technological advancements and privacy concerns in modern times. This state of affairs has greatly contributed to the wanton and unregulated data collection and processing prevalent in both public and private institutions. This is further exacerbated by the lack of policy frameworks on the privacy and data protection. Moreover, the existing and somewhat progressive legal instruments such as the Mass Media and Access to Information Proclamation for example, are not supported by policy frameworks to guide and facilitate their implementation. Moreover, most of the government institutions and private organizations that collect and process personal data do not have data protection policies in place.

86 *Deliver Addis https://deliveraddis.com/*
87 *Ride http://ride8294.com/*

5.3.2 Lack of Institutional Machinery

The lack of an institutional framework to provide oversight on the collection and processing of data by public and private bodies is a significant challenge for Ethiopia. Currently, this mandate is partly undertaken by the Ministry of Communication and Information Technology (MCIT), which has taken the initiative to draft a data protection law. Nevertheless, the Ministry neither has a full mandate nor the required expertise to undertake this task. Key informants from within the Ministry expressed concerns that the Ministry of Science and Technology (MST) and Information Network Security Agency (INSA) needed to do more on this issue. Hence, an independent institution with extensive mandate on data protection and regulation of the concerned stakeholders would be essential.

Further, it is worth noting that private entities that control and process data, particularly in the ICT sector, are growing in number in recent years. However, their policies and practices on data protection are not subject to any oversight by the government or any of its agencies. The Ministry of Communication and Information Technology, which is partly mandated to undertake this regulation, has a very minimal contact with the private sector.

5.3.3 Unregulated Collection and Sharing of Sensitive Private Data

A large number of public and private bodies collect sensitive private data without implementing adequate transparency safeguards. Local government bodies obtain such data without informing the data subjects of the purpose of collection the manner of storage and processing of such data. Almost all of these public and private entities do not adequately inform a user the type of data collected and the purpose it will be used for. Due to the low levels of awareness and limited concern for privacy, users do not usually question or contest such practice. Also, it is hardly possible to assume consent when sufficient information has not been provided.

The government website ethiopia.gov.et informs users of the kind of data it collects and claims to protect that data using Ethiopia's privacy and security act yet Ethiopia doesn't have any of those acts.

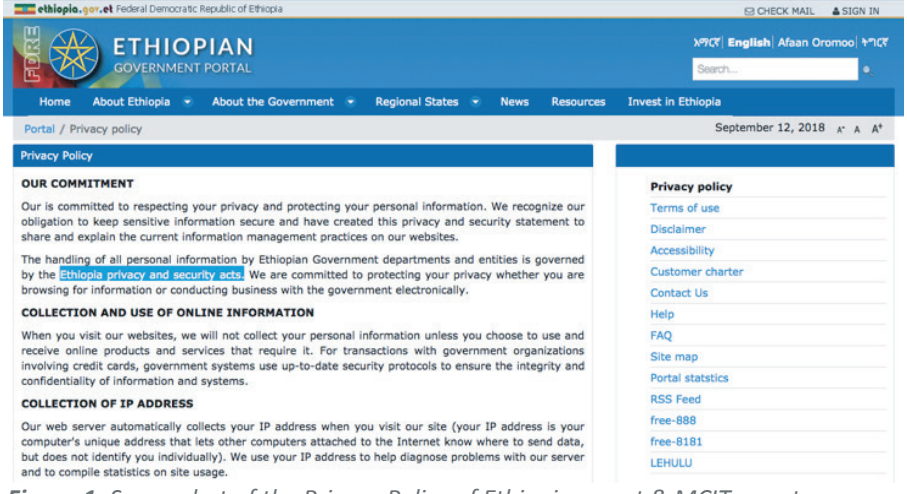

Figure 1. *Screenshot of the Privacy Policy of Ethiopia.gov.et & MCIT.gov.et*

The same level of reckless practice is also witnessed in the private sector where businesses continue to collect personal data without putting in place terms and conditions of use. In the wake of the increasing penetration of e-commerce companies that provide various services, poor data management practices are quite alarming as that risks are high.

