State of Internet Freedoms in Ethiopia 2014

An Investigation Into The Policies And Practices Defining Internet Freedom in Ethiopia

OpenNet Africa

CIPESA

Credits

The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) is grateful to our partners on this project, who offered technical and financial support. They include the Humanist Institute for Co-operation with Developing Countries (Hivos), the Citizen Lab at the University of Toronto and the Canadian International Development Research Centre (IDRC).

This report was produced as part of CIPESA's internet freedoms monitoring initiative, OpenNet Africa. Other country reports have been written for Burundi, Kenya, Rwanda, Tanzania, South Africa and Uganda. The country reports, as well as a regional 'State of Internet Freedoms in East Africa' report, are available at www.opennetafrica.org.

State of Internet Freedoms in Ethiopia 2014
Published by CIPESA
May 2014

Content

Introduction

Ethiopia is a low income country with a population of just under 92 million people.[1] The country has since 1991 been under the one party rule of the Ethiopian People's Revolutionary Democratic Front (EPRDF). Dissidents who use the internet to criticise the one party rule have been accused of promoting terrorism and their websites and blogs were blocked. Ethiopia ranks amongst one of the countries with the lowest ICT use in Africa. This is mainly because of the tight control the government maintains over telecom service provision. Many more people are now getting access to mobile phones and the internet, although the ease with which security services access users' data is worrying.

Ethiopian law allows for surveillance and interception of digital communications. This is coupled with harsh sentences against individuals or entities found to be in contravention of these laws. Studies suggest that perhaps more than any other country in Africa, Ethiopia regularly blocks websites, undertakes surveillance of websites and social media, and charges journalists over content published offline and online.[2] As recently as April 2014, authorities continued to arrest bloggers for criticising government policies.[3] The country's laws provide for legal sanctions against individuals for content they publish online, or the 'illegal use' of telecoms services. Such charges have often been framed as 'promoting terrorism', which can attract a 20 year jail term.

Ironically, Article 29 (2) of Ethiopia's constitution provides that "Everyone has the right to freedom of expression without any interference. This right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any media of his choice." Article 29 of the country's Constitution provides backing for these rights. However, recent proclamations such as the 2008 Media Law, the 2009 Anti-Terrorism Law, the 2012 Telecom Fraud Law and most recently, the National Intelligence and Security Re-establishment Proclamation of 2013 have one after the other taken back the rights provided by the constitution.

Background to ICT usage

Ethio Telecom is the state-owned telecommunications company that maintains a monopoly on the sector. Ethiopia is among the African countries with the lowest internet and mobile phone penetration rates. As of 2010, mobile subscriptions stood at 8 phones per 100 inhabitants.[4] However, according to the Ethiopian government, this figure tripled in 2012, with the country reaching 20.5 million subscribers representing penetration of 24%.[5] This was after management of Ethio Telecom was contracted to France Telecom, which drove down costs and relaxed subscription requirements. Ethio Telecom reported that its total customer base for mobile, fixed line, and data services as of June 2012 had grown by 59%

1 *The World Bank, http://data.worldbank.org/country/ethiopia*
2 *Tests by the Citizen lab have consistently found evidence of hundreds of websites that are blocked, as well as presence of surveillance software. Moreover, Freedom House ranks Ethiopia as 'Not free' in terms of online freedoms.*
3 *BBC, Jailed bloggers spark Ethiopia trend, April 30, 2014; http://www.bbc.com/news/blogs-trending-27212472*
4 *ITU, Mobile Cellular Subscriptions, http://www.itu.int/ITU-D/ict/statistics/*
5 *ITU, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx*

compared with the previous financial year. The growth rate for mobile was more than 64%, while for internet and data services was 72%.[6] Internet usage stands at 1.5%.[7] The national literacy rate is 30%. According to Human Rights Watch, the increasing technological ability of Ethiopians to communicate, express their views, and organise, is viewed less as a social benefit and more as a political threat for the ruling party, which depends upon invasive monitoring and surveillance to maintain control of its population.[8]

Relevant Agencies

The Information Network Security Agency (INSA): The mission of the agency is to be "a reliable, world-class provider of information and information systems with maximum security against any peril." Its mission is to establish efficient information security capability, which relies on research based applications so as to safeguard key government and public information systems from any threat.

