State of Internet Freedom in Ethiopia 2019

Mapping Trends in Government Internet Controls, 1999-2019

January 2020

CIPESA

Table of Contents

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in Ethiopia tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. Other country reports for Bostwana, Burundi, Cameroon, Chad, the DRC, Kenya, Malawi, Nigeria, Rwanda, Senegal, Tanzania, Uganda and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

The research was conducted with support from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Federal Ministry for Economic Cooperation and Development (BMZ).

Editors
Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

State of Internet Freedom in Ethiopia 2019
Published by CIPESA,
www.cipesa.org
January 2020

1 Introduction

1.1 Introduction

Internet freedom in Ethiopia has been on the decline over the past two decades as the government continued to adopt aggressive and sophisticated measures that curtailed internet freedoms. Besides the adoption of retrogressive and repressive policies and laws that criminalise online communication and dissent, the government has utilised surveillance, censorship, filtering, blocking, throttling and internet shutdowns.

In 2004, the government adopted the Ethiopian Aviation Security Proclamation,[1] which empowers the Security, Immigration and Refugee Affairs Authority and the Federal Police Commission to intercept and conduct surveillance without a court warrant, so as to prevent unlawful acts against aviation institutions and flight safety equipment.[2]

The government has also been accused of deploying spyware and other hacking and surveillance tools to snoop on bloggers, journalists, members of the opposition and other critical individuals.[3] Further, it has maintained tight control over internet access, with the state-owned Ethio Telecom having a monopoly on the telecommunications sector and keeping costs of access high, as the country is ranked among the most expensive for internet users.[4]

However, there was a lot of optimism when the current Prime Minister Abiy Ahmed took over in April 2018[5] and introduced sweeping changes in governance, leading to increasing access to the internet and censored content, decreasing online self-censorship, and the release of imprisoned bloggers.[6] In February 2018, authorities released Mamushet Amare, a former leader of the All Ethiopian Unity Party, who had been detained on terrorism-related charges since March 2017.[7] An additional 9,702 prisoners were released in January 2018, a majority of whom were high-profile opposition politicians, journalists, and activists.[8]

[1] *Proclamation No. 432/2004 Ethiopia Aviation Security Proclamation https://chilot.me/wp-content/uploads/2011/09/proc-no-432-2004-ethiopian-aviation-security.pdf*

[2] *Ibid, sections 32(b) and 5(3) of the Proclamation.*

[3] *UK's Firm Surveillance Kit Used to Crash Uganda Opposition http://www.bbc.com/news/uk-34529237*

[4] *The Tragedy of Ethiopia's Internet, http://motherboard.vice.com/read/the-tragedy-of-ethiopias-internet*

[5] *Aljazeera, Ethiopia to release thousands of Oromo Political Detainees https://www.aljazeera.com/news/2018/01/ethiopia-free-thousands-oromo-political-detainees-180127111131976.html*

[6] *How Ethiopia Controls the Internet https://www.usnews.com/news/best-countries/articles/2019-06-21/ethiopia-restores-the-internet-but-digital-censorship-worries-remain*

[7] *Ethiopia 2018 Human Rights Report https://www.state.gov/wp-content/uploads/2019/03/Ethiopia-2018.pdf*

[8] *Ibid*

Further, in June 2018, the government opened access to 264 blocked websites and TV stations.[9] Those allowed back on air included the US-based Ethiopian Satellite Television (ESAT) and Oromo Media Network (OMN). According to AccessNow, in July 2018, almost all of the websites that were previously blocked were accessible, with a few notable exceptions.[10] All media outlets were unblocked except the HTTP version of oromiamedia.org, while most social networking sites were accessible over Wi-Fi and mobile data - except Instagram. Instagram remained accessible over Wi-Fi but was blocked on mobile data. Also, all human rights, LGBTQI, political opposition, and armed group websites were unblocked with the exception of the Ginbot 7-armed group. Others that were unblocked included siphon.ca and ultrasurg.us, while the Tor Project site remains blocked in Ethiopia. Other changes included the privatisation of some government monopolised sectors and making peace with Eritrea.[11]

However, despite the various reforms introduced by the new government, there have been challenges. In spite of the promises by the Prime Minister upon coming to office, there have been numerous incidents which have clawed back on the reforms, as attempts to stifle freedom of expression and access to information online, including through internet shutdowns, have become ubiquitous. Moreover, in response to communal violence that may have been provoked or exacerbated by online speech, the government in 2019 drafted a new hate speech law that would unduly criminalise speech and promote censorship by, among others, broadening the definition of hate speech and the dissemination of fake news.[12] It is therefore important to situate the on-going discussions around internet rights in Ethiopia by providing an in-depth analysis of the trends of how the government policies and practices have shaped and are restricting digital rights in the country.

