Cautious Optimism in Ethiopia's Cyberspace

By Arthur Gwagwa
Sub-Saharan Africa Cyber Threat Modelling
Funded by the Open Technology Fund: https://www.opentech.fund/
Published by the Global South Initiative (GSI) www.globalsouthinitiative.com
September, 30, 2018

Introduction

This brief report examines internet censorship in Ethiopia following the new government's policy shift towards the respect for freedom of expression including online activity. It is based on fieldwork which I conducted in Addis Ababa from July 9-13, 2018 under the Sub-Saharan Africa Cyber Threat Modelling Project. It also builds on my two previous country analyses which can be accessed here and here. During my fieldwork in Addis, I deployed the Open Observatory for Network Interference (OONI) software to test the accessibility of websites and messaging apps, both of which were previously known to have been blocked based on **OONI's network measurement data**. I also manually tested these sites and in addition, interviewed internet users from a wide cross section, including the Zone 9 Bloggers, journalists, government officials, academics and technologists.

Key Findings

- WhatsApp and Telegram were consistently inaccessible on WIFI connected devices, save if accessed through a virtual private network (VPN).
- WhatsApp and Telegram were largely accessible on most occasions on mobile data but inaccessible on a few occasions and users had to use VPN
- Despite a few false positives, all major media outlets, political and human rights websites were accessible.
- The circumvention tools websites such as torproject.org and Psiphon were sometimes inaccessible due to generic timeout errors but accessible when we ran further tests on 20 July 2018.
- Internet users, especially those at risk, detected censorship through news, government announcements and word of mouth and not through technical data science projects such as OONI software. We brought some of these tools to their attention.
- The prolonged shutdowns in Ethiopia resulted in some bloggers losing their accounts due to a number of factors such as a lack of subscription, fatigue, self-censorship. Consequently, the recovery of this work may be a lengthy process.
- Although the internet infrastructure is now unblocked, filtering and throttling may persist and sometimes controls may be tactful and disguised as technical problems.
- The online discussions may not lead to any substantive offline action as the discussions may continue to be moderated: through self-censorship, acculturalisation and fear. Users, who are in this type of situation, need encouragement and solidarity from the global civil society who can support them by establishing a genuine connection directly linking them to the international internet freedom community.
- The Ethiopian Internet governance needs reform which include the repeal of the laws of the current telecommunications infrastructure, ownership and control.
- During the week of 8 August, the national government shut down broadband and mobile internet in the cities of Harar and Dire Dawa and the whole Somali region of Ethiopia which went without access to the internet for four days. This followed growing tensions between the national and regional governments in the Somali region of Ethiopia. Again, on September 17, Ethio Telecom shut down mobile internet networks across the capital city, Addis Ababa, in response to deadly land rights protests.

Main Report

Instant Messaging

We ran both OONI and manual tests on WhatsApp, Telegram and Facebook Messenger. WhatsApp and Telegram were consistently blocked when directly accessed through WIFI connected devices but were accessible through VPN. Access through mobile data was inconsistent and different users provided different and often conflicting accounts of their experiences.

Technical Measurement details: OONIprobe android, software version “1.3.2”428.95s runtime, location ET (AS24757) on WIFI from 9-13 July. The test displayed evidence of possible censorship: the WhatsApp application appeared to be blocked, WhatsApp web appeared to be working properly (WhatsApp web status ok), the WhatsApp registration service appeared to be blocked (WhatsApp endpoints blocked), and there were no WhatsApp endpoints DNS inconsistencies.

Fig 1: WhatsApp was consistently blocked when accessed through WIFI connected devices

Rationalising the inconsistencies

One interviewee said the inconsistencies may be a result of how mobile data works differently from WIFI (ASDN). A group of interviewees thought that probably the government opened the mobile data ports but forgot to open the ASDN ports. This is not the first time this has occurred, for example, for some time, Instagram worked on data via VPN but directly on WIFI.

However, in our view, given INSA's immense censorship experience, it is both improbable and incredible that they forgot to address the anomaly but is probably one way they are gradually and cautiously opening up space, starting with websites while still maintaining some sort of control over messaging apps.

Social media such as Facebook have also been unblocked but the government has maintained moderate control over WhatsApp and Telegram, given their ability to change the quality of the online discourse. The role of social media in civic participation and governments' attempts to censor it is well documented in the Berkman Klein Centre, 2017 and Quartz, 2018 Reports. WhatsApp's increasing role to influence politics in Africa has been highlighted in the same Quartz Report on Zimbabwe.