During 2013, the Ethiopian government revamped the INSA, which is said to be at the forefront of the Ethiopian government's internet control and censorship strategy and "is known to use spyware and other kinds of software to monitor and censor the online activities of Ethiopian citizens, whether social activists, opposition members or journalists."[9] A proclamation approved by parliament gave the agency wide-ranging powers on the country's computer and information network infrastructures, including an expanded mandate to investigate suspected computers, networks, internet, radio, television and social media broadcasts on platforms like Facebook for any possible damage to the country's social, economic, political and psychological well- being. The proclamation stated that social media outlets, blogs and other internet related media had great capabilities to instigate dispute and war, to damage the country's image and create havoc in the economic atmosphere of the country.[10]

The National Intelligence and Security Service (NISS)[11]: Under the National Intelligence and Security Re-establishment Proclamation of 2013, it is stated that a need had arisen to "strengthen" the NISS "so as to protect and defend the sovereignty of the Federal Democratic Republic of Ethiopia, the constitution and constitutional order." The service has the status of a ministry and reports to the Prime Minister. It is mandated to carry out intelligence work inside and outside of the country, including on terrorism and extremism. Under article 8 (7), the NISS is mandated to conduct surveillance, in accordance with a court warrant, "in order to protect national security and prevent threats to national security" and it does this "by entering into any place and by employing various mechanisms." Under article 27, all persons have duty to cooperate, if requested, in furnishing intelligence or evidence necessary for the work of the NISS. Those requested to provide assistance to the service are required to keep the request confidential.

[6] *Ethio Telecom, Performance Press Release, http://www.ethiotelecom.et/press/news.php?id=74*
[7] *http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx*
[8] *Human Rights Watch, "They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia, March 2014*
[9] *RSF, Ethiopia: full online powers, March 56, 2013; http://12mars.rsf.org/2014-en/2014/03/06/ethiopia-full-online-powers/*
[10] *DireTube, Information Network Security Agency (INSA) of Ethiopia is to be reestablished, Nov 5, 2013; http://www.diretube.com/article.php?keywords=The+Information+Network+Security+Agency+%28INSA%29&btn=Search*
[11] *http://chilot.files.wordpress.com/2013/10/national-intelligence-and-security-service-re-establishment-proclamation-english.pdf*

The Ministry of Information and Communication Technology[12] is mandated with formulating ICT policies and strategies, as well as coordinate their implementation. Developing the use of ICTs in agriculture, industry and commerce, education, and health, is specified. The ministry is also mandated with formulating projects and programs to guide ICT development "with focus on strengthening on-going initiatives in all the sectors aimed at improved service delivery and enhancing good governance."

The Ethiopia Telecommunication Agency[13] is the regulator of the telecoms sector. Founded in 1996, its mission is "To regulate that effective, reliable and affordable telecommunication services are equitably distributed to the entire people in Ethiopia in compliance with the industry standards, and consumer protection is ensured."

Legal and Regulatory Environment

There are a number of laws and policies in Ethiopia that govern internet freedoms. The Telecom Fraud Offence Proclamation No. 761/2012 is one of the more recent legal additions which raised considerable international condemnation while it was under debate in 2012.

The Telecom Fraud Offence Proclamation No. 761/2012[14]: This law came into effect on September 4, 2012 and further entrenches the monopoly of the government-owned telecoms provider while introducing a raft of penalties for those that engage in telecom fraud. The preamble to this law states that telecom fraud "is a serious threat to the national security beyond economic losses," which suggests that in presenting this law, the Ethiopian government was starkly mindful of "security implications", or, put more plainly, the breadth of rights to expression which citizens would enjoy by using ICT.

Under Section 9 of this proclamation, whosoever establishes any telecom infrastructure other than that established by the telecom service provider, or bypasses the telecom service provider's infrastructure and provides "any domestic or international telecom service" can be sentenced to 10-20 years in jail. In addition, they are slapped with a fine equal to ten times the revenue they are estimated to have earned. Users of such services can be incarcerated for between three months and two years. In addition to this, they face a fine of Birr 2,500 to Birr 20,000 (US$134 to US$ 1,070). Activists believe that this section can be used against users of online based services such as Skype and VOIP facilities like Google Talk, which are among the services monitored by the Ethiopian government and also widely used by activists.