1.1 Aim of the study

The research sought to document government controls and their effect on the levels of internet freedom in Ethiopia. It traces trends of government regulation and control over a 20-year period, stretching from 1999 to 2019. The study focuses on the proliferation of retrogressive and repressive policies and laws and surveillance capacity of the Ethiopia government; digitisation programmes; and censorships. The findings will inform key stakeholders such as law and policy makers, media, academia, technologists, civil society, and researchers on the measures to undertake to better Ethiopia's digital environment.

[9] *Ethiopia unblocks 264 websites and TV channels https://www.africanews.com/2018/06/23/ethiopia-unblocks-264-websites-and-tv-channels//*

[10] *Ethiopia: Verifying the unblocking of websites https://www.accessnow.org/ethiopia-verifying-the-unblocking-of-websites/*

[11] *Jason Burke, 'These changes are unprecedented': how Abiy is upending Ethiopian politics, the Guardian https://www.theguardian.com/world/2018/jul/08/abiy-ahmed-upending-ethiopian-politics*

[12] *Ethiopia: Bill Threatens Free Expression https://www.hrw.org/news/2019/12/19/ethiopia-bill-threatens-free-expression*

2 Methodology

The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews with purposively selected respondents. Reports of previous studies, media reports, academic works, government documents, and other literature, were reviewed. The literature review generated an understanding of the recent developments in internet freedom in Ethiopia.

The legal and policy analysis included a review of relevant laws, policies, and practices. Such laws and policies include those that govern the telecoms sector, the media, social media use, access to information, interception of communications, security and intelligence agencies, and security enforcement in general.

The Key Informant Interviews (KIIs) were conducted with purposely selected respondents, who included staff of private companies (such as banks and Internet Service Providers), government ministries (such as those responsible for ICT and security), media houses, social media users, human rights defenders and activists, consumers' associations, academics and lawyers.

3 Country Context

This section provides a general overview of the state of Information and Communications Technology (ICT) in Ethiopia. It also highlights the political environment and the factors affecting democratisation processes in the country. In addition, it describes the economic status of Ethiopia, presenting indicators on GDP per capita, income levels and its ranking on the Human Development Index.

3.1 ICT Status

Ethiopia has experienced considerable growth in internet penetration from less than 3% in 2000[13] to 17.7% at the end of December 2019.[14] Most internet users in the country access the internet from their mobile phones.[15] The use of mobile phones has considerably increased in recent years, despite being among the lowest compared to other countries in the eastern Africa region. Statistics from International Telecommunication Union (ITU) indicate that the country has 59.7 mobile-cellular subscribers per 100 persons,[16] which is a significant increase compared to 23.7 subscribers per 100 persons reported in 2014.[17] However, mobile data remained expensive, while the network is prone to frequent outages.

In February 2018, the Ethiopian Council of Ministers reviewed and passed a new proclamation establishing a new federal authority to regulate telecommunication services. The new proclamation establishes the Ethiopian Telecommunications Regulatory Authority as "an independent, transparent, and accountable regulatory authority" aimed at achieving "the government's policy of restructuring the telecommunications market and introducing competition."[18] The state-owned Ethio Telecom is the only provider of telecommunications services in Ethiopia.[19] In June 2018, the government announced its decision to privatise Ethio-telecom in two years and allow other telecommunication service providers to operate in Ethiopia.[20] Despite efforts to turn around the sector, the government has also implemented several internet shutdowns in the country over the years, particularly in response to political events. According to Shutdown Tracker Optimization Project, Ethiopia shut down the internet at least three times in 2018.[21]

[13] *Ethiopia Internet Users https://www.internetlivestats.com/internet-users/ethiopia/*

[14] *Africa Internet Users https://www.internetworldstats.com/africa.htm#et*

[15] *Ibid.*

[16] *ITU data, supra note 20.*

[17] *Human Rights Watch report, supra note 13, p.22.*

[18] *In Ethiopia, impressive momentum for Africa's digital transformation https://news.itu.int/in-ethiopia-impressive-momentum-for-africas-digital-transformation/*

[19] *ICT Market Analysis in Ethiopia 2018 - Challenged by Heavy Regulation & Government Control Over Networks and Poor Telecommunications Infrastructure - https://www.businesswire.com/news/home/20181105005688/en/ICT-Market-Analysis-Ethiopia-2018---Challenged*

[20] *Aaron Maasho, Ethiopia opens up telecoms, airline to private, foreign investors, available at*

[21] *https://www.reuters.com/article/us-ethiopia-privatisation/ethiopia-opens-up-telecoms-airline-to-private-foreign-investors-idUSKCN1J12JJ*
Berhan Taye, Old habits die hard: Ethiopia blocks the internet in the eastern part of the country, again! Available at: https://www.accessnow.org/ethiopia-blocks-internet-in-eastern-part-of-country-again

