Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**299**
Land:	Etiopien
Kilde:	Amnesty International
Titel:	Ethiopia Offline – Evidence of Social Media Blocking and Internet Censorship in Ethiopia.
Udgivet:	14. december 2016
Optaget på baggrundsmaterialet:	2. januar 2017

ETHIOPIA OFFLINE

EVIDENCE OF SOCIAL MEDIA BLOCKING AND INTERNET CENSORSHIP IN ETHIOPIA

OONI

AMNESTY INTERNATIONAL

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

ABOUT OONI

The Open Observatory of Network Interference (OONI) is a free software project under the Tor Project that aims to increase transparency of internet censorship around the world. We aim to empower groups and individuals around the world with data that can serve as evidence of internet censorship events.

Since late 2012, our users and partners around the world have contributed to the collection of millions of network measurements, shedding light on multiple instances of censorship, surveillance, and traffic manipulation on the internet.

We are independent of any government, political ideology, economic interest or religion.

First published in 2016
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: AFR 25/5312/2016
Original language: English

amnesty.org

Cover photo: *Youth in Addis trying to get Wi-Fi Connection.*
©Addis Fortune

OONI

AMNESTY INTERNATIONAL

CONTENTS

EXECUTIVE SUMMARY

Waves of protests against the government have taken place across various parts of Ethiopia since November 2015. These protests have consistently been quashed by Ethiopian security forces using excessive, sometimes lethal, force, which led to scores of injuries and deaths. The crackdown on protests was accompanied by increasingly severe restrictions on access to information and communications in large parts of the country by cutting off internet access, slowing down connections and blocking social media websites.

The protests began on 12 November 2015 in Ginchi, a town in West Shewa Zone of Oromia Region, against the Addis Ababa Masterplan, a government plan to extend the capital Addis Ababa's administrative control into parts of Oromia. The protests continued even after the Government announced in January that they had cancelled the plans, and later expanded into the Amhara region with demands for an end to arbitrary arrests and ethnic marginalization.

Amnesty International's research since the protests began revealed that security forces responded with excessive and lethal force in their efforts to quell the protests. Amnesty International interviewed at least fifty victims and witnesses of human rights abuses during the protests, twenty human rights monitors, activists and legal practitioners within Ethiopia, and also reviewed other relevant primary and secondary information on the protests and the government's response. Based on this research, the organisation estimates that at least 800 people have been killed since the protests began.

Tensions in Oromia escalated at the beginning of October, following a stampede during a religious festival which killed at least 55 people. Fresh protests, some of which turned violent, broke out amidst contestations over who was responsible for the stampede. Oromo activists blamed security forces for firing live ammunition and tear gas into the crowds, while the government blamed anti-peace protestors. The government of Ethiopia declared a state of emergency on 8 October. The state of emergency imposes broad restrictions on a range of human rights, some of which are non-derogable rights, meaning that under international law, they may never be restricted, even during a state of emergency.

In addition to using security forces to quash protests, the Ethiopian authorities have restricted access to internet services during this time. Amnesty International's contacts inside Ethiopia reported that social media and messaging mobile applications such as Facebook, WhatsApp and Twitter, have been largely inaccessible since early March 2016, especially in the Oromia region where the bulk of the protests were taking place. Internet services were also completely blocked in Amhara, Addis Ababa and Oromia Regions following a call by political activists for region-wide protests on the weekend of 6 and 7 August 2016. The protests went ahead during these two days. The government security forces used excessive force against the protesters in Addis Ababa, Amhara and Oromia Regions resulting in the death of at least 100 people.

Internet disruptions started again on 5 October 2016 after protesters in some parts of Oromia targeted businesses, investments, government buildings and security forces in the wake of the stampede during the Irrecha thanksgiving festival in Oromo. Amnesty International's contacts have since reported that internet connections were very slow and social media services have been inaccessible through browsers. Access to the mobile internet connection in Addis Ababa improved for a couple of days in early December, on 4th and 5th, before becoming inaccessible once again.

The Ethiopian government considers that social media has empowered populists and extremists to exploit people's genuine concerns and to spread bigotry and hate. This position was made clear in the Prime Minister's speech to the UN General Assembly in September. Indeed, a number of political and other activists have been arrested and charged under the Anti-Terrorism Proclamation on the basis of their activities on social media platforms. Yonatan Tesfaye, formerly of the Blue Party, was arrested and charged with terrorism crimes because of his Facebook posts criticizing government policy and action.

In the midst of these protests, and in response to the numerous reports from Ethiopia that access to the internet was being blocked, the Open Observatory of Network Interference (OONI) performed a study of internet censorship. OONI is a free software project whose goal is to increase transparency about internet censorship and traffic manipulation around the world. OONI undertook the study in order to assess whether, and to what extent the censorship being reported actually occurred during the protests. OONI sought evidence of websites and instant messaging apps were being blocked; systems causing censorship and traffic manipulation; and inaccessibility of censorship circumvention tools such as Tor and Psiphon.

OONI's software tests were run from a computer inside the country (running on the EthioNet network, the Ethiopia telecom monopoly). Tests were run on a total of 1,403 different URLs, including both Ethiopian and global websites, in order to determine website blocking. Additional OONI tests were run to examine whether systems that could be responsible for censorship, surveillance, and traffic manipulation were present in the tested network. OONI then processed and analysed the network data collected based on a set of criteria for detecting internet censorship and traffic manipulation. The testing period started on 15 June 2016 and concluded on 7 October 2016, immediately prior to the announcement of the state of emergency.

This report, presents the findings of the OONI study, and Amnesty International's human rights analysis of these findings. This report also provides details of the technical methodology OONI used to verify the blockade on WhatsApp and the restrictions on websites with political and other content in a second, distinct section.

KEY FINDINGS

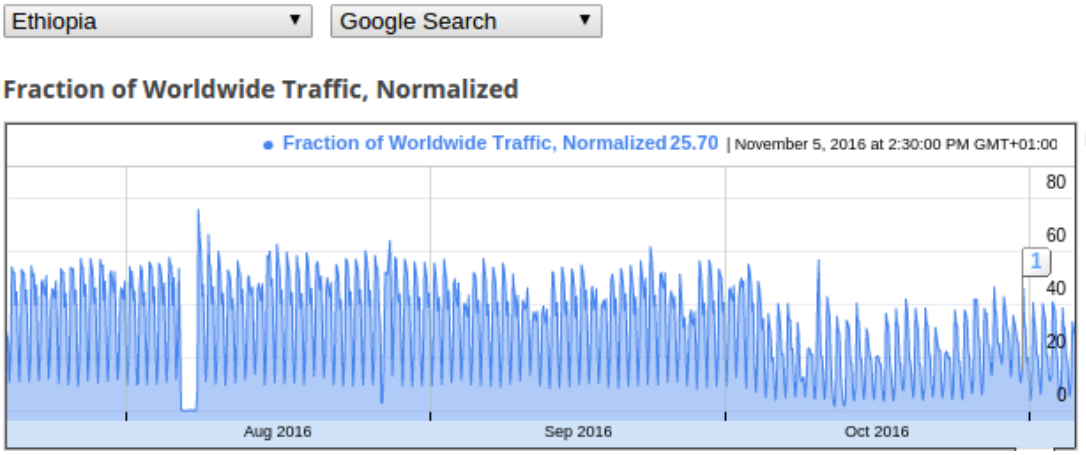
New OONI data published in this report reveals the following:

- WhatsApp was found to be blocked inside Ethiopia
- Deep Packet Inspection (DPI) technology was detected. DPI is a technology that can be bought and deployed on any network, enabling monitoring and filtering of Internet traffic. This can be useful as part of network management, but it can also be used for mass surveillance and internet censorship. This finding suggests that Ethiopia has DPI technology in its possession and is deploying it for censorship purposes inside the country.
- Out of 1,403 different types of URLs that were tested, the types of sites that consistently presented network anomalies and which were more likely to be blocked include:
    - News outlets and online forums
    - Armed groups and political opposition websites
    - LGBTI websites
    - Websites advocating free expression
    - Circumvention tool websites (including Tor and Psiphon)

The above types of websites mostly presented connection (HTTP response) failures, indicating that they were likely blocked by DPI equipment. Overall, 16 different Ethiopian news outlets presented signs of censorship, many of which showed evidence of being blocked prior to the state of emergency declaration.

In the course of this investigation, OONI also sought to verify reports from Ethiopia of a mobile internet shutdown in October 2016. OONI software tests are designed to examine the blocking of sites and services, but do not monitor internet shutdowns as a whole. As such, the organisation referred to third party data such as Network Diagnostic Test (NDT) measurements and Google transparency reports, in an attempt to examine whether the reported internet shutdown could be confirmed.

The below graph from Google's transparency reports illustrates the total volume of Google Search traffic originating from Ethiopia between July and November 2016. As published in an earlier report by OONI and Strathmore University Centre for Intellectual Property and Information Technology Law (CIPIT), the data shows a complete drop in internet traffic in early August, suggesting that a full internet block took place following the call by political activists for region-wide protests on the weekend of 5 and 6 August. While the data shows a decrease in internet traffic during October, there is no strong indication of an internet shutdown along the lines of that observed in early August.



The findings suggest that if an internet shutdown did occur in October, it only occurred in some networks in certain locations, rather than nationwide. Furthermore, the decrease in overall traffic during October could be attributed to temporary mobile internet shutdowns in certain local networks, or to an increase of censorship events (for example, targeted blocking of certain websites and instant messaging services). An examination of data from the circumvention software Tor, shows a spike in traffic from Ethiopia in October, suggesting that more people were seeking ways around censorship. This indicates that there might have been an increase in censorship events following the declaration of Ethiopia's state of emergency.

OONI was unable to confirm the reported mobile internet shutdown in October, partly due to limitations in NDT measurements and Google transparency reports. We therefore strongly encourage internet companies including Facebook, Microsoft, Yahoo and Twitter, to increase transparency around internet traffic data so that internet shutdowns and other censorship events can be investigated and verified quickly, and more accurately.

Many of these acts of censorship took place before the state of emergency was announced, raising questions about whether these measures had any basis in Ethiopian law, as required by international human rights law. While the state of emergency may have subsequently provided a legal framework under Ethiopian law for some of these measures, the state of emergency itself is so broadly drafted that it violates Ethiopia's international legal obligations and permits violations of numerous human rights. Amnesty International and OONI are concerned that unnecessary and disproportionate censorship of the internet will not only continue during the state of emergency, but become institutionalized and entrenched.