It is difficult to say that users have given 'informed consent' when sufficient information to enable them to do so has not been provided. In addition, most of these organizations do not have privacy policies and proper terms and agreements in place, nor do they disclose who they share users' data with. Hence, they collect and process data without adequate legal and institutional protection safeguards.

The same level of insensitivity can also be witnessed in data sharing practices among government and private entities. Laws that establish government institutions, such as intelligence agencies, law enforcement organs and tax authorities among others, contain provisions on sharing of information between government entities as well as the private sector. However, these laws are usually drafted in a generic manner and with broad terms with little regard to the right to privacy.

Furthermore, data collectors sometimes go beyond what is provided for in the few scattered pieces of legislation provisions. For instance, the Vital Events Registration Proclamation mandates the relevant agency to collect personal data when vital events take place. However, in case of marriage the agency collects the fingerprints of the newlyweds, which is not explicitly provided for in the law. Although these types of practices are quite prevalent, there is the landmark case of Riyan Miftah vs. Elsewdi Kebels Plc, where the cassation court ruled that "no image or photograph of a person may be publicly exhibited, sold or disseminated without the consent of the person."[88] The lack of similar complaints and lawsuits can be attributed to the low level of awareness on the issue, including among journalists.

5.3.4 The Lack of Transparency in the Legislative Drafting Process

The drafting process undertaken by MCIT is far as inclusivity and transparency are concerned falls short. The public, civil society organizations, academics, and other concerned non-governmental bodies have not been involved in the drafting process. In order to develop a robust data protection law that safeguards users' rights, the drafting processes needs to be transparent, participatory, and consultative. A number of respondents in this study indicated that they had not been consulted in the drafting process of the data protection draft proclamation and neither were they aware of its existence.

5.3.5 The Risks Associated with Privatization

The Ethiopian government in June 2018, announced plans to privatize certain sectors that had been fully monopolized by the government, including Ethio-Telecom, whose process of privatisation is still underway.[89] Although privatisation can potentially offer immense economic advantages, the privacy risks associated with it cannot be overlooked. This is especially so when there are no adequate legal and institutional frameworks in place. In the Telecom sector for example, companies such as MTN and Vodafone, are already showing interest to enter the Ethiopian market. Opening up the market for these and other companies before putting in place the necessary legal and institutional frameworks could present significant risks to the right to privacy. Moreover, given that the government has decided to sell part of its holding in Ethio-Telecom, the fate of data belonging to the customers of Ethio-Telecom especially in terms of risk of abuse and misuse remains unclear.

88 *Kinfe Michael, Sources of Ethiopian Privacy Laws, available at https://www.abyssinialaw.com/component/k2/item/1544 last accessed 19 June 2018,*
89 *Ethiopia to Privatise a Section of Ethiopian Airlines & Ethio Telecom https://kenyanwallstreet.com/ethiopia-to-privatise-a-section-of-ethiopian-airlines-ethio-telecom/*

5.4 Progressive Steps in Privacy and Data Protection

Currently, the most significant progressive steps towards data protection and privacy in Ethiopia are some minimal provisions in The 2016 Computer Crimes Proclamation and the drafting of the data protection proclamation by the Ministry of Communication and Information Technology. If the shortcomings of the draft protection proclamation are reviewed and revised to respond to the contemporary issues of privacy, it will play a considerable role on improving the existing data protection practice.

Currently, there are not many cases relating to personal data and privacy violations However, there is an important case of *Riyan Miftah vs. Elsewdi Kebels Plc* adjudicated at the Cassation Division of the Federal Supreme Court, whose decisions are binding on lower courts. In this case, an individual successfully defended his right to privacy. The decision of the Court affirmed that a photograph of a person should not be publicly exhibited, sold or disseminated without the consent of the subject individual. A person whose right has been violated in relation to this is entitled to get appropriate damages.[90]

Apart from these positive steps, the initiatives and movements in the area of private data protection and privacy both by public and private bodies are very limited. The minimal involvement of civil society and the media due the stringent media and civil society laws in this regard is further discouraging. However, as a part of the political reforms that are being undertaken in the country, it is expected that these laws will be amended and thereby, provide additional opportunities for positive progressive intervention.