3.2 Political Environment

The Ethiopian People's Revolutionary Democratic Front (EPRDF), which ruled the country since 1991, adopted an ethnic-based federalism. This party, which has ruled the country for more than 27 years, has been widely criticised for its repressive laws and other measures that stifle political opposition and curtail fundamental freedoms. Under the EPRDF, the government routinely restricted freedom of expression, freedom of association, and the right to privacy and other principal rights, particularly since the controversial 2005 election.[22]

However, the country has been going through commendable political reforms since the coming into power of the new Prime Minister Abiy Ahmed in April 2018. The new Prime Minister has freed thousands of political prisoners,[23] lifted bans on some media outlets, unblocked more than 250 websites,[24] decided to privatise some government monopolised sectors, and made peace with Eritrea.[25] 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 on the democratic space in the country is yet to be fully registered.

3.3 Economic Status

In 2000, Ethiopia, the second-most populous country in Africa, was the third-poorest country in the world. Its annual Gross Domestic Product (GDP) per capita was only about $650, and more than 50% of the population lived below the global poverty line, the highest poverty rate in the world.[26] With about 109 million people in 2018, Ethiopia is still the second most populous nation in Africa after Nigeria, and the fastest growing economy in the region. Figures from the World Bank indicate that the country has a (GDP per Capita (PPP) current international of USD 2,018, up from $494.3 in 2000.[27] Further, the country ranks at a low position 173 out of 189 countries, under the UNDP Human Development Indicator ranking of 2018, down from 171 reported in 2000.[28]

The economy is reported to have experienced strong, broad-based growth averaging 9.9% a year between 2007/08 and 2017/18, compared to a regional average of 5.4%. Ethiopia's real (GDP growth decelerated to 7.7% in 2017/18.[29] The high economic growth brought with it positive trends in poverty reduction in both urban and rural areas, leading to a decrease in the share of population living below the national poverty level from 30% in 2011 to 24% in 2016.[30]

[22] *Human Rights Watch Report, supra note 13, p.12.*

[23] *Aljazeera, Ethiopia to free thousands of Oromo Political Detainees, https://www.aljazeera.com/news/2018/01/ethiopia-free-thousands-oromo-political-detainees-180127111131976.html*

[24] *Berhan Taye, Ethiopia: Verifying the unblocking of Websites https://www.accessnow.org/ethiopia-verifying-the-unblocking-of-websites*

[25] *Jason Burke, 'These changes are unprecedented': how Abiy is upending Ethiopian politics, the Guardian, * July 2018, https://www.theguardian.com/world/2018/jul/08/abiy-ahmed-upending-ethiopian-politics*

[26] *The story of Ethiopia's incredible economic rise https://qz.com/africa/1109739/ethiopia-is-one-of-the-fastest-growing-economies-in-the-world/*

[27] *GDP per capita, PPP (current international $), World Bank https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?locations=ET*

[28] *Human Development Indices and Indicators: 2018 Statistical Update http://hdr.undp.org/sites/all/themes/hdr_theme/country-notes/ETH.pdf*

[29] *Ibid*

[30] *Ibid*

4 Results

4.1 Key Trends of the Internet Control Over the Last Two Decades

This section traces the history, evolution and shifts of internet control measures in Ethiopia since 1999. The aim is to provide a deeper appreciation of the intervening political and socio-economic considerations behind the different control measures as introduced and applied by the Ethiopian government.

4.1.1 Weaponising the Law to Legitimise Actions

Legalising Surveillance and Interception of Communication

Surveillance by the government has continued over the past, supported by various laws. In 2004, the government adopted the Ethiopian Aviation Security Proclamation,[31] that empowers the Security, Immigration and Refugee Affairs Authority and the Federal Police Commission to intercept and conduct surveillance without a court warrant, so as to prevent unlawful acts against aviation institutions and flight safety equipment.[32] Before its adoption, the Ethiopian government had in 2002 amended Proclamation No. 49/1996 providing for the regulation of telecommunications, and prohibiting non-state actors from providing telecommunication services, leaving the monopoly of the sector to the state-owned Ethio Telecom.[33]

The Ethiopian Anti-Terrorism Proclamation of 2009[34] similarly provides for interception of communications. Under Article 14, it authorises interception of communication of the individual including telephone, fax, radio, internet, electronic, postal and similar communications. Communication service providers are required to cooperate when requested by the National Intelligence and Security Service (NISS) to conduct the interception. Those who fail to cooperate can be imprisoned for between three and 10 years.