OONI has unearthed evidence of systematic interference with access to numerous websites belonging to independent news organizations and political opposition groups, as well as sites supporting freedom of expression and LGBTI rights. Such widespread interference and blocking is a violation of people's freedom of expression, and specifically, people's right to hold opinions without interference, and their right to receive and impart information of all kinds as guaranteed under article 19 (1) and (2) of the International Covenant on Civil and Political Rights (ICCPR), which Ethiopia has ratified.

Ethiopia's position on the use of social media indicates that the authorities are invoking their obligations to restrict freedom of expression where such freedom is abused, as articulated in article 19 (3) of the ICCPR. However, the acts of censorship uncovered by OONI's study are inconsistent with the requirements laid out in the ICCPR to restrict these rights. Specifically, that any restrictions will be provided by law and are necessary to respect the rights or reputations of others; or for the protection of national security or of public order, public health or morals. Any restrictions to freedom of expression is subject to a three part test: that they are legal; necessary and proportional. The acts of censorship evidenced in OONI's study fail to meet the test. They are arbitrary, being carried out in the absence of clear and precise law in the country which governs access to internet and social media, restrictions/blockade of websites and social media, and clear legal procedures governing restrictions, including administrative and judicial procedures to challenge such restrictions and blockades. The acts of censorship also fail the test of proportionality. The censorship acts uncovered by OONI were not restricted to specific content; rather the censorship was happening at a large scale, with dozens of websites and popular communications platforms like WhatsApp affected over the space of several months.

The decision to restrict people's ability to receive and impart information by censoring internet access during the protests, only served to sweep the underlying issues fuelling the protests under the carpet. To fully address the situation that led up to the state of emergency, the government must genuinely commit to addressing the underlying human rights violations that triggered the protests in the first place; and respect its

human rights obligations. This includes refraining from blocking access to the internet and ensuring that all its people can enjoy their right to express their opinions; even those who criticise government policy and action; and guarantee their right to expression and association online and offline.

Social media companies should make available publicly verifiable data on network traffic originating from countries around the world, to ensure transparency when social media restrictions or heavy network disruptions occur.

METHODOLOGY

This report has two distinct sections. Part 1 of the report presents Amnesty International and OONI´s joint findings related to internet censorship during the protests that have rocked Ethiopia since November 2015. Part 2 of the report provides a detailed overview of OONI´s technical study, including the full range of tests performed on Ethiopia´s network and acknowledged limitations in the methodology.

Amnesty International has been documenting the protests since they began, as well as the state response to the same. Primarily, Amnesty International has conducted this research remotely, relying on victim and eyewitness testimony, which has been taken through at least 50 phone and email interviews. Amnesty International researchers have also used a variety of other primary and secondary information to corroborate and verify witness accounts of specific incidents including at least 20 phone and email interviews with human rights monitors in Ethiopia; members of Ethiopian political opposition parties including spokespersons; media reports; reports and images posted on social media; and Ethiopian government communications. Amnesty International has tried unsuccessfully on two separate occasions to engage with the Ethiopian authorities on the protests.

The information gathered by Amnesty International and used in this report, is to provide the background, and context within which the OONI network measurement study was carried out. It is not intended to provide comprehensive information on the human rights violations that have occurred in the context of the protests. For more information and analysis on the protests, please visit Amnesty International's website.

The Open Observatory of Network Interference (OONI) is a free software project that aims to increase transparency about internet censorship and traffic manipulation around the world. OONI undertook a network measurement study, which run from 15 June to 7 October 2016. OONI used multiple free and open source software tests it had designed to examine the following:

Blocking of websites and instant messaging apps.

Detection of systems responsible for censorship and traffic manipulation.

Reachability of circumvention tools (such as Tor, Psiphon, and Lantern) and sensitive domains.

It is important to note that the technical findings are subject to limitations, and do not necessarily reflect a comprehensive view of internet censorship in Ethiopia. The methodology, and its limitations, are discussed in detail in part 2 of the report.

1. PART 1: EVIDENCE OF INTERNET CENSORSHIP

1.1 BACKGROUND: SUSTAINED PROTESTS

Despite the lack of confirmed data about casualties, an estimated 800 people have been killed due to excessive or otherwise unlawful use of force by the security forces – some of which may amount to extrajudicial executions – since the beginning of the protests in November 2015.[1] The United Nations High Commissioner for Human Rights has described[2] the situation as "*extremely alarming*" and urged Ethiopia to allow international human rights observers into the country. The Ethiopian government, however, rejected[3] this UN request, arguing that it alone is responsible for the security of its citizens.

There have been almost continuous protests in parts of Ethiopia since November 2015. The protests in Oromia region were initially triggered by plans to extend the capital, Addis Ababa, into Oromia, but continued even after the Addis Ababa Masterplan was scrapped in January, evolving into demands for accountability for human rights violations, ethnic equality and the release of political prisoners.

In August 2016, people in the Amhara Region joined protests against arbitrary detention of members of the Wolkait Amhara Identity and Self-determination Committee. The Ethiopian security forces have consistently used excessive, including lethal, force to disperse the protesters.[4] Over 600 protesters in Oromia and 200 in Amhara have been killed as a result. Hundreds of political activists, human rights defenders, journalists and protesters have been arrested. Since the start of the protests in November last year, the police have charged at least 200 people, including journalists, bloggers and opposition political party leaders, under the Anti-Terrorism Proclamation. Their trials were ongoing as of November 2016.

Tensions in Oromia escalated again following a stampede during the Irrecha religious festival on 2 October that resulted in the death of at least 55 people.[5] The cause of the stampede, and the number of casualties, is contested. The government has claimed that protesters triggered the stampede, while Oromo activists claim that the government security forces caused the stampede when they fired tear gas canisters and shot live ammunition into the crowds. Following the stampede, fresh protests broke out in Oromia with a number of them turning violent. Protesters attacked foreign and local businesses, farms, and vehicles, especially those near Addis Ababa.

In response to the wave of protests, the government of Ethiopia severely restricted internet access and declared a state of emergency on 8 October 2016.[6] The state of emergency imposes broad restrictions on a

[1] Amnesty International, Ethiopia: Reform Only Feasible Way out of Mounting Crisis, 18 October 2016, (Ref: AFR 25/5003/2016).
[2] The Guardian, UN demands Ethiopia admit observers amid reports dozens killed in protests, available at https://www.theguardian.com/world/2016/aug/11/un-ethiopia-observers-reports-dozens-dead-protests (last viewed on 6 December 2016).
[3] Aljazeera, Ethiopia says UN observers not needed as protests rage, http://www.aljazeera.com/news/2016/08/ethiopia-observers-needed-protests-rage-160811105846673.html (last viewed on 6 December 2016).
[4] Amnesty International, Ethiopia: Reform Only Feasible Way out of Mounting Crisis, 18 October 2016, (Ref: AFR 25/5003/2016).
[5] Amnesty International, Ethiopia: Reform Only Feasible Way out of Mounting Crisis, 18 October 2016, (Ref: AFR 25/5003/2016).
[6] Amnesty International, Ethiopia: Reform Only Feasible Way out of Mounting Crisis, 18 October 2016, (Ref: AFR 25/5003/2016).

variety of human rights, some of which are non-derogable rights, meaning that under international law, they may never be restricted, even during a state of emergency.[7] The arrest and detention of protesters and politically-outspoken individuals critical of government action continues, including Zone-9 bloggers Natnael Feleke on 4 October and Befeqadu Hailu on 11 November. The government forces also arrested Anania Sorri and Daniel Shibeshi (members of former Unity Party) and Elias Gebru (journalist) on 18 November 2016. The three of them had posted their picture showing the protest sign on 28 October 2016.[8]

The Government of Ethiopia continues to accuse the Ethiopian diaspora based opposition political parties, Egypt and Eritrea for supporting and fostering the protests.[9]

1.2 INTERNET CENSORSHIP DURING PROTESTS

Testimonies gathered by Amnesty International from different parts of the Oromia region indicate that social media mobile applications such as Facebook, WhatsApp, and Twitter, were largely inaccessible since early March 2016, especially in the Oromia region, where residents were waging protests against the government since November 2015.

"… You can't use social media apps across Oromia for the last 6 weeks [since Mid-March]. I personally checked it in Ambo town in West Shawa Zone and In Batu/Ziway in East Shawa Zone and all [along] the road to there. The blackout is directed to the apps [both Android and IOS] but, the whole internet is too slow and not working at all in some parts of the Region."

Moreover, the witnesses Amnesty International spoke to in the Oromia region and neighbouring cities, such as Hawassa, said that not only are the popular social media applications largely inaccessible, but that the internet has also been rendered unusually slow.

"All the way to Hawassa from Addis Ababa, I was not able to access Skype and Facebook. Even after I reached Hawassa, the connection was too slow that I was not able to have decent Skype conversation during the night."

The Government blocked access to Facebook, Instagram, Twitter and Viber during the National University Exam week "to prevent students being distracted from studying during the exam period and to prevent the spread of false rumours"[10]. Accordingly, those social media outlets were reportedly inaccessible throughout the country from 9-14 July 2016.

Internet services were also reportedly[11] not available in Amhara, Addis Ababa and Oromia Regions following the call for region-wide protests on the weekend of 6 and 7 August 2016. During these two days, the government used excessive, including lethal force against protesters in Addis Ababa, Amhara and Oromia Regions resulting in the death of at least 100 people.

Social media and mobile internet was also reportedly[12] unavailable from 5 October 2016 after protests in some parts of Oromia targeted businesses, investments, government buildings and security forces, during a proclaimed "week of rage".

In addition, the government employed legislative and judicial tools to discourage the use of internet and social media for expression of dissenting views. The government passed a new computer crimes law in June 2016[13] that among other things penalises distribution of "violent messages, audio, or video." The law also authorizes the Ministry of Justice to issue a warrant for interception or surveillance, and people suspected of computer crimes can be held in pre-trial detention for up to four months. The law has had a chilling effect on the flow of information about human rights violations perpetrated by the security forces against protesters.