Websites Connectivity

We ran tests and also manually tested several previously blocked media outlets, human rights, LGBTI and political opposition and armed groups, examples of which are listed below. All sites worked consistently. However, LGBTI site http.www.glil.org and site https//www.3wishes.com appeared to be blocked. They were also not accessible on PC when we tried to open them. However, they were easily accessible through an Android mobile device. What therefore appeared to be cases of blocking might just have been false positives probably caused by firewalls or filters. Some political opposition websites such as Oromo Media and Ginbot were also not accessible via PC but accessible via mobile devices. Probably, in our view, since INSA registers all mobile devices, it is easy to access websites via mobile phones as this gives INSA the ability to monitor such devices.

Circumvention tools

AS pointed out in the previous OONI Report, circumvention sites such as the torproject.org were inaccessible but easily accessible via opera VPN but accessible sometimes especially, when opened through a mobile device. Further tests over time are still needed to come to a firm conclusion.

Websites tested

Media outlets
https://ecadforum.com/
https://mereja.com/index/
http://www.ethioforum.org

Human rights and LGBTI
www.hrw.org
https://amnesty.org.
http://www.cyberethiopia.com/
http://www.samesexmarriage.ca/
www.glil.org

Political opposition and armed groups
http://www.eprp.com
http://www.onlf.org
http://www.ginbot7.org

Middle boxes

We ran tests for Http header field manipulation and for the HTTP invalid request line. The results showed that everything was okay. However, this does not confirm the absence of middle boxes, given their pervasive use in the past, this may only confirm that they were not in use when we ran the tests.

Network Performance

This included dash streaming and NDT Speed test on ET (AS24757). The results showed download speed of 1.77 mbit/s; upload speed of 4.38 mbit/s and Ping-262.0 ms. Dash streaming did not run due to errors

Censorship Detection Tools Awareness Raising

During our interviews we sought to ascertain how activists are able to identify whether websites are blocked or not and one of the Zone 9 bloggers said, “We knew that the government was blocking websites, first, as sites failed when you tried to log onto them, and second, we share stories within the media community on which websites are working or aren’t working.”

The activists had started keeping an eye on the websites from 22 June 2018, when the government announced it would unblock 264 websites.

“Although there are a few lists of unblocked sites circulating, the government never published a comprehensive list of the unblocked sites. Despite not having a full current list of unblocked websites, we can verify the unblocking because no one in our community and beyond is reporting that my blog or website is blocked as we used to” (Zone 9 Blogger).

We then explained how the OONI probe can improve and assist to verify which sites were still blocked and which ones weren’t.

However, average internet users were aware of the Psiphon circumvention tool and one in two interviewees had used it and other tools to circumvent social media blockages.

Consequences of internet controls

Permanent loss of websites and social media accounts.

However, one consequence of the sustained blockades is that some, if not most people gave up on their websites and blogs. “If you don’t have visitors to your blog here in Addis Ababa, there is no need to maintain the blog. You give up because of the censorship; most of them stopped paying hosting fees and the site hosts simply took the sites down” (Hailu)

“We also lost our social media accounts, for example, Twitter accounts, during the internet shutdowns that occurred during the successive states of emergency. Twitter has an elaborate verification process for one to recover their account” (Zone 9 blogger). Most users who lost their accounts were not prepared to or weren’t able to go through this verification process. From a technical point of view, when ones use VPN to access the account, VPN changes one’s country, Twitter asks for one’s country and if the applicant enters ‘Ethiopia’ while they are virtually logged from a peered server in another country, the verification process fails. Loss of accounts collaterally impacted on free speech. To give an example, Samuel Getachew, a prominent journalist who was responsible for breaking the latest news on his Twitter was also affected. This also included Belay Manaye and Abraham Desta, member of Arena opposition group from the Tigri region who had his Twitter account locked.

The New York-based Access Now helped journalists to recover their accounts, including helping the Zone 9 Bloggers when they left prison. A good example is Fekadu Hailu. When he was jailed, the police forced him to surrender his social media passwords, he immediately instructed his friend to notify Facebook and Twitter to disable the accounts to prevent an illegal access by the state. After prison, he requested Access Now to help him recover the accounts.

Intercept evidence in criminal trials.

“The state had started monitoring our blogs and phones and used our telephone conversations as evidence in court, for instance, the Zone 9 blogs were blocked within two weeks of creating them. As a matter of public record, I was jailed 4 times from April 2014-October 2015 on account of my online activism and criticism directed against the government. We were only acquitted as the state witnesses could not corroborate the evidence upon which it relied” (Zone 9 Blogger).

The Future

Most of the interviewees' views on the country's status quo reflect the views of those in exile whom we also interviewed in May-June, 2018.

They see the future to be promising, for example, before 2015 the government blocked the internet throughout the country but since 2016, they have just been blocking in Addis Ababa but kept the internet on in the Oromo region which had previously been rocked by protests.

Also, there is less self-crsnorship as Ethiopians have since started openly discussing sensitive issues without fear. To support this, we carried out most of the interviews in open hotel lobbies and cafes and some of the bloggers had no problem to have their names cited in the report other than the judge who felt being cited would affect his job.