In Section 15, the law provides that digital or electronic evidence; evidence gathered through interception or surveillance; and information obtained through interception conducted by foreign law enforcement bodies, are admissible as evidence in court. This would apply to investigations into crimes committed through online mediums.

[12] *Ethiopia Ministry of Communications and Information Technology, http://www.mcit.gov.et/web/english/laws-and-standards-in-the-ict-sector*
[13] *Ethiopian Telecommunication Agency, http://www.eta.gov.et/*
[14] *See http://www.abyssinialaw.com/uploads/761.pdf*

Meanwhile, under Section 6, a 3 to 8 year prison sentence and a fine of Birr 30,000 to Birr 80,000 (US$ 1,500 to US$ 4,100) is prescribed for "whosoever uses or causes the use of any telecom network or apparatus to disseminate any terrorising message connected with a crime punishable under the Anti-Terrorism Proclamation" or an obscene message punishable under the Criminal Code[15]. A number of journalists, bloggers, and democracy activists have been charged and sentenced under the anti-terrorism law.

Section 4 of the telecom fraud law deals with offences related to provision of telecom services. Whosoever provides telecom service without a valid license commits an offence and shall be punishable with imprisonment spanning 7 to 15 years plus a monetary fine. Section 5 deals with offences related to unauthorised access to a telecom network, as well as interception, altering or damaging the contents of telephone calls, data, identification code or any other personal information of subscribers. The punishment is imprisonment of 10 to 15 years plus a fine ranging from Birr 100.000 to Birr 150.000 (US$ 5,200 to US$ 7,700).

The Anti-Terrorism Proclamation No.652/2009[15]: This law came into force in August 2009 and provides in Section 6 under the "encouragement of terrorism" provisions that anyone who publishes a statement "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" can be imprisoned for 10 to 20 years. Those found guilty of committing terrorist acts can be imprisoned for between 15 years and life, or punished by death. Failure to disclose terrorist acts attracts a 3 to 10 year jail term.

The Anti-Terrorism Proclamation authorises interception of communication under Section 14. It states that the National Intelligence and Security Service, upon getting a court warrant, may: a) intercept or conduct surveillance on the telephone, fax, radio, internet, electronic, postal and similar communications of a person suspected of terrorism; b) enter into any premise in secret to enforce the interception; or c) install or remove instruments enabling the interception. Furthermore, communication service providers are required to cooperate when requested by the National Intelligence and Security Service to conduct the interception. Those who fail to cooperate with authorities in interception, and some other offenses listed in this law, can be imprisoned for between three and ten years.

The National ICT Policy of 2009: Chapter One of the National ICT Policy [17] states that apart from being an enabler of socio-economic development, ICT also supports Ethiopia's on-going process of democratisation and good governance. The policy notes, "ICT promotes democratic governance by enabling all citizens to participate in the political process as well as have access to global knowledge and information. Thus, the goal of the government is to ensure that all citizens have equal and equitable access to government services and to knowledge and information." Despite this realisation of the role ICTs can play in promoting citizens' participation in democratic processes, the policy makes no further mention of encouraging citizens' participation in governance through ICTs.

[15] *See http://www.refworld.org/pdfid/49216b572.pdf*
[16] *http://chilot.files.wordpress.com/2011/01/anti-terrorism.pdf*
[17] *See http://www.mcit.gov.et/web/english/the-national-ict-policy*

Internet Freedoms Violations

There are several impediments to the enjoyment of internet freedoms in Ethiopia. This has been the case particularly since the disputed elections of 2005, when the government blocked access to independent websites and social media in the face of protests by the opposition.[18] [19] Since then, blatant and consistent affronts to online freedoms have continued. An extensive study published by Human Rights Watch in 2014 showed that Ethiopian security officials could access the records of all phone calls made inside Ethiopia with few restrictions; and that users' emails and phone recordings had been tendered as evidence against perceived anti-government activists tried under the anti-terrorism law. The government was also using "some of the world's most advanced surveillance software to target key individuals in the diaspora."