---

[7] Human Rights Watch, Legal Analysis of Ethiopia's State of Emergency, available at https://www.hrw.org/news/2016/10/30/legal-analysis-ethiopias-state-emergency (last viewed on 9 December 2016), 30 October 2016.
[8] Article 1 of the Directive for the implementation of the state of emergency declaration prohibits "Any communication that will create misunderstanding between people or unrest" including "…signs".
[9] BBC, Ethiopia blames Egypt and Eritrea over unrest, available at http://www.bbc.com/news/world-africa-37607751 (last viewed on 23 November 2016).
[10] Aljazeera, Ethiopia blocks social media sites over exam leak, available at: http://www.aljazeera.com/news/2016/07/ethiopia-blocks-social-media-sites-exam-leak-160711183939642.html, and http://www.bbc.com/news/world-africa-36763572 (last viewed on 8 December 2016).
[11] BBC: What is behind Ethiopia's wave of protests? Available at http://www.bbc.com/news/world-africa-36940906 (last viewed on 22 November 2016).
[12] Africa News, Ethiopia partially lifts internet shutdown amid protest tension, available at http://www.africanews.com/2016/10/05/ethiopia-partially-lifts-internet-shutdown-amid-protest-tension/ (last viewed on 22 November 2016), and BBC, available at http://www.bbc.com/news/live/world-africa-37390903 (last viewed on 23 November 2016).
[13] Computer Crimes Proclamation, Ethiopian Broadcast Corporation, Ethiopian Parliament approves cyber-crime Proclamation, available at http://www.ebc.et/web/ennews/-/parliament-approves-cyber-crime-proclamation (last viewed on 23 November 2016).

The Ethiopian government has relied on the Anti-terrorism Proclamation (ATP) to charge and convict people who have criticized government policy and action on social media platforms. The Ethiopian Government arrested and charged Yonatan Tesfaye[14], a political activist and former public relation head of the Blue Party, with terrorism crimes under the ATP because of the content of his posts on Facebook. The Zone-9 bloggers[15] and Zelalem Workalemahu et al[16] were also tried because of their online activities. The prosecutor charged the Zone-9 bloggers with terrorism crimes for using encrypted software to ensure the security of their communications. In Zelalem Workalemahu et al the court convicted the first defendant, Zelalem Workalemahu, for provision of training on online encryption methods.[17]

The Ethiopian Prime Minister's speech at the United Nations General Assembly in September 2016, gave an indication of the government's views around the use of social media: "social media has certainly empowered populists and other extremists to exploit people's genuine concerns and spread their message of hate and bigotry without any inhibition."[18]

It is unlikely that social media played a crucial role in mobilizing the protests, given that internet penetration in the country remains very low at 2.9%. However, it has aided protesters in uncovering acts of violence committed by the security forces. Previous protests in the country, such as the April 2014 Oromo Protest[19] against the Addis Ababa Master Plan and the Muslim protest[20] against government interference in religious affairs since 2012 did not attract international media coverage. However, the current protests in Oromia and Amhara Regional States have gained a relatively greater media coverage due to the use of social media, even in very small towns, where witnesses have reported on events and the violence committed by the security forces, sometimes in real-time.[21] For instance, the footage from the Irrecha tragedy on 2 October 2016 was available on social media platforms almost in real time.[22]

Google traffic data[23] depicts an acute decline of traffic on 6 and 7 August 2016, when there was a call by political activists for protests in Addis Ababa, Oromia, and Amhara. The internet shutdown tallied with the heavy-handed response of the security forces to the protests on these dates. Since social media was not accessible on those days in Amhara, Oromia and Addis Ababa there were very little reports at the time of the violence by the security forces. It was only after 8 August 2016 that pictures, footage, and reports of excessive force by security forces started to emerge on social media.

[14] *Federal Public Prosecutor Vs Yonatan Tesfaye Regassa*, Charge, F/P/P 414/08, 04 May 2016.
[15] Federal Public Prosecutor v Soliyana Shimelis et al, Federal High Court Judgement, C/F/No. 155040.
[16] Federal Public Prosecutor v Zelalem Werq-Agenyehu et al, Verdict, C/F/No 158194.
[17] Freedom House, Freedom on the Net 2016, available at https://freedomhouse.org/report/freedom-net/2016/ethiopia (last viewed on 07 December 2016).
[18] http://www.un.org/apps/news/story.asp?NewsID=55022#.WBrYUC197IV (last viewed on 8 December 2016).
[19] Amnesty International, Because I am Oromo: Sweeping repression in the Oromia region of Ethiopia (Ref: AFR 25/006/2014)
[20] Amnesty International, Ethiopia: widespread violations feared in clampdown on Muslim protests, (Ref: AFR 25/010/2012)
[21] Examples include http://europe.newsweek.com/oromo-protests-why-ethiopias-biggest-ethnic-group-demonstrating-430793?rm=eu, and https://www.theguardian.com/world/2015/dec/11/ethiopia-protests-master-plan-addis-ababa-students. The hashtag for the Oromia protest was also running since the start of the protest in Oromia: https://twitter.com/hashtag/oromoprotests?lang=en
[22] Facebook and Twitter were commonly used social media networks to report the protests and the violence the security forces were committing. Moreover, diaspora based television and internet media such as the Oromia Media Network (OMN) and Ethiopian Satellite Television (ESAT) were able to cover the protests on daily basis.
[23] Fully detailed in Section 1.3.4.

STATE OF EMERGENCY

Ethiopia is currently in a *state of emergency* for six months, as announced by the government on 8 October 2016.

The Government has arrested more than 11,000 people for "violence and property damage."[24] Among those in detention are bloggers, journalists, and members of the political opposition, for publicly criticizing the government, the state of emergency declaration or for posting the protest sign[25] on Facebook.

Under the state of emergency, all unauthorized protests and assemblies are banned. Sharing information about protests through social media platforms, such as Facebook and Twitter, is prohibited, while two TV stations run for the Ethiopian diaspora, ESAT and the Oromia Media Network, are banned due to their coverage of the protests.

The state of emergency declaration imposes broad derogations on a variety of human rights, some of which affect non-derogable rights according to Article 4 (3) of the International Covenant on Civil and Political Rights (ICCPR).[26] The state of emergency declaration established a Command Post chaired by the Prime Minister with the power to determine the specific restrictions, measures, and geographic scope in the implementation of the state of emergency.

The Command Post has broad powers, including to:

- Prohibit any overt or covert incitement for violence or ethnic conflict, in whatever form of expression;
- Stop or suspend any media;
- Prohibit any assembly, association and demonstration;
- Arrest anyone suspected of using violence in the areas the Command Post identifies. Those arrested will be educated and released and, if necessary, they will be punished under relevant law;
- Search and seize any person or place and confiscate where necessary;
- Impose curfew;
- Block any road or public place or evacuate and move people from certain places;
- Evacuate people vulnerable to threats and keep them in safe places for a limited period of time;
- Use proportionate force necessary for the implementation of the state of emergency;
- Suspension of substantive and procedural laws of the country.

Accordingly, the Command Post issued a Directive on 15th October, which further enumerated the acts prohibited, the state of emergency measures, and the obligations to keep and communicate records.[27] The directive conferred the security forces with the powers to:

- Arrest without warrant;
- Detain those arrested at places designated by the Command Post until the end of the state of emergency;
- Search without warrant anytime and anywhere;
- Monitor and control any messages through radio, TV, articles, pictures, photographs, theatre and movies.

Sources told Amnesty International that[28] the security forces have demolished a number of private satellite frequency receivers in the Oromia and Amhara regions, barring access to the broadcasts of the Ethiopian Satellite Television and Oromia Media Network. Several witnesses have also told Amnesty International that they were unable to access mobile internet service in Oromia, Addis Ababa, and Amhara Regional States resulting in information blackout on the human rights situation in those regions. However, it is not clear why the mobile internet remains unavailable.

[24] http://www.fanabc.com/english/index.php/news/item/7370-inquiry-board-says-11,-607-people-arrested-under-emergency-law (last viewed on 8 December 2016).

[25] The protesters have been showing hands crossed over their head as a sign of protest. The sign has attracted media attention when the Ethiopian Athlete displayed it when crossing the finish line during the 2016 Rio Olympic.

[26] Amnesty International, Ethiopia: Reform Only Feasible Way out of Mounting Crisis, 18 October 2016, (Ref: AFR 25/5003/2016)

[27] http://www.fanabc.com/index.php/component/k2/item/19458 (last viewed on 8 December 2016).

1.3 FINDINGS OF THE NETWORK MEASUREMENT STUDY

The Open Observatory of Network Interference (OONI) performed a study of internet censorship in Ethiopia in the midst of tensions and ongoing public protests in Oromia region, and prior to the announcement of the country's state of emergency. The aim of this study was to understand whether and to what extent the censorship being reported actually occurred during the protests, and to provide evidence in relation to:

- Blocking of websites and instant messaging apps.
- Detection of systems responsible for censorship and traffic manipulation.
- Reachability of common circumvention tools used to get around censorship (such as Tor and Psiphon).

OONI's software tests were run from an OONI probe running from a computer inside the country (running on the EthioNet network, the Ethiopia telecom monopoly). Tests were run on a total of 1,403 different URLs, including Ethiopian websites as well as URLs that are commonly accessed around the world. All URLs were tested for blocking. Other OONI tests were run to examine whether systems that could be responsible for censorship, surveillance, and traffic manipulation were present in the tested network. OONI processed and analyzed the network measurement data collected from these tests based on a set of formula for detecting internet censorship and traffic manipulation.

The testing period started on 15 June 2016 and concluded on 7 October, immediately prior to the announcement of the state of emergency. The testing was also limited due to security risks to people involved in conducting the testing. Even though Ethio Telecom is government owned and Ethiopia's main ISP, it is likely that censorship was implemented differently across locations, and that the findings of this study do not necessarily represent nationwide censorship. A detailed explanation of the methodology, including limitations, can be found in part 2 of this report.

1.3.1 WHATSAPP BLOCKED

OONI has designed a new software test for examining the reachability of WhatsApp.

This test attempts to perform an HTTP GET request, TCP connection and DNS lookup to WhatsApp's endpoints, registration service and web version over the vantage point of the user. Based on this methodology, WhatsApp's app is likely blocked if TCP/IP connections to its endpoints and/or registration service fail; if the DNS lookup illustrates that different IP addresses have been allocated to its endpoints; and/or if HTTP requests do not send back a response to OONI's servers. Similarly, WhatsApp's website is likely blocked if any of the above apply to web.whatsapp.com.

In October, OONI ran a new software test for examining the reachability of WhatsApp. This test was ran from a local vantage point in Ethiopia (Ethio Telecom) in an attempt to examine whether and how WhatsApp was censored. The collected measurement data illustrates that while both HTTP and HTTPS requests to web.whatsapp.com succeeded, HTTPS requests to WhatsApp's registration service failed, and so did TCP connections to WhatsApp's endpoints. This indicates that WhatsApp's website was accessible, but its *app* was blocked.