However, a former government official was cautious, "Ethiopians talk in groups but don't do so in the street or protest".

Despite the reforms, in a way, basic controls will remain. An official who works in the DNS section of Ethio Telecoms said, "Ethio Telecoms will continue filtering for other reasons because filtering and throttling have always been there before pervasive surveillance." Yet another one said, "In future, just like in the past, the blocking may be done tactically as the government may just say that the internet is down." In our view, these controls are usually applied 'just in time' as temporary disconnections or event-based denial of selected content or services. These techniques can be difficult to verify, as they can be made to look like technical errors applied in ways that assure plausible deniability.

The views on tactful censorship agree with those of the Ethiopians whom we interviewed in Washington, especially that the government will not dismantle its surveillance capabilities but instead redirect it to genuine cases of national security in future.

At the moment, INSA and ETHIO Telecoms are in one compound. INSA registers all new phones' IMEI and regulates the integrated system.

Further another threat emanates from both Ethio Telecoms and INSA employees including those with decision-making powers who do not support the prime minister's current reforms. According to an Ethio Telecoms worker, "I don't think the current blocking is government sanctioned, as these people still hold power in some agencies e.g. the PM had to fire the director of INSA, and he poses the strongest opposition to the PM. These people even once blocked the PM's cell phone."

Political reforms

The current general political and ethnic reforms are the major impetus behind the government's policy shift on censorship and surveillance practices. It is important to understand Ethiopia's ethnic and political landscape in order to appreciate the broader reforms and their impact on future censorship.

The former Prime Minister, Meles Zenawi, was from the south. Many people perceive him to have been mostly controlled by the Tigrayan People's Liberation Front (TPLF) and were seen as their puppet which is why he had to resign.

The new prime minister of the Oromo Liberation Front (OLF) has a strong backing of most Oromia dissidents, such as Jawar Mohammed, Neamin Zekele, Mohamed Ademo, Henok Kabisa, and Eskinder Negar most of whom have been the subjects of targeted threats, based on various grounds including ethnicity. The Oromo constitute the largest ethnic group. Although there have been previous OLF leaders, they did not get support from the Oromo dissidents as these leaders were controlled by TPLF, a member of the ruling EPRDF.

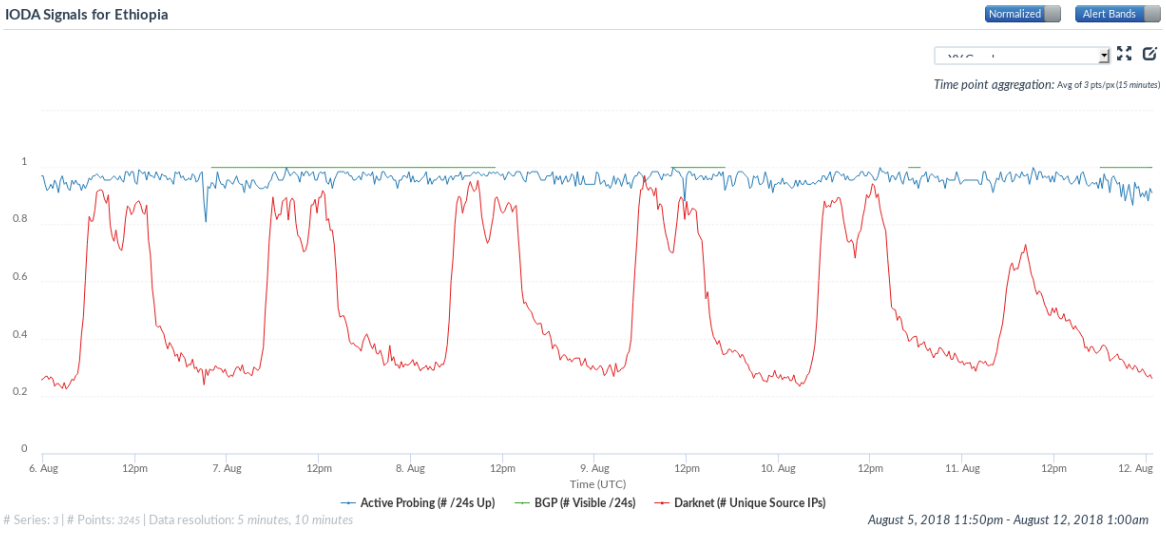
If the new prime minister didn't have the power he wouldn't have been able to delist groups previously listed as terrorist organisations such as the OLF and Ginbot 7. That's why he is supported by all.