At the end of April 2014, the government arrested six bloggers and three journalists, accusing them of working with foreign organisations and rights activists through "using social media to destabilise the country."[20] The bloggers, who are members of a group called Zone 9, that used blogs, Facebook and Twitter, had their website blocked in Ethiopia and were mainly using other Facebook and Twitter. The arrests came days after the group announced plans to rejuvenate its activism.[21]

In September 2012, the OpenNet Initiative (ONI), conducted technical tests of internet filtering which found that Ethiopia continued to block online political and news content, including the blogs and websites of a number of recently convicted journalists and bloggers. Tests conducted between 2008 and 2010 had also found extensive evidence of filtering of political content. In the 2012 tests, it was found that the majority of websites blocked contained content directly related to Ethiopia, including online portals such as Nazret (http://nazret.com), Cyber Ethiopia (http://cyberethiopia.com), and diaspora media such as Toronto based TZTA Ethiopia Newspaper (http://www.tzta.ca). Critical political organisations' websites, including the website of the Solidarity Committee for Ethiopian Political Prisoners (http://www.socepp.de/) and that of the Oromo independence organisation (http://www.oromoliberationfront.org), were also blocked.

[18] *Barry Malone, "VOA Says Ethiopia Blocks Website as US Row Escalates," Reuters, March 29, 2010, http://af.reuters.com/article/topNews/idAFJOE62S0KX20100329?rpc=401&feedType=RSS&feedName=topNews&rpc=401&sp=true.*
[19] *Google Blocked in Ethiopia: http://news.softpedia.com/news/Google-Blocked-In-Ethiopia-53799.shtml*
[20] *Addis Standard, Ethiopia Files Charges Against a Group of Bloggers, Journalists Detained Over the Weekend, http://allafrica.com/stories/201404281454.html*
[21] *See http://zone9ethio.blogspot.com/*
[22] *Update on information controls in Ethiopia, November 1, 2012; https://opennet.net/blog/2012/11/update-information-controls-ethiopia*

Tests conducted by the Citizen Lab from July to August 2013 on Ethionet, and shared with the authors of this report, showed that 62 websites of a test list of 1,412 could not be accessed in Ethiopia.

Table: *Categorised blocked URLs and methods of blocking in Ethiopia (Source: Citizen Lab test lists [23])*

Category	*Category Description*	*Total number tested*	*Number blocked*	*Blocking methods*
Political	Opposition, human rights, freedom of expression, minority rights and religious movements	1412	51	*The websites were blocked using methods difficult to distinguish from network problems including:* • Connection aborted as a result of an injected TCP reset (RST) packet • DNS Error – Resolution process failed • SSL Dropped – Client did not receive Server Hello response during SSL handshake • UNREQ SYN – Client did not receive response to initial SYN during TCP handshake
Social	Sexuality, gambling, illegal drugs and alcohol, and socially sensitive/offensive topics		3	
Conflict & Security	Armed conflicts, border disputes, separatist movements, and militant groups		2	
Internet tools	Web sites that provide e-mail, Internet hosting, search, translation, Voice -over Internet Protocol (VoIP), telephone service, and circumvention methods		6	
	Total	**1412**	62	

In September 2012, Ethiopia passed a law called The Telecom Fraud Offence Proclamation which criminalised the use of Skype and other VoIP services like Google Talk. The use of these services would be punishable by up to 15 years in prison. Authorities said these measures were necessary because of "national security concerns" and the need to protect the monopoly of the sole, state-owned telecommunications/ ISP provider - Ethio Telecom – which has been accused of filtering citizens' internet access to opposition blogs and independent news outlets.