	WEB.WHATSAPP.COM	WHATSAPP ENDPOINTS	WHATSAPP REGISTRATION SERVICE
HTTP REQUEST	Success	-	-
HTTPS REQUEST	Success	-	Failed
TCP CONNECTION	-	Failed	-
DNS LOOKUP	Consistent	Consistent	Consistent

	WEB.WHATSAPP.COM	WHATSAPP ENDPOINTS	WHATSAPP REGISTRATION SERVICE
RESULT	Accessible	Blocked	Blocked

1.3.2 DEEP PACKET INSPECTION DETECTION

An Ethiopian news website (ecadforum.com) was found to be blocked in October based on the use of Deep Packet Inspection (DPI) technology. DPI enables its users to analyze data packets and protocols. This can be useful as part of network management, but it can also be used for data mining and internet censorship.

The blocking of ecadforum.com by DPI equipment was uncovered through OONI's HTTP host test which was run from a local vantage point in Ethiopia. This test attempts to examine whether the domain names of websites are blocked, and to detect the presence of "middle boxes" (software that could potentially be used for censorship and/or traffic manipulation) in tested networks.

As part of OONI's testing, we performed HTTP requests towards one of OONI's control servers. This server sends back any data it receives. In absence of censorship equipment, we would be able to view ooniprobe's request. But when we sent the HTTP host header containing the domain "ecadforum.com" to our control server, we noticed that the connections would get *reset*. We were only able to receive the control response when requesting a subdomain of "ecadforum.com" and when we prefixed the request method (GET) with the newline character. This is summarized in the table below:

	ECADFORUM.COM
NORMAL GET REQUEST	Blocked
MODIFIED GET REQUEST	Not blocked
GET REQUEST TO SUBDOMAIN	Not blocked
GET REQUEST TO DOMAIN + \T (TAB CHARACTER)	Not blocked
GET REQUEST TO XYZECADFORUM.COMZYX	Not blocked

This leads us to conclude that the devices implementing this type of interception were in fact "smart" enough to understand the HTTP protocol and could only implement blocking when they found the request to match what they expected to be "valid" HTTP. Therefore, DPI equipment was most likely present in the tested network and used to implement censorship.

1.3.3 WEBSITES BLOCKED

MEDIA OUTLETS

Ethiopia's state of emergency imposes restrictions on media. Yet, as part of our study numerous Ethiopian news outlets presented signs of DNS, HTTP, and TCP/IP blocking after the state of emergency declaration. (See part 2 of this report for the full methodology).

The table below illustrates the amount and types of network anomalies detected when testing such sites.

TESTED WEBSITES	DNS	HTTP-DIFF	HTTP-FAILURE	TCP/IP	ANOMALIES
HTTP://ECADFORUM.COM/	2	0	13	0	15
HTTPS://MEREJA.COM	0	2	8	0	10
HTTP://MEREJA.COM	0	0	10	0	10
HTTP://ZEHABESHA.COM/	1	0	8	0	9
HTTP://ETHIOMEDIA.COM	0	0	8	0	8
HTTP://ETHSAT.COM	0	0	8	0	8
HTTP://ETHIOPIANREVIEW.COM	0	0	8	0	8
HTTP://WWW.ETHIOPIANREVIEW.COM	0	0	7	0	7
HTTP://WWW.ETHIOMEDIA.COM/INDEX.HTML	0	0	7	0	7
HTTP://WWW.ETHIOFORUM.ORG	0	0	7	0	7
HTTP://WWW.QUATERO.NET	0	0	7	0	7
HTTP://WWW.GOOLGULE.COM	1	0	6	0	7
HTTP://WWW.OGADEN.COM	0	0	7	0	7
HTTP://OROMIAMEDIA.ORG/	0	0	2	4	6
HTTP://WWW.DEBTERAW.COM	0	0	6	0	6
HTTP://WWW.NAZRET.COM	0	0	6	0	6
HTTP://WWW.TZTA.CA/TZTA/ENGLISH.HTM	0	0	5	0	5
HTTP://WWW.TZTA.CA	0	0	5	0	5
HTTPS://WWW.OROMIAMEDIA.ORG/	0	0	0	4	4
HTTP://WWW.SATENAW.COM/	0	0	3	0	3
HTTPS://OROMIAMEDIA.ORG/	0	0	0	3	3
HTTP://WWW.SATENAW.COM/AMHARIC/	0	0	3	0	3
HTTP://NAZRET.COM	0	0	3	0	3
HTTP://WWW.ETHIOPIANREPORTER.COM	0	3	0	0	3

In some cases, we tested different versions of the *same* sites to examine whether censorship could potentially be circumvented. We tested various versions of certain sites, such as both the HTTP and HTTPS versions of oromiamedia.org. In all such cases however, access to these sites presented signs of network interference, as illustrated in the table above.

Overall, 16 different Ethiopian news outlets presented signs of censorship. As no block pages were detected, we cannot confirm any censorship events with absolute certainty. However, the sites that presented the

highest amount of network anomalies are more likely to have actually been blocked, while those with fewer network anomalies are less likely to have been tampered with. As such, ecadforum.com – with the highest amount of network anomalies – was most likely blocked by DPI equipment (as explained previously), while access to it might have also been interfered with based on DNS tampering. On the other hand, sites which presented fewer cases of network anomalies (such as satenaw.com) are less likely to have been blocked, though this remains a possibility.

In any case, it was interesting to see that out of the 1,403 different URLs (1,217 URLs in the "global list" and 186 URLs in the "Ethiopian list") that were tested for censorship as part of this study, access to these 16 Ethiopian news outlets presented the highest levels of network anomalies, indicating that they were most likely tampered with. These sites include oromiamedia.org, a diaspora based media enterprise that reports mainly on Oromia, one of the main regions that has been at the heart of the protests and civil unrest in 2016.

The restrictions imposed under the state of emergency include a ban on access to the ethsat.com news outlet. This website, which is run by the Ethiopian diaspora, aims to "promote free press, democracy, respect for human rights and the rule of law in Ethiopia" and also publishes in Amharic. However, we tested access to this site prior to Ethiopia's state of emergency declaration and our findings show that it presented many network anomalies. As with ecadforum.com, access to ethsat.com presented high levels of HTTP interference, indicating that it might have also been blocked by DPI equipment *before* it was even officially banned.

An Amharic online forum (mereja.com) also presented high levels of HTTP interference, and was possibly blocked by DPI as well. While it's likely that news sites have been blocked in order to restrict dissemination of information around the protests, the potential blocking of an Amharic forum might be to block communication, coordination and information dissemination amongst Amharic protesters.

POLITICAL OPPOSITION AND ARMED GROUPS

As part of our study we found the websites of Ethiopian armed groups and political opposition groups to be tampered with. In the case of those related to armed groups espousing violent opposition to the Ethiopian government, censorship may fall within the permissible restrictions to freedom of expression under international human rights law.[29]

The table below summarizes our findings:

Tested websites	DNS	HTTP-diff	HTTP-failure	TCP/IP	Anomalies
http://ginbot7.org/	1	0	8	0	9
http://www.eprp.com	0	0	7	0	7
http://www.eppf.net	0	0	7	0	7
http://www.onlf.org	0	0	7	0	7
http://www.oromoliberationfront.org	0	0	7	0	7
http://patriotg7.org/	1	0	4	0	5

Ginbot 7 is a national political party and part of Ethiopia's political opposition. In 2009 the Ethiopian government accused Ginbot 7 of fostering a coup attempt to overthrow the government, which Ginbot 7 denied.[30] Ginbot 7 is one of the proscribed organizations under the Anti-Terrorism Proclamation[31], which is potentially why ginbot7.org was blocked. Through our testing we found that access to this website presented a high amount of network anomalies. In September 2016 we tested ginbot7.org by sending multiple HTTP GET requests to access the site. In all cases however, we never received a response.

[29] ICCPR Art 20 (1).
[30] Ginbot-7, Press release, available at https://web.archive.org/web/20120418222418/http:/www.ginbot7.org/Ginbot_7_PressRelease_25_April_2009.htm (last viewed on 8 December 2016).
[31] Freedom House, Freedom in the World 2012, available at https://freedomhouse.org/report/freedom-world/2012/ethiopia (last viewed on 6 December 2016).

The Ethiopian People's Revolutionary Party (EPRP) is a national political party which was founded by the Ethiopian diaspora and which is currently headquartered in the United States. During the 1970s Ethiopia's then military government declared open war ("Red Terror" campaign)[32] against the EPRP and other political opponents, resulting in the death of around 250,000 Ethiopians. Similar to ginbot7.org, we found eprp.com inaccessible due to HTTP response failures as part of our testing.

The Oromo Liberation Front (OLF) is a regional political party that was established by Oromo nationalists in the early 1970s to promote self-determination, and which was designated[33] as a "terrorist organization" by Ethiopia's government. The Ethiopian People's Patriotic Front (EPPF) is an armed opposition group in north western Ethiopia that was originally founded to overthrow the EPRDF regime. As part of our testing, the websites of both groups appeared to be inaccessible due to HTTP response failures.

Similarly, the websites of two armed opposition groups, the Ogaden National Liberation Front (ONLF) and the Patriotic Ginbot 7 Movement for Unity and Democracy, also presented HTTP response failures as part of our testing. The ONLF is a separatist armed group that is fighting for the independence of the Ogaden region in eastern Ethiopia, bordering with Somalia. An Ogaden news website was also found to be inaccessible, as illustrated in the table of the previous section of this report.

LGBTI WEBSITES

As part of OONI's testing, access to sites supporting LGBTI rights appeared to be tampered with since we did not receive HTTP responses when querying them. These sites, and our research findings, are included in the table below:

Tested websites	DNS	HTTP-diff	HTTP-failure	TCP/IP	Anomalies
http://www.queernet.org	1	0	3	0	4
http://www.samesexmarriage.ca	0	0	4	0	4
http://www.ifge.org	0	0	4	0	4

The International Foundation for Gender Education (IFGE) is a US-based educational organization that promotes acceptance for transgender people, while samesexmarriage.ca is a Canadian site that promotes same-sex marriage. QueerNet is a project of the Online Policy Group (a non-profit dedicated to online policy research around digital rights issues) which provides free online services (such as email hosting, websites, and mailing lists) for LGBTI communities.

Same-sex sexual activity is prohibited in Ethiopia under Article 629 of the Criminal Code[34] punishable up to fifteen years imprisonment. All three websites appeared to be inaccessible in September 2016, but appeared to be accessible when tested again in early October 2016.

HUMAN RIGHTS WEBSITES

Two sites promoting freedom of speech and expression also presented signs of network anomalies as part of our study.