In 2006, the Ethiopian government established the Information Network Security Agency (INSA) and set up the country's first cyber intelligence unit. The Agency was re-established in 2013, under the Information Network Security Agency Re-establishment Proclamation No. 808/2013 with the objective of ensuring “that information and computer based key

[31] *Ethiopia’s Aviation and Security Proclamation https://chilot.me/wp-content/uploads/2011/09/proc-no-432-2004-ethiopian-aviation-security.pdf*

[32] *Ibid, sections 32(b) and 5(3) of the Proclamation*

[33] *Text of the proclamation https://chilot.me/2011/08/proclamation-no-491996telecommunications/*

[34] *Ethiopia’s Anti-Terrorism Proclamation https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/85140/95140/F260526391/ETH85140.pdf*

infrastructures are secured, so as to be enablers of national peace, democratization and development programs."[35] Under Article 12 of the Proclamation, every concerned body has an obligation to cooperate with the Agency in exercising its powers and duties pursuant to the Proclamation.

Further, the Computer Crime Proclamation 958/2016[36] permits the real-time collection of computer data under its Article 25. The investigatory organ may request a court warrant to conduct real-time interception or surveillance on computer data, data processing service, or internet and other related communications of suspects. Further, it requires under Article 24, for service providers to retain the computer traffic data disseminated through their computer systems or traffic data relating to data processing or communication service for one year. The data is required to be kept secret unless a court orders for its disclosure.

Under Article 27 of the National Intelligence and Security Service Reestablishment Proclamation,[37] all persons have a duty to cooperate with the NISS when requested and furnish intelligence or evidence necessary for the work of the service. Failure to comply is punishable under the provisions of the Criminal Code.

Rise of National Security, Fighting Terrorism as Justifications for Repressive Laws

The protection of national security, preservation of public order and the fight against terrorism have been widely used on the continent to enact repressive legislation. Moreover, the terms such as "national security" and "public order" have not been clearly defined and are therefore ambiguous and abused to extend to all aspects of society with a common trait of promoting impunity by state security agencies in their operations.

The Ethiopia's 2009 Anti-Terrorism Proclamation[38] defines "digital evidence" as information of probative value stored or transmitted in digital form that is any data, which is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device, and includes a display, print out or other output of such data;[39] while public service is defined as electronic, information communication, transport, finance, public utility, infrastructure or other similar institutions or systems established to give public service.[40]

The Proclamation was widely misapplied and abused to enforce censorship, silence dissidents, and unduly compromise fundamental rights and freedoms.[41] The terrorism law permits the police to detain terrorims suspects without charge for up to a maximum of four months, during investigations.

In 2013, Ethiopia, introduced the Telecom Fraud Offense Proclamation, which criminalised call back services, Voice Over Internet Protocol (VoIP) services like WhatsApp, Viber, Skype, and others. The government justified the need for the law, stating in its preamble that "telecom fraud is a serious threat to national security".[42]

[35] *Information Network Security Agency Re-establishment Proclamation No. 808/2013 https://chilot.me/wp-content/uploads/2014/09/proclamation-no-808-2013-information-network-security-agency.pdf*

[36] *Computer Crime Proclamation https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/103967/126636/F1922468791/ETH103967.pdf*

[37] *National Intelligence and Security Service Reestablishment Proclamation https://chilot.files.wordpress.com/2014/09/proclamation-no-804-2013-national-intellegence-and-security-services-establishment.pdf*

[38] *Anti-Terrorism Proclamation 652/2009 https://www.refworld.org/docid/4ba799d32.html*

[39] *Article 2(8) of the Anti-Terrorism Proclamation*

[40] *Article 2(7) of the Ant-Terrorism Proclamation*

[41] *The Terrorism of 'Counterterrorism': The Use and Abuse of Anti-Terrorism Law, the Case of Ethiopia http://eujournal.org/index.php/esj/article/view/9348/8911*

[42] *Telecom Fraud Offences Proclamation No - 761/2012 https://chilot.me/2012/12/proclamation-no-7612012-telecom-fraud-offence-proclamation/*

Excessive and Punitive Responses

The year 2005 marked a turning point for Ethiopia, setting the tone for its subsequent repressive actions in the years that followed. After the controversial May 2005 general election and the unrest that ensued, the government commenced a widespread crackdown and meted violence on protesters, leading to serious human rights violations[43] including extra-judicial killings of 193 and the injury of 763 persons, arbitrary arrests, unlawful detention and torture of tens of thousands of people, including opposition leaders, by Ethiopian security forces.[44]

The censorship in Ethiopia was in turn part of broader limits to free expression and the freedom to assemble and associate, and also the enactment of restrictive laws such as the Proclamation on Broadcasting Services in 2007;[45] the Proclamation to Provide for Freedom of the Mass Media and Access to Information adopted a year later further limited freedom of speech, right to access information and press freedom in the country.[46] Moreover, the Proclamation to Provide for the Registration and Regulation of Charities and Societies enacted in February 2009, restricted non-government organisations that received more than 10% of their financing from foreign sources from engaging in essentially all human rights and advocacy activities, leading to the closure of several organisations.