[23] *Citizen Lab, Ethiopia 2013 Testing Results, https://citizenlab.org/2014/04/citizen-lab-collaborates-human-rights-watch-internet-censorship-testing-ethiopia/*

[24] *Frederic Lardinois, Ethiopian Government Bans Skype, Google Talk And All Other VoIP Services, http://techcrunch.com/2012/06/14/ethiopian-government-bans-skype-google-talk-and-all-other-voip-services/*

In June 2012, award-winning Ethiopian journalist and blogger Eskinder Nega was convicted on charges of "terrorist acts", "encouragement of terrorism", and "high treason" for allegedly attempting to spark an Arab spring-style revolt in the country. Many other journalists and human rights activists were also found guilty in absentia, including Abebe Gellaw of the online news platform Addis Voice, and Mesfin Negash and Abiye Teklemariam, both editors of Addis Neger Online.[25] In May 2013, the Supreme Court upheld the conviction and 18-year prison sentence for Nega.[26] Nega was accused of conspiring with Ginbot 7, an oppositional political group labelled a terrorist organisation by the Ethiopian government. Up to 150 websites were reportedly blocked in Ethiopia, including those owned by independent news organisations, political parties, bloggers, and international organisations such as Human Rights Watch and the Committee to Protect Journalists.[27] In March 2013, Ethiopia was accused of blocking the Arabic and English language websites of Al Jazeera, after the network aired programmes on protests in the country.[28]

Studies during May 2012 showed that the Tor Network anonymising tool was blocked and the government had deployed deep-packet inspection technology. Furthermore, internet scans conducted in 2013 by the Citizen Lab discovered a campaign using FinFisher in Ethiopia to target individuals linked to an opposition group. It was found that the FinSpy campaign in Ethiopia used pictures of Ginbot 7, an Ethiopian opposition group, as bait to infect users. This gave strong suggestions that the Ethiopian government was using FinSpy.[29]

In February 2014, an American citizen of Ethiopian origin living in Maryland sued the Ethiopian government for infecting his computer with secret spyware, wire-tapping his private Skype calls, and monitoring his entire family's every use of the computer for months. Represented by the Electronic Frontier Foundation (EFF), 'Mr. Kidane' alleged that the Ethiopian government intruded into his communications in an attempt to gather information on members of the Ethiopian diaspora who criticised the Addis Ababa regime. Forensic examination of his computer showed that it had been infected when he opened a Microsoft Word document stealthily sent by agents of the Ethiopian government, which that contained hidden surveillance malware FinSpy.[30]

In addition, tests conducted by Freedom House found that by April 2013, 70 websites related to news and opinion, 16 websites belonging to different Ethiopian political parties, 40 blogs, seven multimedia websites, and 40 Facebook pages were not accessible in Ethiopia.[31] According to Freedom House's State of the Net 2013 report, Ethiopia's centralised backbone made internet access highly vulnerable to widespread service disruptions at the hands of the authorities.

In July 2012, internet and mobile phone text messaging speeds were reported to be extremely slow amid a series of uprisings by Ethiopian Muslims in protest against alleged religious discrimination by the government. It was also during this time that some

[25] *David Smith, Blow to press freedom as Ethiopia convicts 24 of plotting rebellion, June 28, 2012, The Guardian.*
[26] *Rainey Reitman, In Violation of Constitution, Ethiopian Blogger Will Face 18 Years in Prison, May 2, 2013; https://www.eff.org/deeplinks/2013/05/violation-constitution-ethiopian-blogger-will-face-18-years-prison*
[27] *IMF.org and Economist.com Joined the Long List of Blocked Websites in Ethiopia, June 27, 2012; http://ethsat.com/2012/06/26/imf-org-and-economist-com-joined-the-long-list-of-blocked-website-in-ethiopia/*
[28] *Ethiopia 'blocks' Al Jazeera websites; http://www.aljazeera.com/news/africa/2013/03/201331793613725182.html; accessed on March 19, 2013*
[29] *https://citizenlab.org/tag/finfisher/ http://www.huffingtonpost.com/2013/03/13/finspy-spyware-activists_n_2864579.html http://www.networkworld.com/news/2013/031413-finfisher-spyware-seen-targeting-victims-267693.html*
[30] *Electronic Frontier Foundation, American Sues Ethiopian Government for Spyware Infection, February 18, 2014, https://www.eff.org/press/releases/american-sues-ethiopian-government-spyware-infection*
[31] *47 Independent tests conducted by Freedom House consultant, early 2013.*

individuals complained that text messages took days, even weeks, to reach their recipients.[32] International news outlets have become increasingly targeted for censorship. Al Arabiya and both of Al Jazeera's Arabic and English websites were both blocked intermittently throughout 2012 and early 2013, while the Washington Post became a new target for blocking after the paper reported on Prime Minister Meles Zenawi's whereabouts in August 2012.[33] At the time, Zenawi had not been seen in public for several weeks due to ill health and government suppressed discussions about his whereabouts and state of health. He died in August 2012. This article remained blocked as of April 2014.