Tested websites	DNS	HTTP-diff	HTTP-failure	TCP/IP	Anomalies
http://www.cyberethiopia.com	0	0	5	0	5
http://www.cyberethiopia.com/warka4/	0	0	5	0	5

[32] Red Terror Martyrs' Memorial Museum, http://rtmmm.org/
[33] Freedom House, Freedom in the World 2012, available at https://freedomhouse.org/report/freedom-world/2012/ethiopia (last viewed on 6 December 2016).
[34] The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation No.414/2004.

http://www.fepproject.org	0	0	0	3	3

Cyber Ethiopia is a Swiss-based non-profit organization that aims to promote human rights in Ethiopia through programs and policy recommendations that uphold freedom of speech and expression online. The Free Expression Policy Project is a think tank on artistic and intellectual freedom. It provides research and advocacy on free speech, copyright, and media democracy issues.

When querying cyberethiopia.com, we did *not* receive an HTTP response, indicating that access to the site was blocked. Our results regarding fepproject.org are different. When testing the site in June and October 2016, we were able to successfully connect to it. However, all attempts to establish TCP connections to the site during August and September 2016 failed and presented timeout errors. It remains unclear if fepproject.org was intentionally blocked throughout August and September 2016 based on TCP/IP blocking, or if connections to the site failed due to transient network failures.

CENSORSHIP CIRCUMVENTION WEBSITES

Amongst the many sites that presented HTTP response failures are the sites of major censorship circumvention tools: Tor and Psiphon.

Tested websites	DNS	HTTP-diff	HTTP-failure	TCP/IP	Anomalies
http://www.psiphon.ca	0	0	7	0	7
http://www.ultrasurf.us	0	0	7	0	7
http://www.torproject.org	0	0	7	0	7
https://ultrasurf.us	1	0	4	0	5
http://ultrasurf.us	0	0	5	0	5
http://psiphon.ca	0	0	5	0	5

Tor is a free and open source network designed to provide anonymity to its users by bouncing their communications across a distributed network of relays, thus masking their real IP addresses and enabling them to circumvent censorship. Psiphon is free and open source software that utilizes SSH, VPN, and HTTP proxy technology to enable its users to circumvent censorship. Ultrasurf is freeware that utilizes an HTTP proxy server to enable its users to bypass censorship.

Both torproject.org and ultrasurf.us appeared to be inaccessible between June and October 2016 due to HTTP response failures, while psiphon.ca presented the same failures from August 2016 onwards. The fact that all three sites presented HTTP response failures and that http://ultrasurf.us, https://ultrasurf.us and http://psiphon.ca appeared to be slightly more accessible than http://www.ultrasurf.us and http://www.psiphon.ca indicate the presence of Deep Packet Inspection (DPI) equipment in the tested network (as explained in the DPI section of this report).

While toproject.org was found to be inaccessible, we did not find Tor software itself being blocked in Ethiopia during the testing period.

PRACTICAL TOOLS TO CIRCUMVENT UNLAWFUL CENSORSHIP IN ETHIOPIA

Organizations and companies hosting websites that may be blocked in Ethiopia can consider hosting their websites on a Tor hidden service to hide its IP address and prevent blocking. It is also recommended to add HTTPS to your site through Let's Encrypt.

Individuals seeking to access blocked websites, may consider using the below circumvention tools and services to get around blocks. **Note:** under Anti-terrorism Proclamation, use of digital security tools have been used in the past to prosecute bloggers and activists, even if there is no provision of law that outlaws use of internet security tools, including tor. Yet It is vital that you understand the security risks in accessing such tools.

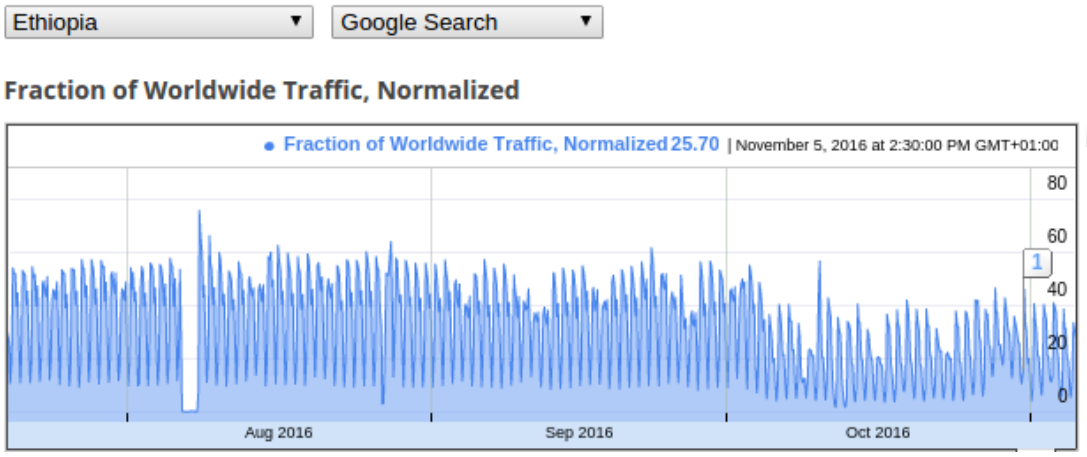
- Use Tor Browser (or other circumvention tools) to circumvent censorship and access blocked sites.
- If torproject.org is blocked, download Tor Browser here.
- If the Tor network is blocked, get Tor bridges to circumvent the blocking and connect to it.
- Use the VPN mode of Orbot to access WhatsApp (and other IM apps) on Android over the Tor network.

1.3.4 INTERNET SHUTDOWN

Numerous reports surfaced in October regarding a mobile internet shutdown in Ethiopia[35], and this was also reported to Amnesty International by contacts on the ground.

OONI software tests are designed to examine the blocking of sites and services, but do not monitor internet shutdowns as a whole. As such, we referred to third party data such as NDT measurements and Google transparency reports in order to assess whether we could confirm the reported internet shutdown.

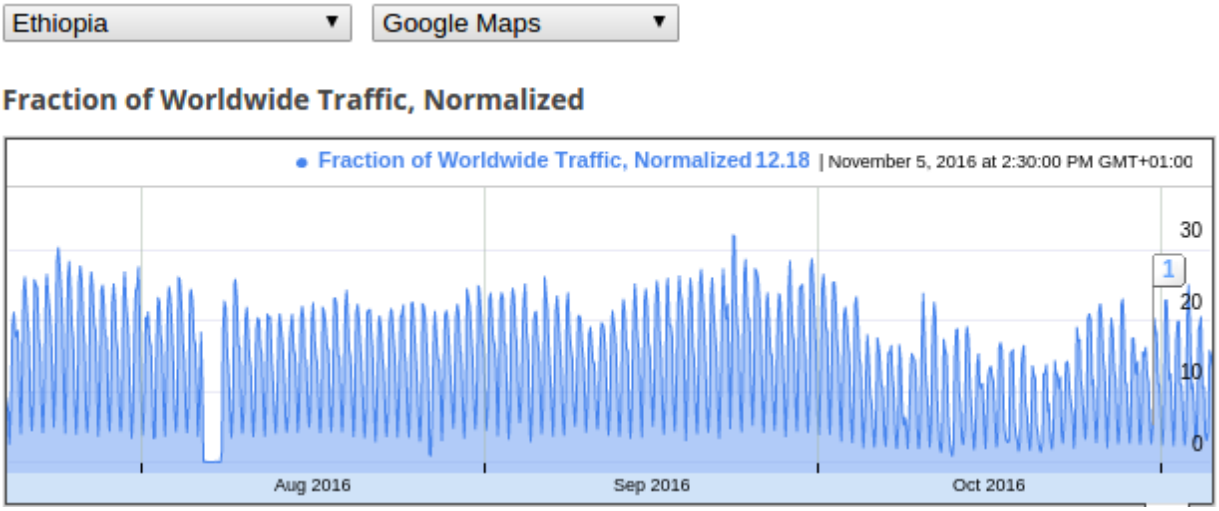
The below graph from Google's transparency reports illustrates the total volume of Google Search traffic originating from Ethiopia between July and November 2016. As published in an earlier report by OONI, the data shows a complete drop in Internet traffic in early August, suggesting that a full Internet block took place following the call for region-wide protests on the weekend of 5 and 6 August. While the data shows a decrease in internet traffic during October, there is no strong indication of an internet shutdown along the lines of that observed in early August.



Google Transparency Report, Ethiopia, Google Search traffic between July and November 2016.

As Google Maps is another Google service that is commonly used via mobile phones, we also looked at Google Maps traffic originating from Ethiopia between July and November 2016.

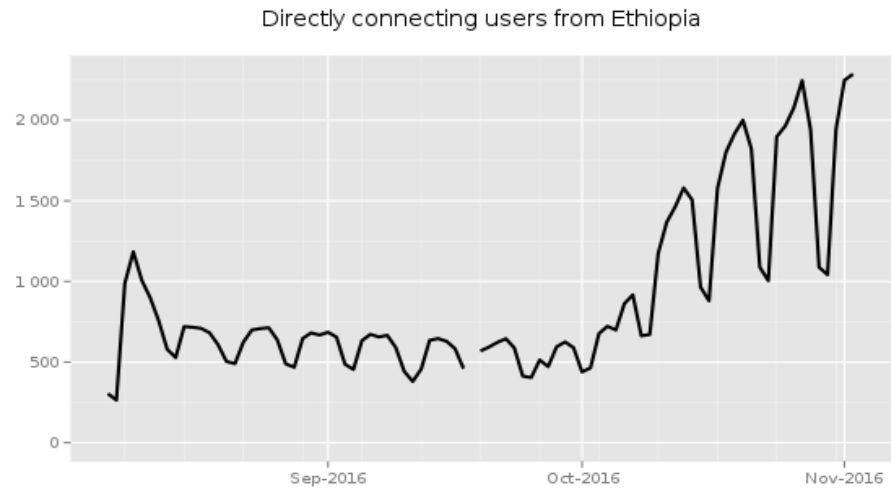
[35] Freedom House, Freedom on the Net 2016, available at https://freedomhouse.org/report/freedom-net/2016/ethiopia (last viewed on 07 December 2016). See also Al Jazeera, Oromo protests: Ethiopia unrest resurges after stampede, available at http://www.aljazeera.com/news/2016/10/ethiopia-protests-resurge-stampede-deaths-161006044616074.html (last viewed on 07 December 2016).



Google Transparency Report, Ethiopia, Google Maps traffic between July and November 2016.