4.1.2 Disrupting Networks – From SMS Censorship to Social Media Blockage to Internet Throttling

Over the years, network disruptions have emerged as a major technique which the Ethiopian government, like several other African governments, has employed to stifle digital rights. The disruptions are mostly ordered by governments eager to disrupt communications and curtail citizens' access to information to limit what the citizens can see, do, or communicate. The disruptions have mostly been initiated around election times, public protests, and during national exams. In several cases around the continent, security agencies work with national communications regulators to order the disruption, mostly citing national security or public order considerations, and referencing the regulator's powers to order service providers to interrupt services.[47]

Early Years of SMS Blockage

In 2005, Ethiopia recorded its first network disruption, following the May post-election unrest, when the government turned off SMS, claiming the opposition had been using SMS to organise protests. The service was unblocked after more than two years.[48] The government also blocked access to independent websites and some popular blogging sites in the face of protests by the opposition.[49]

Tests conducted between 2008 and 2010 on websites and blogs found extensive evidence of filtering of political content,[50] implying that the network disruption was part of a larger campaign by the Ethiopian government to thwart opposition organising through digital mediums. In June 2019, the country's text messaging services were shut down without

[43] *Ethiopia row over 'massacre' leak http://news.bbc.co.uk/2/hi/africa/6067386.stm; Ethiopian protesters 'massacred' http://news.bbc.co.uk/2/hi/africa/6064638.stm*

[44] *Ethiopia: Crackdown Spreads Beyond Capital https://www.hrw.org/news/2005/06/15/ethiopia-crackdown-spreads-beyond-capital; Why We Don't Hear About the Conflict in the Ogaden https://slate.com/news-and-politics/2007/09/why-we-don-t-hear-about-the-conflict-in-the-ogaden.html*

[45] *Proclamation On Broadcasting Service No. 533/2007 https://www.refworld.org/docid/4ba79aae2.html*

[46] *Proclamation to Provide For Freedom of The Mass Media And Access To Information No. 590/2008 https://www.refworld.org/docid/4ba7a6bf2.html*

[47] *CIPESA, A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa https://cipesa.org/?wpfb_dl=252*

[48] *Ethiopia anger over texting and internet blackouts https://www.bbc.com/news/world-africa-48653392*

[49] *Bogdan Popa, Google Blocked in Ethiopia http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml*

[50] *CIPESA, State of Internet Freedom in Ethiopia https://cipesa.org/?wpfb_dl=178*

explanation, sparking anger across the country.[51] The shutdown coincided with the nationwide exams, which some say may be the reason for the shutdown, speculating that it was intended to stop students from cheating in examinations.[52]

Network Shutdowns Become Endemic

The Ethiopian government has over the years implemented multiple and long-running network disruptions. Following uprisings in some regions, it continuously blocked social media sites and carried out national and regional internet blackouts, often citing national security threats or the need to stem cheating during national exams as the basis for the disruptions.[53]

In July 2016, the government ordered that access to Facebook, Twitter, Instagram, Viber, WhatsApp and other sites be blocked. The government claimed the country-wide ban was necessary after university entrance exams were posted online. Hence, the internet blockage was intended to prevent students from being distracted from studying during the exam period and also to prevent the spread of false rumours.[54] In addition, other incidents of social media and internet shutdowns were recorded in Ethiopia in 2017 during similar exam periods.[55] Again in 2019, the government shut down access to text messaging services and the internet during national school examinations.[56]

In August 2016, Ethiopia had shut down the internet during protests by the Oromo and Amhara ethnic groups against their alleged marginalisation by the government.[57] Similarly, in 2018, the government shut down broadband and mobile internet in the eastern part of the country amid growing tensions between the national and regional governments in the Somali region of Ethiopia.[58] In July 2019, the government shut down the internet for 10 days following the assassination of six top government officials, with the government alleging that the killings were part of a coup attempt.[59] In total, more than a dozen government-ordered internet disruptions have been recorded in Ethiopia over the past five years.[60]

According to Netblocks, an organisation which monitors freedom of access to the internet, a one-day shutdown of the internet costs Ethiopia at least USD 4.5 million, over and above the everyday inconvenience and frustration.[61] Following a visit to Ethiopia in 2019, David Kaye, the United Nations Special Rapporteur on the right to freedom of opinion and expression, noted that the Ethiopian government had shut down the internet eight times in 2019 alone.[62] Further, he pointed out that it was alarming for the government to resort to shutting down the internet in times of public protest or even school exams. He noted that no government official could articulate the legal basis for the shutdowns and expressed concern that such actions were undertaken without constraint under law or policy. The Rapporteur strongly urged the government to discontinue the practice.