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

6. Conclusion and Recommendations

6.1 Conclusions

Data protection and privacy are not new concepts in Ethiopia's legal framework. The constitution and several subsidiary laws protect both the traditional and the modern conceptions of privacy both offline and online. However, there are similar laws that limit the right to privacy. Laws like the Anti-Terrorism Proclamation, Computer Crime law, and the Anti-Corruption law among others pose threats to the enjoyment of the right to privacy in Ethiopia. These laws were designed to give law enforcement agencies undue power to quell dissenting voices. Consequentially, these laws have been used by authorities to gain unlawful access to the correspondence, communication, and personal lives of Ethiopians. This situation is further exacerbated by the lack of adequate legal, policy and institutional frameworks to protect privacy and personal data in Ethiopia. Many of the privacy protecting provisions are fragmented into different legislation, and those that are meant to give direction on data protection or personal information regulations do not have implementing policy guidelines.

Moreover the lack of a comprehensive institutional framework to provide oversight on the collection and processing of data by public and private bodies remains a significant challenge in the country. As a result, the large number of public and private institutions that collect private data, continue to amass the data collected without transparent safeguards for the data and with little or no regulation. Some including government agencies do not obtain consent before they collect, process, store, and share the data. Even though some of these practices could give rise to legal action by the affected data subjects, there has only been one prominent legal challenge relating to privacy in the country.

Furthermore, the private sector and civil society are missing in the data protection discourse in Ethiopia. The drafting process is not transparent and consultative. The private sector, civil society, the media, and academics were not consulted when the government first started the drafting process a decade ago and they are still not engaged in the process today. Without engaging the major stakeholders in the drafting process, the data protection challenges in the country will not be adequately addressed. Moreover, the privatisation of Ethio-telecom and the liberalisation of the telecommunication sector would mean that many more players in the private sector will start collecting personal data. Without the enactment of a robust data protection and privacy law, the challenges faced by data subjects will be exponential.

6.2 Recommendations

The Government should:

- Enact a comprehensive data protection and privacy law that sufficiently defines the duties of data controllers and processors and the rights of data subjects.
- Ensure the data protection law development process is consultative, transparent, and participatory, involving all concerned actors including data subjects and the private sector.
- Develop appropriate policies to facilitate the implementation of laws and guide the works of its organs in relation to privacy and data protection.
- Establish an independent organ mandated to oversee and enforce data protection and privacy in the country. This is particularly essential given the unwarranted surveillance track record of the intelligence and law enforcement in Ethiopia.
- Equip its organs and their employees with adequate knowledge in safeguarding data protection and privacy.
- Review and redraft all legislations that infringe on the right to privacy to ensure they adequately protect all citizens including the Anti-Terrorism Proclamation, Computer Crime Proclamation, the Anti-Corruption Proclamation and others.
- Put in place appropriate legal and institutional mechanisms before the privatization process takes place in order to minimize the risks on private data protection.
- Require all government agencies to appoint data protection officers or data protection compliance officers within their office.

Private institutions should:

- Adopt data protection guidelines, policies and regulations that spell out the terms and conditions for the users of their services.
- Train their employees to comply with private data protection laws and policies
- Employ compliance officers to oversee compliance with data privacy protection standards.

Civil Societies and Academia should:

- Advocate for legal and institutional changes on privacy and data protection.
- Advocate for a better private data protection practice and lead the changes in this regard by providing research based inputs and best practices.
- Keep government and other bodies in check in their data protection engagement.
- Actively demand for more involvement in policy formulation processes.

The Media should:

- Accelerate awareness creation on data protection and privacy.
- Repot more on cases concerning data protection and privacy violations.
- Follow and report on the development of the draft bill and related policy developments.

.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org