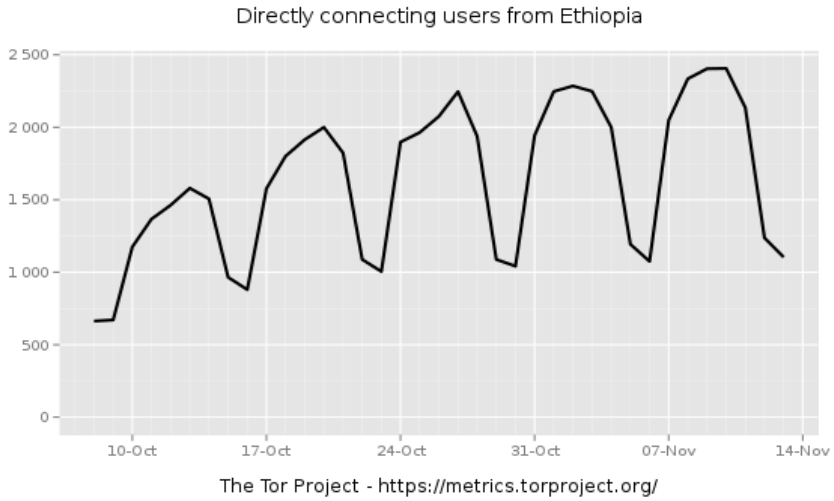
Similar to Google Search traffic, Google Maps traffic appears to be disrupted in August but not in October. The above graphs indicate that if an internet shutdown did occur in October, it only occurred in some networks in certain locations, rather than nationwide. Furthermore, the decrease in overall traffic during October could be attributed to temporary mobile internet shutdowns in certain local networks, or to an increase of censorship events (for example, targeted blocking of certain websites and instant messaging services).

Interestingly, there appears to be a spike in the usage of Tor circumvention software in Ethiopia during October, indicating that internet services might have been less accessible. This is illustrated via Tor Metrics data below:



The Tor Project - https://metrics.torproject.org/

The graph below shows an increase in Tor usage from 8th October, when Ethiopia's state of emergency was declared.



Tor Metrics data, combined with third party internet traffic data, indicates a possible increase in censorship events following the declaration of Ethiopia's state of emergency.[36] While there is no strong indication of an internet shutdown, it is possible that certain mobile data service might have temporarily been shut down in certain locations in Ethiopia at specific points in time.

It is worth noting that OONI's inability to confirm the reported mobile internet shutdown might also in part be due to limitations in the data sources that we referred to. We therefore encourage companies (like Facebook) to increase transparency around internet traffic data so that internet shutdowns and other censorship events can be studied and evaluated more accurately.

1.4 INTERNATIONAL HUMAN HIGHTS LAW

The International Covenant on Civil and Political Rights (ICCPR), to which Ethiopia is a state party, guarantees freedom of expression. This includes the "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 other media of his choice."[37] This right is also protected under Article 9 of the African Charter on Human and Peoples' Rights, to which Ethiopia is a state party.[38]

Regarding restrictions on access to internet resources, the United Nations Human Rights Committee has stressed that any restrictions "generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3 of Article 19 of the ICCPR. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."[39]

The UN Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the Internet which was passed on 1 July 2016, "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures."[40]

The abuse of freedom of expression in the form of propaganda for war, advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence[41] may be subject to restrictions under the ICCPR,[42] but these restrictions must meet three requirements laid out in the covenant. The first requirement is that restrictions must be provided by law, which is "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly". Additionally, "a law may not

[36] Embassy of the United States, Ethiopia Announces Restrictions under State of Emergency, available at https://ethiopia.usembassy.gov/ethiopia-announces-restrictions-under-state-of-emergency.html (last viewed on 9 December 2016).
[37] International Covenant on Civil and Political Rights, Article 19 (2).
[38] http://www.achpr.org/instruments/achpr/
[39] United Nations Human Rights Committee, General Comment No 34, para. 43.
[40] United Nations Human Rights Council, Resolution on the Promotion, protection and enjoyment of human rights on the Internet, A/HRC.32/L.20, para. 10.
[41] International Covenant on Civil and Political Rights, Article 20 (1) and (2).
[42] International Covenant on Civil and Political Rights, Article 19 (3).

confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."[43]

The second requirement is that restrictions must be "necessary" to achieve one of the enumerated legitimate aims under the ICCPR. The third requirement provides, among other things, that "restrictive measures must conform to the principle of proportionality… they must be the least intrusive instrument amongst those which might achieve their protective function."[44]

OONI's findings provide evidence of systematic interference with access to numerous websites belonging to independent news organizations and political opposition groups, as well as sites supporting freedom of expression and LGBTI rights. Such widespread interference and blocking is a violation of Ethiopia's obligations under article 19 of the ICCPR.

The restrictions on access to information as per the findings of this report fail to meet the legality test, which is the first requirement under article 19 (3). Ethiopia lacks clear and precise law that governs access to internet and social media, restrictions/blockade of websites and social media, and the legal procedures. The inventory of Ethiopian relevant telecommunications, cybercrimes, security, and intelligence laws reveals the absence of provisions that govern content control and access to internet in the Country. The laws that established the Information Network Security Agency[45] and the National Intelligence and Security Service[46] authorize neither of the institutions to restrict access to internet and social media, censor websites for any reason. The Telecom Fraud Offences Proclamation[47] does not authorize any of the Government agencies to control and restrict access to internet, websites, or social media application in the country. As such, the internet censorships, blockade of WhatsApp, and restrictions of certain websites are arbitrary, being conducted without any specific national law. Moreover, in the absence of such law, the country also lacks the administrative and judicial procedures for challenging such restrictions and blockades.

The internet restrictions also fail the proportionality test, because the interference is not limited to specific content; rather interference is happening at a very large scale, with dozens of websites affected over the space of several months. Similarly, blocking access to WhatsApp, a popular communications platform in Ethiopia is not a justifiable restriction on freedom of expression and access to information.

Ethiopia's practices of restricting access to large numbers of websites, as well as services such as WhatsApp is therefore a clear violation of the rights to freedom of expression and access to information.

The ICCPR permits derogation from certain rights during emergencies.[48] However, such derogations must meet several criteria in order to be lawful. Most importantly, "the situation must amount to a public emergency which threatens the life of the nation, and the State party must have officially proclaimed a state of emergency."[49] Measures taken subject to a derogation must be "limited to the extent strictly required by the exigencies of the situation."[50]The African Charter on Human and Peoples' Rights does not have a provision that provides for derogation during emergencies.[51]

The state of emergency declaration allows the Command Post to "stop or suspend any mass media and communications" throughout the country. The geographic coverage of this measure violates the requirement that derogations under state of emergency must be limited to exigencies of the situation.

The Ethiopian Government has repeatedly alleged that the violence after the Irrecha tragedy prompted the declaration of the state of emergency. While the violence occurred primarily in some districts of Oromia and Amhara, it is unclear how the exigencies of the situation would strictly require the imposition of such measures with a geographic scope that covers the whole of the country.

---

[43] United Nations Human Rights Committee, General Comment No 34, para. 25.
[44] United Nations Human Rights Committee, General Comment No 34, para. 34.
[45] Information Network Security Agency Re-establishment Proclamation No 808/2013.
[46] National Intelligence and Security Service Re-establishment Proclamation No 804/2013.
[47] Telecom Fraud Offence Proclamation No. 761/2012
[48] International Covenant on Civil and Political Rights, Art. 4.
[49] United Nations Human Rights Committee, General Comment No 29, para. 2.
[50] United Nations Human Rights Committee, General Comment 29, para. 4.
[51] The African Commission on Human and Peoples Rights (African Commission), in its case law, interpreted the absence of the derogation clause in case of public emergency to imply that public emergencies does not warrant derogations from the provisions of the Charter. See *Commission Nationale des Droits de l'Homme et des Libertes v Chad (2000) AHRLR 66 (ACHPR 1995),* para. 21. However, the practice of the African Commission does not reflect this decision in its state reporting procedure, where the Commission has repeatedly failed to find governments' action and constitutional provisions with regard to derogations in public emergency as outright violations. The Commission's Press Release and Resolution on Ethiopia immediately after the adoption of the state of emergency also lacks a statement that recognizes that the ACHPR does not allow derogation during state of emergency. See http://www.achpr.org/press/2016/10/d321/, and http://www.achpr.org/sessions/59th/resolutions/356/.

1.5 CONCLUSION

In the midst of ongoing protests in Ethiopia, access to WhatsApp was found to be blocked, and the covert presence of Deep Packet Inspection (DPI) equipment was not only unveiled, but it was also found to be filtering access to an independent Ethiopian media website (ecadforum.com).

Research conducted by OONI between June and October 2016 shows that access to WhatsApp as well as at least 16 news outlets were blocked prior to the state of emergency. Also targeted were websites supporting Lesbian, Gay, Bisexual, Transgender and Intersex (LGBTI) rights, organizations advocating freedom of expression, sites run by opposition groups and armed movements, as well as websites that offer censorship circumvention tools, such as TOR and Psiphon.

Interestingly, all of these sites consistently presented HTTP response failures when queried, while the testing of different versions of the same sites appeared to bypass the filter in certain cases. This pattern is identical to that of ecadforum.com, indicating that most (if not all) of the above types of sites were likely filtered by DPI equipment as well.

The Amnesty International research findings during the same period corroborate OONI's findings, indicating that other social media applications were very slow, not working properly or inaccessible, particularly in regions affected by the protests.

The evidence suggesting that the government is deploying Deep Packet Inspection (DPI) technology to filter access to internet traffic is concerning. Though it has many legitimate functions, DPI enables effective surveillance and filtering of internet traffic, increasing the States' ability to restrict access to the internet, fully or partially, on command.

Many of the acts of censorship identified by OONI took place before a state of emergency was announced, and violated Ethiopia's obligation to respect, protect and fulfil its people's right to receive and impact information. The acts of censorship, conducted outside a clear legal framework, over several months and affecting dozens of websites and social media platforms failed to meet the criteria set out under the ICCPR for restrictions on freedom of expression.

While the State of Emergency may have subsequently provided a legal framework under Ethiopian law for some of these measures, the State of Emergency itself is so broadly drafted that it violates Ethiopia's international legal obligations and permits violations of numerous human rights. The power the state of emergency bestows upon the Command post to monitor and suspend all communications and media throughout Ethiopia is unnecessarily expansive. The protests and the violence following the protest have been limited to Oromia, Amhara, Konso District in Southern Nations Nationalities and Peoples Region (SNNPR) and Addis Ababa.

Amnesty International and OONI are concerned that unnecessary and disproportionate censorship of the internet will not only continue during the state of emergency, but become institutionalized and entrenched.

1.6 RECOMMENDATIONS

- **TO ETHIOPIAN AUTHORITIES**

Amnesty International and OONI request the Ethiopian government to respect and protect and fulfil freedom of expression on the internet. Specifically, they request the Ethiopian Authorities to:

- Refrain from blocking access to the internet
- Refrain from unlawful censorship of the internet
- Ensure that limitations on the right to seek or impart information on the internet fully adhere to the requirements of article 19 (3) of the ICCPR. Specifically, that the restrictions comply with the three-tier test of legality, necessity and proportionality, and that they are subject to judicial review.

