The Reforms Ethiopia Needs to Advance Internet Freedom

July 2018

Background

Since April 2018, the new Ethiopian government has been undertaking unprecedented political and economic reforms. This follows countrywide protests that forced the former Prime Minister Hailemariam Dessalegn to resign in February 2018, leading to the appointment of a young and charismatic new premier, Abiye Ahmed two months later. Since then, the government has freed thousands of prisoners; announced measures to liberalise the telecom, aviation, and transportation sectors; and dropped charges against many opposition leaders, bloggers, and activists. Further, the new administration has lifted the state of emergency that had been reinstated in February 2018, reconnected mobile and broadband internet services that were cut off since 2016, and unblocked 246 websites, blogs, and news sites that have been inaccessible for over a decade.

These changes in Ethiopia did not come at a whim. The protests that started in November 2015 in the Oromia region spread to other parts of the country. In response to these protests, the previous government continuously blocked social media sites and implemented national and regional internet blackouts, often claiming it aimed to safeguard national security or to stem cheating during national exams. Consequently, the Oromia region lost internet connectivity for two weeks in March 2018, three weeks before the new prime minister was sworn in. Moreover, as access to the internet deteriorated in the country, the government criminalised freedom of expression online and offline. The arbitrary arrests, detention, and torture of members of the Zone Nine bloggers collective showed how far the government was willing to go to suppress dissenting voices.

The new Prime Minister and his cabinet have promised to open the democratic space in the country and expand freedom of expression online and offline. However, these reforms should go beyond the unblocking of a few hundred websites; they should bring in real changes that will make it impossible to regress to old habits. Therefore, reforms to be implemented must expand internet penetration from the current 15%, to the larger offline majority. Laws that prosecute freedom of expression online and offline like the Anti-Terrorism Proclamation and Computer Crime Proclamation must undergo substantial revisions to meet international standards. Further, the changes within the law enforcement and intelligence agencies should go beyond replacing old officials with new ones, but must tame the undue power given to these bodies to conduct unwarranted surveillance and censorship of netizens. Lastly, the new government should desist from internet shutdowns and censorship.

Below is a detailed description of prevailing challenges to internet freedom in Ethiopia and proposed reforms the Ethiopian government needs to undertake to improve internet freedom in the country.

1. Legislative Environment

The Ethiopian government has used courts and the law to crack down on online and offline activities of critics and opponents. As the government introduced legislation like the Freedom of the Mass Media and Access to Information Proclamation of 2008, the Anti-Terrorism Proclamation of 2009, the Computer Crime Proclamation of 2016, and other laws, access to information, and freedom of expression plummeted. When these proclamations came into effect, they did what they were designed to do: they facilitated and legitimised the arrest, trial, and prosecution of dissenting voices online and offline.

Therefore, in order to sustain the positive reforms that have opened up the online and offline space in Ethiopia, the government must amend the Anti-Terrorism Proclamation, the Computers Crime Law, the Telecom Fraud law, the Freedom of the Mass Media and Access to Information Proclamation, the Broadcasting Service Proclamation, and the Charities and Societies Proclamation. The amendments should strongly protect freedom of expression that is granted in the constitution, and specifically provide for protection of digital rights.

- **Anti-Terrorism Proclamation- No 652/2009**

The Anti-Terrorism Proclamation of 2009 was instrumental in suppressing internet freedom in Ethiopia. The number of people charged under this proclamation is unknown. However, it is estimated that over 900 individuals were indicted over their online activity under this proclamation. Those prosecuted have included bloggers, journalists, editors, activists, musicians, and producers. To strengthen online rights, the new Ethiopian government should amend this Proclamation to put it in line with international minimum standards. Additionally, prosecution should only be of those who pose genuine threats rather than mere dissenting voices. At a bare minimum, the government must amend the proclamation to:

- Limit the definition of 'terrorist acts' under the proclamation. Article 3 provides an overly broad and vague definition of what a 'terrorist act' entails.[1] It has been wantonly used to clamp down on dissenting voices.
- Define what entails encouragement of terrorists under Article 6, as this article conflates free and political speech with the encouragement of terrorism.[2]
- Articles 12 and 22[3] fail to protect the media and journalists. They force journalists to disclose names of their sources and to testify against them. The amendment to these articles should introduce protection of journalists and their sources as per international standards.
- Repeal provisions on unwarranted surveillance. Monitoring of electronic communication and covert searches are provided for under Article 14 (3) which states: "Any communication service provider shall cooperate when requested by the National Intelligence and Security Service to conduct the interception" and Article 14(4) which states: "The National Intelligence and Security Services or the Police may gather information by surveillance in order to prevent and control acts of terrorism."