An online Forbes article titled, "Requiem for a Reprobate Ethiopian Tyrant Should Not Be Lionized", which was written in response to the local and global praise of the late Prime Minister's debatable economic growth achievements, was also blocked in Ethiopia in August 2012 and remained so at the time of writing, according to Freedom House's State of the Net report for 2013. In addition, some restrictions are placed on the effective use of mobile phones, such as the requirement for a text message to obtain prior approval from Ethio Telecom if it is to be sent to more than ten recipients. A bulk text message sent without prior approval is automatically blocked.[34]

In October 2012, Jemal Kedir, 32, was found guilty of "rumour-mongering" and handed a one-year jail term. Federal prosecutors charged that messages he sent through his SMS were intended to "provoke dissension, arouse hatred against the government, or stir up acts of violence or political, racial or religious disturbances." [35]

Recommendations

Ethiopia should amend The Anti-Terrorism Law 2009 [for example Sections 6 and 14], The Telecom Fraud Law 2012 [Sections4, 5, 6, 9, 15] and the NISS Re-establishment Proclamation 2013 [Article 27, Article 8 (7)] as they all detract from the rights of citizens and contradict the constitution. The revisions should extend the space for free expression by citizens without fear of reprisals from state authorities or non-state actors. Amendments should lower the powers of state organs in monitoring and investigating journalists and bloggers and lower the penalties. Further the Telecom Fraud law in Ethiopia should be amended to allow free use of services such as VOIP.

Definitions of what constitutes terrorism need to be narrowed down so they do not include citizens, journalists and bloggers that are expressing legitimate opinion both offline and online. The amendments should also include judicial oversights over surveillance, including guidelines to be used in accessing individual's data, monitoring the communications, and under what circumstances evidence gathered under conditions that flout laid-down regulations may be rejected by courts of law.

[32] *Freedom of the Net 2013; and "Ethiopian Authorities Crack Down on Muslim Press," Committee to Protect Journalists, August 9, 2012, http://www.cpj.org/2012/08/ethiopian-authorities-crack-down-on-muslim-press.php.*
[33] *Mohammed Ademo, "Media Restrictions Tighten in Ethiopia," Columbia Journalism Review, August 13, 2012, http://www.cjr.org/behind_the_news/ethiopia_news_crackdown.php?page=all.*
[34] *Freedom House, Freedom On The Net 2013- Ethiopia*
[35] *Liya Terefe, Ethiopian man jailed for one year for inciting public disorder using text messages, http://sodere.com/profiles/blogs/ethiopian-man-jailed-for-one-year-for-inciting-public-disorder*

The Ethiopian telecommunications sector should be liberalised to promote pluralism and diversity and so that users have increased options and better services. Having a single provider also bodes negatively for users' privacy since a centralised backbone and internet exchange makes it easier for the state to filter, monitor, and block internet access.

Civil society - including activists, media, bloggers, academia and other progressive elements need skills training in online safety and online ethics.

This report was produced by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) under the Open Net Africa initiative (www.opennetafrica.org) which monitors and promotes internet freedoms in a number of African countries including Ethiopia, Kenya, Rwanda, Burundi, Tanzania, Uganda and South Africa. As part of the project, we are documenting internet rights violations, reviewing cyber security policies and how they affect internet freedoms, promoting information availability and conducting awareness-raising.

The production of this report was supported by the Humanist Institute for Co-operation with Developing Countries (Hivos), the Citizen Lab at the University of Toronto and the Canadian International Development Research Centre (IDRC).

Collaboration on International ICT Policy in East and Southern Africa (CIPESA)
156-158 Mutesa II Road, 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