[51] *Ethiopia anger over texting and internet blackouts https://www.bbc.com/news/world-africa-48653392*

[52] *Ibid*

[53] *Freedom of the Net Report 2017 https://freedomhouse.org/report/freedom-net/2017/ethiopia*

[54] *Ethiopia blocks Facebook and other social media for exams http://www.bbc.com/news/world-africa-36763572*

[55] *Ethiopia blocks internet 'to stop exam cheats' https://www.bbc.com/news/technology-40118378*

[56] *Ethiopia anger over texting and internet blackouts https://www.bbc.com/news/world-africa-48653392*

[57] *What is behind Ethiopia's wave of protests? http://www.bbc.com/news/world-africa-36940906*

[58] *Old habits die hard: Ethiopia blocks internet in the eastern part of the country, again! https://www.accessnow.org/ethiopia-blocks-internet-in-eastern-part-of-country-again/*

[59] *Internet restored in Ethiopia 10 days after assassinations https://wgme.com/news/nation-world/internet-restored-in-ethiopia-10-days-after-assassinations*

[60] *Access Now Shutdown Tracker https://internetshutdowns.in/*

[61] *Ethiopia anger over texting and internet blackouts https://www.bbc.com/news/world-africa-48653392*

[62] *United Nations Special Rapporteur on the right to freedom of opinion and expression*
David Kaye Visit to Ethiopia, 2-9 December 2019 End of mission statement https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25402&LangID=E

4.1.3 Surveillance Galore: The Build-Up of States' Capacity

Despite the existence of several provisions within the legal and policy frameworks, by 2005 reports of surveillance and interception of communication in Ethiopia, and elsewhere in Africa were few. However, the Ethiopian government has in successive periods continued to enhance its technical capacity to intercept and conduct surveillance.

Going High-Tech to Implement Surveillance

The national security and intelligence apparatus have since 2005 consistently targeted opposition groups, critics, journalists, and researchers with sophisticated surveillance software.[63] According to the Human Rights Watch, the government has been reported to use surveillance not only to fight terrorism and crime, but as a key tactic in its abusive efforts to silence dissenting voices in the county. Hence, "anyone that opposes or expresses dissent against the government is considered to be an 'anti-peace element, or a 'terrorist'.[64] Moreover, opposition leaders and journalists have over the years, reported suspicions of telephone tapping, other electronic eavesdropping, and surveillance, and that government agents have attempted to lure them into illegal acts by calling and pretending to be representatives of previously designated terrorist groups.[65]

In 2011, the Ethiopian government established the Federal Police Commission with power to investigate crimes relating to information networks and computer systems and install CCTV cameras to facilitate the prevention and investigation of crime.[66] This move facilitated mass surveillance of citizens, in the absence of clear information as to the capabilities of the system and general oversight.

In 2013, the government re-established the National Intelligence and Security Services (NISS) with a ministerial status and as an autonomous body of the federal government.[67] This institution has broad intelligence and security mandate and power to investigate threats "against the national economic growth and development activities" and to gather intelligence on serious crimes and terrorist activities. It is responsible for many of the human rights violations that happened in the country before 2017 including mass and illegal surveillance of citizens both online and offline, censorship of dissenting voices, torture, and intimidation of dissenting voices online and offline.

In 2018, authorities were reported to have blocked access to Virtual Private Network (VPN) providers that enable users to circumvent government screening of internet browsing and email, with reports that such surveillance resulted in arrests.[68] Additionally, the pattern of surveillance and arbitrary arrests of Oromo university students based on perceived dissent and participation in peaceful demonstrations have been reported. Also, activists in the LGBTI community have reported surveillance and feared for their safety.[69]

[63] *How Ethiopia Controls the Internet https://www.usnews.com/news/best-countries/articles/2019-06-21/ethiopia-restores-the-internet-but-digital-censorship-worries-remain*

[64] *How the NSA built a secret surveillance network for Ethiopia https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/*

[65] *Ethiopia 2018 Human Rights Report https://www.state.gov/wp-content/uploads/2019/03/Ethiopia-2018.pdf*

[66] *Ethiopian Federal Police Commission Establishment Proclamation https://chilot.me/wp-content/uploads/2012/02/proclamation-no-720-2011-ethiopian-feeral-police-commission-establishment.pdf*

[67] *National Intelligence and Security Service Reestablishment Proclamation No. 804/2013 https://chilot.files.wordpress.com/2014/09/proclamation-no-804-2013-national-intellegence-and-security-services-establishment.pdf*