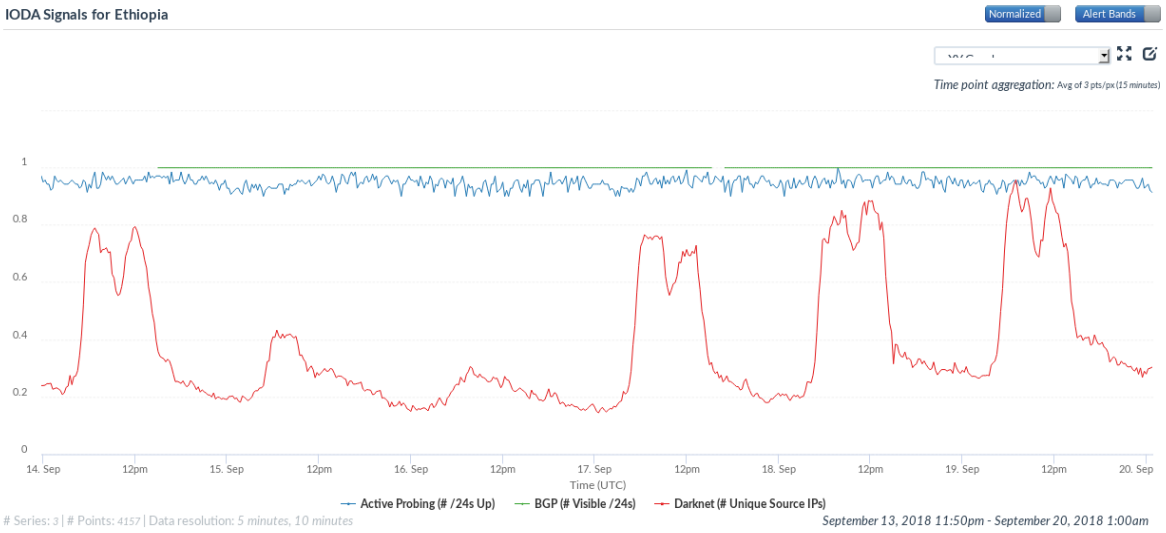
Also, his technology background, as is the former director of INSA, ironically makes him appreciate internet freedom. He realises one can't control people, internet users can use encryption, can also just hop platforms, and that government's huge support base is not on social media since it's mostly rural.

Current developments

During the week of 8 August, the government's commitment to reforms and in particular its efforts to re-direct its cyber capabilities should serve legitimate national interests was tested as the national government shut down broadband and mobile internet in the cities of Harar and Dire Dawa and the whole Somali region of Ethiopia which went without access to the internet for four days. This followed growing tensions between the national and regional governments in the Somali region of Ethiopia. According to our country source, Befekadu Hailu, the federal government cut off the internet to suppress imminent violence when the national government was trying to arrest the president for the regional government of Somali which prompted the supporter of President Abdi Mohammed Omer (AKA Abdi Illey) to violently attempt to stop it. Whether cutting off the internet was a necessary and proportionate response to the imminent violence is debatable. Access Now's statement," the government's actions this past weekend show that Ethiopia still has a long way to go to protect freedom of expression and access to information in the country. The lack of transparency around the decision to cut off the internet and the deafening silence from the Ministry of Communications and Information Technology (MCIT) and Ethio-Telecom continue to make shutdown incidents in Ethiopia a mystery". Again, on September 17, Ethio Telecom shut down mobile internet networks across the capital city, Addis Ababa, in what appeared to be an effort to quell social unrest. The protests led to the deaths of at least20 people were rooted in ethnic conflict and the administration of land rights policies.

Below: IODA Data on the August and September 2018 Internet Disruptions. However, the data does not show significant disruptions that could have affected the
entire country.





Recommendations

The government should continue implementing measures that would ensure a free flow of information, including the right to impart and receive information. This should include removing hurdles that hinder the free and regular flow of daily and peaceful activities. One such practical step would be to make all instant messaging apps fully accessible regardless of the means of connection.

Amend or repeal all legislation that criminalises the exercise of freedom of expression, including online speech. One practical step from such an amendment should include:

- Fully re-directing the state's cyber capabilities towards the development of its digital society, economy and fending the country from real threats
- Institute a robust accountability and transparency oversight mechanism over its intelligence-gathering programme. This should involve a reform to the current internet governance regime, for example ending the monopoly and split the services of both agencies.
- The government and its agencies should invest in and encourage local content and an active digital society. At the same time, the government should allow the global civil society to work within Ethiopia to support and encourage the civic tech space to have a more critical view on technology, inclusion, economy and democracy since a vibrant digital society is good both for democracy and the digital economy.
- In order to sustain the gains in the tech space, the government should continue on a path of political reform in a manner that acknowledges Ethiopia's ethnic diversity, promotes tolerance and cohesion and seek sustainable solution to ethnic tensions.
- Address the issue of protests in accordance with international law and in circumstances where this may lead to the curtailment of freedom of expression including online; state's response should be proportionate and comply with its international obligations including the International Covenant on Civil and Political Rights.