- **TO SOCIAL MEDIA COMPANIES (E.G. FACEBOOK, MICROSOFT, YAHOO AND TWITTER):**
  - Make available publicly verifiable data on network traffic originating from countries around the world, to ensure transparency when social media restrictions or heavy network disruption occur.

2. PART 2: METHODOLOGY

The methodology of this study, in an attempt to identify potential censorship events in Ethiopia included the following:

- Test lists
- OONI network measurements
- Data analysis

OONI's free software tests were run from a local vantage point (EthioNet) in Ethiopia. Some tests examined two lists of URLs: the one being relevant to Ethiopia, while the other including URLs that are commonly accessed around the world. All URLs included in these two lists were tested for blocking. Other OONI tests were run to examine whether systems that could be responsible for censorship, surveillance, and traffic manipulation were present in the tested network. Once network measurement data was collected from these tests, the data was subsequently processed and analyzed based on a set of formula (heuristics) for detecting internet censorship and traffic manipulation.

The testing period started on 15 June 2016 and concluded on 7 October 2016.

2.1 TEST LISTS

An important part of identifying censorship is determining *which* websites to examine for blocking.

OONI's software (called *ooniprobe*) is designed to examine URLs contained in specific lists ("test lists") for censorship. By default, ooniprobe examines the "global test list", which includes a wide range of internationally relevant websites, most of which are in English. These websites fall under 30 categories, ranging from news media, file sharing and culture, to provocative or objectionable categories, like pornography, political criticism, and hate speech.

These categories help ensure that a wide range of different types of websites are tested, and they enable the examination of the impact of censorship events (for example, if the majority of the websites found to be blocked in a country fall under the "human rights" category, that may have a bigger impact than other types of websites being blocked elsewhere). The main reason why objectionable categories (such as "pornography" and "hate speech") are included for testing is because they are more likely to be blocked due to their nature, enabling the development of heuristics for detecting censorship elsewhere within a country.

In addition to testing the URLs included in the global test list, ooniprobe is also designed to examine a test list, which is specifically created for the country that the user is running ooniprobe from, if such a list exists. Unlike the global test list, country-specific test lists include websites that are relevant and commonly accessed within specific countries, and such websites are often in local languages. Similar to the global test list, country-specific test lists include websites that fall under the same set of 30 categories, as explained previously.

All test lists are hosted by the Citizen Lab on GitHub, supporting OONI and other network measurement projects in the creation and maintenance of lists of URLs to test for censorship. Some criteria for adding URLs to test lists include the following:

- The URLs cover topics of socio-political interest within the country.

- The URLs are likely to be blocked because they include sensitive content (i.e. they touch upon sensitive issues or express political criticism).
- The URLs have been blocked in the past.
- Users have faced difficulty connecting to those URLs.

The above criteria indicate that such URLs are more likely to be blocked, enabling the development of heuristics for detecting censorship within a country. Furthermore, other criteria for adding URLs are reflected in the 30 categories that URLs can fall under. Such categories, for example, can include file-sharing, human rights, and news media, under which the websites of file-sharing projects, human rights NGOs and media organizations can be added.

As part of this study, the URLs included in *both* the Citizen Lab's test list for Ethiopia and its global list were tested for blocking.

A core limitation to the study is the *bias* in terms of the URLs that were selected for testing. The URL selection criteria, for example, included the following:

- Websites that were more likely to be blocked because their content expressed political criticism.
- Websites of organizations that were known to have previously been blocked and were thus likely to be blocked again.
- Websites reporting on human rights restrictions and violations.

The above criteria reflect bias in terms of which URLs were selected for testing, as one of the core aims of this study was to examine whether and to what extent websites reflecting criticism were blocked, limiting open dialogue and access to information across the country. As a result of this bias, it is important to acknowledge that the findings of this study are only limited to the websites that were tested, and do not provide a complete view of other censorship events that may have taken place before and after the testing period.

2.2 OONI NETWORK MEASUREMENTS

The Open Observatory of Network Interference (OONI) is a *free software* project that aims to increase transparency about internet censorship and traffic manipulation around the world. Since 2011, OONI has developed multiple *free and open source software tests* designed to examine the following:

- Blocking of websites.
- Blocking of instant messaging apps.
- Detection of systems responsible for censorship and traffic manipulation.
- Reachability of circumvention tools (such as Tor, Psiphon, and Lantern) and sensitive domains.

As part of this study, the following OONI software tests were run from a local vantage point in Ethiopia:

- Web connectivity
- HTTP invalid request line
- HTTP header field manipulation
- HTTP host

The web connectivity test was run with the aim of examining whether a set of URLs (included in both the "global test list" and the "Ethiopian test list") were blocked during the testing period and if so, how. The HTTP invalid request line and HTTP header field manipulation tests were run with the aim of examining whether systems (that could potentially be responsible for censorship and/or surveillance) were present in the tested network. The HTTP host test was run to not only examine if tested URLs were blocked, but to also examine whether specific systems were used in the tested network to implement such blocking.

The sections below document how each of these tests are designed for the purpose of detecting cases of internet censorship and traffic manipulation.

2.2.1 WEB CONECTIVITY

This test examines whether websites are reachable and if they are not, it attempts to determine whether access to them is blocked through DNS tampering, TCP connection RST/IP blocking or by a transparent HTTP proxy. Specifically, this test is designed to perform the following:

- Resolver identification
- DNS lookup
- TCP connect
- HTTP GET request

By default, this test performs the above (excluding the first step, which is performed only over the network of the user) both over a control server and over the network of the user. If the results from both networks match, then there is no clear sign of network interference; but if the results are different, the websites that the user is testing are likely censored.

Further information is provided below, explaining how each step performed under the web connectivity test works.

1. RESOLVER IDENTIFICATION

The domain name system (DNS) is what is responsible for transforming a host name (e.g. torproject.org) into an IP address (e.g. 38.229.72.16). Internet Service Providers (ISPs), amongst others, run DNS resolvers which map IP addresses to hostnames. In some circumstances though, ISPs map the requested host names to the wrong IP addresses, which is a form of tampering.

As a first step, the web connectivity test attempts to identify which DNS resolver is being used by the user. It does so by performing a DNS query to special domains (such as whoami.akamai.com) which will disclose the IP address of the resolver.

2. DNS LOOKUP

Once the web connectivity test has identified the DNS resolver of the user, it then attempts to identify which addresses are mapped to the tested host names by the resolver. It does so by performing a DNS lookup, which asks the resolver to disclose which IP addresses are mapped to the tested host names, as well as which other host names are linked to the tested host names under DNS queries.

3. TCP CONNECT

The web connectivity test will then try to connect to the tested websites by attempting to establish a TCP session on port 80 (or port 443 for URLs that begin with HTTPS) for the list of IP addresses that were identified in the previous step (DNS lookup).

4. HTTP GET REQUEST

As the web connectivity test connects to tested websites (through the previous step), it sends requests through the HTTP protocol to the servers which are hosting those websites. A server normally responds to an HTTP GET request with the content of the webpage that is requested.

5. COMPARISON OF RESULTS: IDENTIFYING CENSORSHIP

Once the above steps of the web connectivity test are performed *both* over a control server and over the network of the user, the collected results are then compared with the aim of identifying whether and how tested websites are tampered with. If the compared results do *not* match, then there is a sign of network interference.

Below are the conditions under which the following types of blocking are identified:

- DNS blocking: If the DNS responses (such as the IP addresses mapped to host names) do *not* match.
- TCP/IP blocking: If a TCP session to connect to websites was *not* established over the network of the user.
- HTTP blocking: If the HTTP request over the user's network failed, or the HTTP status codes don't match, or all of the following apply:

- The body length of compared websites (over the control server and the network of the user) differs by some percentage
- The HTTP headers names do not match
- The HTML title tags do not match

It is important to note, however, that DNS resolvers, such as Google or a local ISP, often provide users with IP addresses that are closest to them geographically. Often this is *not* done with the intent of network tampering, but merely for the purpose of providing users with localized content or faster access to websites. As a result, some false positives might arise in OONI measurements. Other false positives might occur when tested websites serve different content depending on the country that the user is connecting from, or in the cases when websites return failures even though they are not tampered with.

2.2.2 HTTP INVALID REQUEST LINE

This test tries to detect the presence of network components ("middle box") which could be responsible for censorship and/or traffic manipulation.

Instead of sending a normal HTTP request, this test sends an invalid HTTP request line - containing an invalid HTTP version number, an invalid field count and a huge request method – to an echo service listening on the standard HTTP port. An echo service is a very useful debugging and measurement tool, which simply sends back to the originating source any data it receives. If a middle box is not present in the network between the user and an echo service, then the echo service will send the invalid HTTP request line back to the user, exactly as it received it. In such cases, there is no visible traffic manipulation in the tested network.

If, however, a middle box is present in the tested network, the invalid HTTP request line will be intercepted by the middle box and this may trigger an error and that will subsequently be sent back to OONI's server. Such errors indicate that software for traffic manipulation is likely placed in the tested network, though it's not always clear what that software is. In some cases though, censorship and/or surveillance vendors can be identified through the error messages in the received HTTP response. Based on this technique, OONI has previously detected the use of BlueCoat, Squid and Privoxy proxy technologies in networks across multiple countries around the world.

It's important to note that a false negative could potentially occur in the hypothetical instance that ISPs are using highly sophisticated censorship and/or surveillance software that is specifically designed to not trigger errors when receiving invalid HTTP request lines like the ones of this test. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

2.2.3 HTTP HEADER FIELD MANIPULATION

This test also tries to detect the presence of network components ("middle box") which could be responsible for censorship and/or traffic manipulation.

HTTP is a protocol which transfers or exchanges data across the internet. It does so by handling a client's request to connect to a server, and a server's response to a client's request. Every time a user connects to a server, the user (client) sends a request through the HTTP protocol to that server. Such requests include "HTTP headers", which transmit various types of information, including the user's device operating system and the type of browser that is being used. If Firefox is used on Windows, for example, the "user agent header" in the HTTP request will tell the server that a Firefox browser is being used on a Windows operating system.

This test emulates an HTTP request towards a server, but sends HTTP headers that have variations in capitalization. In other words, this test sends HTTP requests which include valid, but non-canonical HTTP headers. Such requests are sent to a backend control server which sends back any data it receives. If OONI receives the HTTP headers exactly as they were sent, then there is no visible presence of a "middle box" in the network that could be responsible for censorship, surveillance and/or traffic manipulation. If, however, such software is present in the tested network, it will likely normalize the invalid headers that are sent or add extra headers.