- **Computer Crime Proclamation of 2016**

The Computer Crime Proclamation of 2016 supplements other proclamations that restrict internet freedom. It also criminalises legitimate speech and defamation and gives intelligence and law enforcement agencies untamed power to conduct surveillance and searches. For this law, amendments should:

- Narrow the definition of, "intimidation" and decriminalise defamation. Article 13(1) does not define what intimidation means and therefore can be construed to criminalise legitimate speech.[4] Article 13(3) criminalises defamation even though the international standard gears towards decriminalising defamation.[5]
- Limit the liability of intermediaries like social media sites and blogging platforms for content and speech the government deems illegal, under Article 16. As the offline civic space shrunk in Ethiopia, those with access to the internet moved the discourse to the digital sphere to express their opinions. Forcing these platforms to police speech in compliance with the government litmus test for what is acceptable speech will continue to be detrimental to internet freedom in the country.

1 *Article 3 of the Proclamation defines a "terrorist acts" as, "Whosoever or a group intending to advance a political, religious or ideological cause by coercing the government, intimidating the public or section of the public, or destabilizing or destroying the fundamental political, constitutional or, economic or social institutions of the country."*

2 *Article 6 of the Proclamation define "encouragement of terrorists" as, "Whosoever publishes or causes the publication of a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission or preparation or instigation of an act of terrorism stipulated under Article 3 of this proclamation is punishable with rigorous imprisonment from 10 to 20 years."*

3 *Article 22 of the Proclamation stipulates that "The police may request from any government institution, official, bank or a private organization or an individual to be given information or evidence which he reasonably believes could assist to prevent or investigate terrorism cases. Anyone so requested shall have the duty to give the information or evidence."*

4 *Article 13(1) "Whoever intentionally intimidates or threatens another person or his families with serious danger or injury by disseminating any writing, video, audio or any other image through a computer systems shall be punishable, with simple imprisonment not exceeding three years or in a serious cases with rigorous imprisonment not exceeding five years."*

5 *Article 13(3) "disseminates any writing, video, audio or any other image through a computer system that is defamatory to the honor or reputation of another person shall be punishable, upon complaint, with simple imprisonment not exceeding three years or fine or both."*

- **Telecom Fraud Offences Proclamation No - 761/2012**

Enacted in 2012, the Telecom Fraud Offense Proclamation is another piece of legislation used to quash internet freedom in Ethiopia. For instance, Article 8 criminalises the provider and the recipient of call-back services[6] by providing for "imprisonment from 5 to 10 years and with fine equal to five times the revenue estimated to have been earned by the person during the period of time he provided the call-back service."

The ambiguous definition of call-back service makes Voice Over Internet Protocol (VoIP) services like WhatsApp, Viber, and Skype illegal, although the government has assured the public of the contrary without amending the law. Moreover, criminalising call-back services which are at times the only affordable services people can access, renders the Proclamation neither in line with the right of access to information nor with the principles of universal access to the internet and other telecom services. The government justifies the need for this law in the preamble to the Proclamation by stating that "telecom fraud is a serious threat to national security". Amendments to this law should delimit what national security entails in the telecom sector, and describe what kind of telecom fraud poses a threat to national security.

Other Legislations That Affect Internet Freedom in Ethiopia

The Freedom of Mass Media and Access to Information Proclamation No 590/2008, the Broadcasting Service Proclamation No 533/2007, and the Charities and Societies Proclamation No 621/2009, were introduced to restrict dissenting voices and thus affect internet freedom in Ethiopia. For instance, the Freedom of the Mass Media and Access to Information Proclamation of 2008 has been crucial in stifling the fledgling free press across the country. In addition, the Broadcasting Services Proclamation has been used to withhold broadcasting licenses from independent media houses, while the Charities and Societies Proclamation restricts civil society organisations from engaging on human rights and internet freedom issues. Although these laws may not directly affect internet freedom, a country without an independent and free press and robust civil society would be unable to achieve meaningful internet freedom. These laws should be amended accordingly to ensure media freedom and an unrestrictive operating environment for human rights organisations.

2. Surveillance of Online Activity

Aided by the Anti-Terrorism, Computer Crime, and Telecom Fraud Offense laws, among others, the Ethiopian government has spied on and restricted the online activities of Ethiopians at home and abroad. The national security and intelligence apparatus have persistently targeted opposition groups, activists, journalists, and researchers with malware attacks for years and some of the targets have fallen prey to these attacks as recently as December 2017. According to Wikileaks documents, the government at one time paid the Hacking Team close to one million Euros to surveil activists and others in the diaspora.