[68] *Ibid*

[69] *Ethiopia 2018 Human Rights Report https://www.state.gov/wp-content/uploads/2019/03/Ethiopia-2018.pdf*

The Ethiopian telecommunications Corporation (ETC), which later became Ethio Telecom, is reported to have signed contracts with three major Chinese companies - ZTE, Huawei and China International Telecom Corporation (CITCC) - to rapidly develop the country's infrastructure in 2006.[70] Further, ZTE signed an additional $1.6 billion deal to be ETC's sole vendor for nine equipment packages, which were not disclosed. In 2013, ZTE and Huawei were announced as successful bidders of a $1.6 billion deal to upgrade Ethio Telecom's infrastructure. In addition, Ethio Telecom uses the ZSmart customer management system from ZTE, which is reported to provide the government with full access to user information, the ability to intercept SMS text messages, to record phone conversations, and to locate targeted individuals through real-time geo-location tracking of mobile phones.[71] In 2017, it was reported that the United States National Security Agency, in exchange for local knowledge and an advantageous location, provided Ethiopia with technology and training integral to electronic surveillance.[72]

4.1.4 The Push Towards Determining Identity Amidst Poor Oversight

Over time, the Ethiopian government has progressively introduced measures that would enable its security agencies to identify telecommunication services users with precision. From SIM card registration, successive regimes have since adopted digital identities and incorporated biometrics and artificial intelligence, albeit with poor or no oversight.

Rapid Adoption of Biometric Data Collection

In 2012, the Ethiopian government introduced the Vital Events and Registration Proclamation, 2012.[73] The law proposed the introduction of national identity cards with identification numbers for citizens. It also requires the collection and storage of biometrics of citizens in a centralized system. The stored information could be disclosed to other organs for specified purposes such as 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.

In September 2017, the Ethiopian government, through the Ministry of Communication and Information Technology (MCIT), embarked on the process of registering mobile phone owners on Ethio Telecom network that has over 50 million subscribers.[74] The system matches 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. Mandatory SIM card registration in Ethiopia requires users to provide their names, photo ID, signature, relatives' phone numbers, and addresses.

[70] *"They Know Everything We Do" Telecom and Internet Surveillance in Ethiopia https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia*

[71] *Ibid*

[72] *How the NSA built a secret surveillance network for Ethiopia https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/*

[73] *Registration of Vital Events and National Identity Card Proclamation, Proclamation No.760/2012 https://chilot.me/wp-content/uploads/2017/04/proclamation-no-902-2015-registration-of-vital-events-and-national-identity-card.pdf*

[74] *Ethiopia government in mobile phone registration drive to curb smuggling, fraud http://aptantech.com/2017/09/ethiopia-government-in-mobile-phone-registration-drive-to-curb-smuggling-fraud/*

4.2 Positive Developments

Despite negative trends that hindered internet freedom and digital rights in past decades, there have been some positive developments to advance these rights in Ethiopia. These include the recent adoption of progressive legislation and repeal of repressive legislation.

4.2.1 Adoption of Progressive Legislation

Ethiopia passed the Communication Regulatory Proclamation in June 2019 to facilitate the liberalisation of the telecom sector in the country, establish a sector regulator, allow the licensing of new operators, and end the state-owned Ethio Telecom's monopoly.[75] The proclamation establishes the Ethiopian Telecommunications Regulatory Authority as "an independent, transparent, and accountable regulatory authority" so as to achieve "the government's policy of restructuring the telecommunications market and introducing competition."[76]

4.2.2 Repeal of Repressive Legislation

Prime Minister Ahmed Abiy committed to revisiting the laws that provided the illegitimate basis for detaining so many political prisoners. Following this, in July 2018 the Federal Attorney General's office established a 13-member justice reform advisory council to address a range of critical issues, including revising repressive laws and improving judicial independence.[77] As a result, the Charities and Registration Proclamation has already been amended. Other repressive laws awaiting reform include the Anti-Terrorism Proclamation, the Freedom of the Mass Media and Access to Information Bill, and the Computer Crime Proclamation.

[75] *Text of proclamation https://addisstandard.com/wp-content/uploads/2019/02/Draft-Communication-Serv-Proclamation-.pdf*

[76] *In Ethiopia, impressive momentum for Africa's digital transformation https://news.itu.int/in-ethiopia-impressive-momentum-for-africas-digital-transformation/*

[77] *Hope for Revision of Ethiopia's Draconian Laws? https://www.hrw.org/news/2018/08/27/hope-revision-ethiopias-draconian-laws*

5 Conclusion and Recommendations

5.1 Conclusion

The study has found that over the last two decades, the Ethiopian government broadened the range of measures that govern the use of digital communications including the internet. It is evident that the country has employed legislation to legitimise practices which are otherwise unlawful to impose restrictions and internet controls.