Depending on whether the HTTP headers that are sent and received from a backend control server are the same or not, OONI is able to evaluate whether software – which could be responsible for traffic manipulation – is present in the tested network.

False negatives, however, could potentially occur in the hypothetical instance that ISPs are using highly sophisticated software that is specifically designed to not interfere with HTTP headers when it receives them. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

2.2.4 HTTP HOST

This test is designed to examine:

- Whether the domain names of websites are blocked;
- The presence of "middle boxes" (software that could be responsible for censorship and/or surveillance) in tested networks;
- Whether censorship circumvention techniques are capable of bypassing the censorship implemented by the "middle box".

OONI's HTTP Host test implements a series of techniques which help it evade getting detected from censors and then uses a list of domain names (such as bbc.co.uk) to connect to an OONI backend control server, which sends the host headers of those domain names back to OONI. If a "middle box" is detected between the network path of the probe and the OONI backend control server, its fingerprint might be included in the JSON data that OONI receives from the backend control server. Such data also informs OONI if the tested domain names are blocked or not, as well as how the censor tried to fingerprint the censorship of those domains. This can sometimes lead to the identification of the type of infrastructure being used to implement censorship.

2.3 DATA ANALYSIS

Through its data pipeline, OONI processes all network measurements that it collects, including the following types of data:

COUNTRY CODE

OONI by default collects the code which corresponds to the country from which the user is running ooniprobe tests from, by automatically searching for it based on the user's IP address through the MaxMind GeoIP database. The collection of country codes is an important part of OONI's research, as it enables OONI to map out global network measurements and to identify where network interferences take place.

AUTONOMOUS SYSTEM NUMBER (ASN)

OONI by default collects the Autonomous System Number (ASN), which corresponds to the network that a user is running ooniprobe tests from. The collection of the ASN is useful to OONI's research because it reveals the specific network provider (such as Vodafone) of a user. Such information can increase transparency in regards to which network providers are implementing censorship or other forms of network interference.

DATE AND TIME OF MEASUREMENTS

OONI by default collects the time and date of when tests were run. This information helps OONI evaluate when network interferences occur and to compare them across time.

IP ADDRESSES AND OTHER INFORMATION

OONI does *not* deliberately collect or store users' IP addresses. In fact, OONI takes measures to remove users' IP addresses from the collected measurements, to protect its users from potential risks.

However, OONI might *unintentionally* collect users' IP addresses and other potentially personally-identifiable information, if such information is included in the HTTP headers or other metadata of measurements. This, for example, can occur if the tested websites include tracking technologies or custom content based on a user's network location.

NETWORK MEASUREMENTS

The types of network measurements that OONI collects depend on the types of tests that are run. Specifications about each OONI test can be viewed through its git repository, and details about what collected network measurements entail can be viewed through OONI Explorer or through OONI's list of measurements.

OONI processes the above types of data with the aim of deriving meaning from the collected measurements and, specifically, in an attempt to answer the following types of questions:

- Which types of OONI tests were run?
- In which countries were those tests run?
- In which networks were those tests run?
- When were tests run?
- What types of network interference occurred?
- In which countries did network interference occur?
- In which networks did network interference occur?
- When did network interference occur?
- How did network interference occur?

To answer such questions, OONI's pipeline is designed to process data which is automatically sent to OONI's measurement collector by default. The initial processing of network measurements enables the following:

- Attributing measurements to a specific country.
- Attributing measurements to a specific network within a country.
- Distinguishing measurements based on the specific tests that were run for their collection.
- Distinguishing between "normal" and "anomalous" measurements (the latter indicating that a form of network tampering is likely present).
- Identifying the type of network interference based on a set of heuristics for DNS tampering, TCP/IP blocking, and HTTP blocking.
- Identifying block pages based on a set of heuristics for HTTP blocking.
- Identifying the presence of "middle boxes" within tested networks.

However, false positives and false negatives emerge within the processed data due to a number of reasons. As explained previously (section on "OONI network measurements"), DNS resolvers (operated by Google or a local ISP) often provide users with IP addresses that are closest to them geographically. While this may appear to be a case of DNS tampering, it is actually done with the intention of providing users with faster access to websites. Similarly, false positives may emerge when tested websites serve different content depending on the country that the user is connecting from, or in the cases when websites return failures even though they are not tampered with.

Furthermore, measurements indicating HTTP or TCP/IP blocking might actually be due to temporary HTTP or TCP/IP failures, and may not conclusively be a sign of network interference. It is therefore important to test the same sets of websites across time and to cross-correlate data, prior to reaching a conclusion on whether websites are in fact being blocked.

Since block pages differ from country to country and sometimes even from network to network, it is quite challenging to accurately identify them. OONI uses a series of heuristics to try to guess if the page in question differs from the expected control, but these heuristics can often result in false positives. Due to this, OONI only confirms an instance of blocking when a known block page has manually been added to the list of block pages that OONI supports.

However, this means that when a block page is not presented by the censor OONI cannot confirm with absolute certainty that blocking is occurring. For the purpose of this study we have extended our methodology to also take into account unusual failures that could be triggered by the censor. In particular, we have looked at sites that appear to fail consistently (in the same way) and constantly over the testing period, therefore most likely *not* due to transient networking errors.

OONI's methodology for detecting the presence of "middle boxes" – systems that could be responsible for censorship, surveillance and traffic manipulation – can also present false negatives if ISPs are using highly sophisticated software that is specifically designed to *not* interfere with HTTP headers when it receives them, or to *not* trigger error messages when receiving invalid HTTP request lines. It remains unclear though if such software is being used. Moreover, it's important to note that the presence of a middle box is not necessarily indicative of censorship or traffic manipulation, as such systems are often used in networks for caching purposes.

Upon collection of more network measurements, OONI continues to develop its data analysis heuristics, based on which it attempts to accurately identify censorship events.

2.4 ACKNOWLEDGEMENT OF LIMITATIONS

The findings of this study present various limitations, and do not necessarily reflect a comprehensive view of internet censorship in Ethiopia on a nationwide level.

The first limitation is associated with the testing period, which started on 15th June 2016 and concluded on 7th October 2016, immediately prior to the declaration of Ethiopia's state of emergency on 8th October. Therefore, censorship events which may have occurred before and/or after the testing period (such as the reported mobile internet shutdown in October 2016) were not examined as part of this study. Furthermore, security challenges for people conducting such tests in Ethiopia limited our ability to perform daily measurements and tests were inevitably run quite sporadically across the testing period. As such, censorship events that may have occurred on days that tests were not run might not be included as part of this study.

Even though measurements were collected from Ethio Telecom, which is Ethiopia's main telecommunications service provider, the findings of this study do not necessarily apply on a nationwide level. Ethio Telecom might have applied censorship in *some* locations of Ethiopia, while not in others. Given that OONI software tests were run from the same location across the testing period, we do not know whether the censorship events found through this study apply nationwide or not.

Another limitation is associated to the types of URLs that were tested as part of this study. While a total of 1,403 different URLs were tested for censorship as part of this study, not all the URLs on the internet were tested, indicating the possibility that other websites not included in test lists might have been blocked.

Finally, the data analysis heuristics as part of this study also present limitations. This is due to the fact that many false positives almost inevitably emerge within the collected measurement data, limiting our ability to confirm censorship events with confidence, especially when block pages are not present.

https://www.amnesty.org/en/latest/news/2016/05/ethiopia-release-opposition-politician-held-for-facebook-posts/

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US

info@amnesty.org

+44 (0)20 7413 5500

JOIN THE CONVERSATION

www.facebook.com/AmnestyGlobal

@AmnestyOnline

AMNESTY INTERNATIONAL

OONI

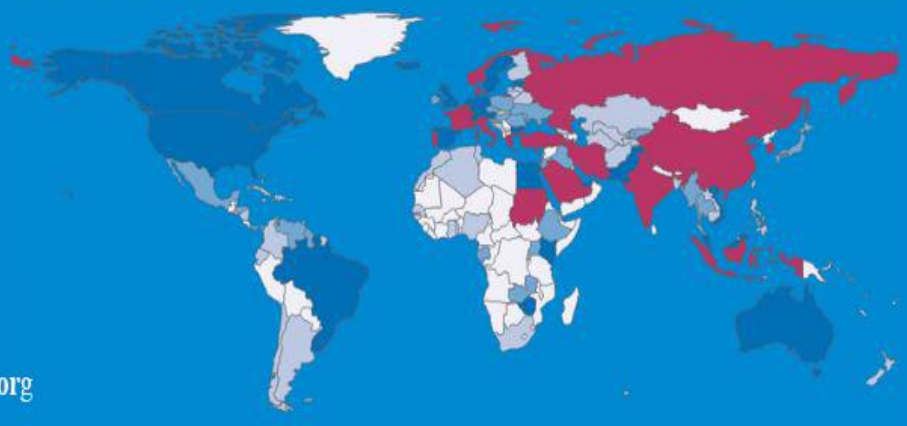
Open Observatory of Network Interference

A free software, global observation network for detecting censorship, surveillance and traffic manipulation on the internet

OONI Explorer

OONI has been monitoring internet censorship around the world since 2012

Explore OONI Data www.ooni.torproject.org



ETHIOPIA OFFLINE

EVIDENCE OF SOCIAL MEDIA BLOCKING AND INTERNET CENSORSHIP IN ETHIOPIA

Waves of protests against the government have taken place across various parts of Ethiopia since November 2015. These protests have consistently been quashed by Ethiopian security forces using excessive, sometimes lethal, force which has led to scores of injuries and deaths.

The crackdown was accompanied by equally severe restrictions on freedom of expression and access to information. This report documents violations of these rights based on testimony from Amnesty International's contacts inside Ethiopia and network measurements performed by OONI. The report presents evidence of the Ethiopian authorities' blocking of websites and instant messaging services, internet slowdowns, and blocking of common circumvention tools, over a period of several months.

These restrictions on access to information and communications in large parts of the country amount to violations of Ethiopia's obligations under international human rights law.

Amnesty International and OONI call on the Ethiopian government to refrain from blocking access to the Internet and unlawfully censoring the internet or restricting access to communications platforms. We also strongly encourage Internet companies including Facebook, Microsoft, Yahoo and Twitter, to increase transparency around internet traffic data so that internet shutdowns and other censorship events can be investigated and verified quickly, and more accurately.

AMNESTY INTERNATIONAL

www.amnesty.org

OONI

www.ooni.torproject.org