In addition to targeted digital attacks, the social media activity of Ethiopians is highly surveilled. The Ethiopian government has on several occasions prosecuted individuals for their social media activities. The physical threat and the psychological trauma of surveillance endured by many Ethiopian activists and journalists are yet to be sufficiently studied.

If the government is committed to defending freedom of expression online and offline and opening up civic space including in the digital sphere, these targeted malware attacks and undue surveillance of online activities need to stop. The undue power given to law enforcement agencies to conduct unwarranted surveillance needs urgent reform. Ethiopia needs to introduce strong independent judicial oversight over the work of the intelligence and security apparatus as it relates to electronic surveillance, interception of communication and other actions so as to lessen the harm done by these agencies. Government also needs to make efforts to change the culture of hostility this unit has developed towards the internet freedom community in the country.

[6] *Call back service is defined as "the use of dial tone of a foreign telecom operator for international connection without the knowledge of the domestic telecom operator or fraudulently making international calls into apparent domestic calls"*

3. Internet Shutdowns and Censorship

During the three year protests in the Oromia region, most of the country except the capital, Addis Ababa, did not have access to mobile internet. Moreover, there were a series of national and regional internet shutdowns in June 2016, August 2016, and May 2017. As protests grew stronger in the country, the government intensified measures to block and restrict access to multiple social media platforms including Facebook, Twitter, WhatsApp, Instagram, Viber, Telegram, and others, and as such, these platforms were only accessible through the use of Virtual Private Networks (VPN). As of the end of June 2018, Instagram remained inaccessible via mobile internet across Ethiopia. The authorities justified the shutdowns citing reasons such as a need to forestall cheating during national exams or to thwart national security threats. However, the reality on the ground is markedly different. In fact, the shutdowns often happened when there were protests and extrajudicial killings of protesters around the country.

The shutdowns have not only had a significant impact on freedom of expression and disrupted the lives of many Ethiopians. There has been a significant economic cost too. A September 2017 CIPESA report estimates that Ethiopia lost USD 3,499,741 per day due to internet shutdowns and USD 874,935 per day of social media shutdowns. Comparing Ethiopia to other countries in sub-Saharan Africa, the same report indicates that Ethiopia lost over USD 132.1 million during the 36 days of national and regional shutdowns and the seven days of social media disruptions, making it the most affected country in the region.

Shutting down the internet and social did not silence the protesters or their calls for justice and reform and yet it had a high economic cost to businesses as well as to country's gross domestic product, inconvenienced the livelihoods of many, and denied millions their right of access to information. In light of these adverse effects, the government ought to desist from censorship and internet shutdowns, and instead take concrete legislative and practical moves to promote free speech and access to information.

4. Connectivity and Access

Ethiopia's internet penetration rate stood at 15.4% in 2017. The state-owned and sole telecom provider, Ethio-Telecom, has over 66.2 million mobile phone subscribers and out of these, only 16 million are internet users while 4%, or 3.8 million, are active social media users. According to the Affordability Index, when compared to other countries, Ethiopia scores 22 out of 100, which is indicative of poor ICT infrastructure, low broadband adoption rate, and ICT policies that fail to foster equitable access.

It is therefore essential that the government takes concrete steps to bridge the digital divide and expand internet access and affordability. The priorities should include efforts to strengthen the infrastructure in the country and bring in smart policies that boost competition in the telecom sector. Affordability strategies should be in line with the Alliance for Affordable Internet's policy recommendation of 1GB for 2% or less of average monthly income.

The new administration has indicated interest to privatise the telecom sector. This move could potentially bring down connectivity costs. However, the government needs to fully liberalise the telecoms sector and create a competitive industry. Alongside such a liberalisation exercise, the government should enact a strong data protection and privacy law to safeguard user rights.

CIPESA acknowledges the primary contribution of **Berhan Taye** to this brief.

About CIPESA

CIPESA

CIPESA was established in 2004 under the Catalysing Access to Information and Communications Technologies in Africa (CATIA) initiative, which was mainly funded by the UK's Department for International Development (DfID). CIPESA is a leading centre for research and the analysis of information aimed to enable policy makers in East and Southern Africa understand ICT policy issues and for various stakeholders to use ICT to improve governance and livelihoods.

www.cipesa.org **@cipesaug** **programmes@cipesa.org**