Ethiopia was probably the first sub-Saharan African country to begin blocking internet sites, with the first reports of blocked websites appearing in May 2006 when opposition blogs were unavailable.[78] The country also introduced several laws to enable the interception of communications, and to criminalise free speech. In 2009, the government enacted the Anti-Terrorism Proclamation- No 652/2009, under which it is estimated that over 900 individuals were indicted over their online activity.[79] In 2012, Ethiopia enacted the Telecom Fraud Offences Proclamation, which became one of the pieces of legislation used to quash internet freedom.

Although the current Prime Minister Abiy's government has raised the level of optimism with respect to positive legal reforms and respect for human rights, his government is still embroiled in conflict. Despite the progress, there have still been numerous attempts to stifle freedom of expression and access to information online with incidents of internet shutdowns in the country continuing unabated. If these are not halted and become endemic, there is a likelihood that all the positive gains may be lost.

[78] *Human Rights Watch, "They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia, https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia*

[79] *Zelalem Kibret, The Terrorism of 'Counterterrorism': The Use and Abuse of Anti-errirism Law, The Case of |Ethiopia, http://eujournal.org/index.php/esj/article/view/9348*

5.2 Recommendations

Government

- Respect human rights and freedoms, especially the right to freedom of expression, access to information and privacy as enshrined in the Ethiopia constitution and in international instruments that Ethiopia has ratified.
- Define clearly in policies and laws the acceptable measures, terms, and circumstances in which internet controls may be applied, in line with constitutional and international human rights standards, and ensure there is transparency, accountability and judicial oversight.
- Ensure there are sufficient safeguards and principles including 'privacy by design' in laws and policies for the robust protection of the right to privacy and personal data.
- Fast-track reforms to ensure that all repressive policies, laws and practices are reviewed, abolished and new ones that are rights-respecting are adopted.
- Ensure comprehensive consultation and meaningful participation of key stakeholders including civil society, academia, business and the technical community in policy and legislative reforms.

Companies

- Adopt and implement the United Nations Business and Human Rights Principles and safeguard the rights of customers by default.
- Require that government requests for internet controls and disruptions comply with the rule of law and due process.
- Terms and conditions of privacy and data usage must be clear and open, and agreements must be honoured.
- Adopt the use of technologies that make it difficult to carry out surveillance, interception of traffic and internet shutdown.

Media

- Collaborate with other stakeholders in the promotion of internet and press freedom.
- Challenge laws that limit press freedom and citizens' access to information online and offline.
- Promote digital safety and the protection of journalists.
- Build the media's capacity and knowledge on internet freedom issues.

Academia

- Conduct evidence-based policy and legal research.
- Disseminate research findings and recommendations to promote internet freedom.
- Include internet freedom in their curriculum to ensure students are made aware of the pertinent issues.
- Collaborate with other stakeholders in the promotion of internet freedom.

Civil Society

- Collaborate to promote internet freedom through active monitoring, advocacy, research, and public interest litigation.
- Create awareness, build capacity, and sensitise the public and key stakeholders through innovative initiatives to create greater understanding of internet freedom issues and on best practices to advance digital rights.
- Mainstream human rights organisations should incorporate internet freedom in their programming and collaborate better with specialised organisations working on internet freedom.
- Monitor and expose government collaboration, including projects, developments, procurement, and training with foreign governments, which could potentially violate human rights and threaten internet freedom.
- Advocate against government adoption of foreign-inspired censorship, data collection and surveillance methods and technologies.
- Advocate and remind state agencies of their obligations under international human rights instruments.
- Build stronger multi-stakeholder coalitions locally, regionally, and globally to push-back against internet controls and promote internet freedom.

[72] *Twitter war shines light on how Rwanda intimidates press https://cpj.org/blog/2014/03/twitter-war-shines-light-on-how-rwanda-intimidates.php retrieved on 19/10/2019*

[73] *#BBCtrending: The troll in the president's office, https://www.bbc.com/news/blogs-trending-26536732*

[74] *https://www.refworld.org/docid/5be16afd116.html*

[75] *https://www.theeastafrican.co.ke/news/ea/Rwandans-troll-outgoing-Francophonie-boss-over-Rwigara-case/4552908-4844674-53luju/index.html*

[76] *https://www.chronicles.rw/2019/03/04/oxfam-director-byanyima-under-fire-over-her-uganda-rwanda-comments/*

[77] *Rwanda: National Election Commission to censor candidates' online campaign messages https://www.article19.org/resources/rwanda-national-election-commission-to-censor-candidates-online-campaign-messages/ retrieved on 19/10/2019*

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