Network Disruptions and the Law in Ethiopia: A Legal Guide

Kinfe Micheal Yilma, PhD.

DEFENDING THE INTERNET WITH DATA

August/September 2021

Table of Contents

Acknowledgement

The author gratefully thanks Halefom Hailu Abraha for his critical comments and suggestions on earlier drafts of this work. Gratitude is also due to a number of individuals and organizations in Ethiopia for providing useful information during the preparation of this work. A number of undergraduate and graduate students at Addis Ababa University Law School provided invaluable research assistance for which the author is thankful. The Author also acknowledges the financial support provided by Internews Network through its OPTIMA Grants program.

Introduction

Ethiopia's attempt at regulating behaviour in cyberspace over the past decade conjures a mixed picture. While quite progressive policies and laws have been introduced, a number of regulatory practices with no clear legal basis have also run in parallel. One case in point is network disruption which has recently emerged as a prime regulatory tool in Ethiopia. The government has imposed total and partial Internet blackouts on several occasions in the past few years. Be it for purposes of preventing exam cheating, the spread of disinformation or averting the circulation of conspiracy theories regarding certain political events; Internet shutdowns have become recurring episodes. Of course, network disruption has been part of the government's regulatory repertoire long before the Internet become a source of problematic content. One recalls here past practices of jamming foreign-based satellite television and radio stations[1] — which appears to have resurfaced recently[2] — and rampant practices of blocking access to websites.[3] In the run up to and after the 2005 controversial general elections for instance, the Ethiopian government had suspended Short Messaging Services (SMS).[4]

Widespread protests of 2015 have been a turning point in the proliferation of network disruptions in Ethiopia. Ever since, the government has disrupted communication networks, including total and partial Internet shutdowns, several times. At the time of writing this *Legal Guide*, total network disruption is in place in the regional state of Tigray where there is an ongoing war between Tigray Defence Forces (TDF) and forces of the Federal Government of Ethiopia and Eritrea.[5] Reports of network disruptions have also been common in other parts of Ethiopia such as several provinces in the Oromia regional state and the Amhara region. Often, such far-reaching measures are taken without any apparent legal basis, and rarely have the government provided a proper explanation. In the rare instances where the government offered a legal justification, it relies on vague provisions of the law.

To a degree, the arbitrary nature of network disruptions is facilitated by the fact that the communications sector has been – until recently – under State monopoly. While a private telecom operator has recently been awarded a license, Ethio-telcom — a state enterprise — has rarely made its views clear about the recurrent culture of network disruptions in Ethiopia. Other relevant stakeholders such as civil society groups working in the field of human rights generally and 'digital rights' in particular are also yet to take steps in predicting, preventing and responding to network disruptions. This apathy towards network disruptions in Ethiopia is attributable to a number of factors. One relates to the limited level of Internet penetration, and hence, limited uptake of Information and Communication Technologies (ICTs) in the

[1] See Media Sustainability Index: Ethiopia (2010, IREX) 131.
[2] See, e.g., The Government of Ethiopia Jammed Dimsti Woyane and Tigray Media House, Tigray Today Facebook Page <https://bit.ly/3xrz4ho>; Eutelsat, DSTV Knocked Two Tigrai-based Broadcasters Off Air (The Reporter, 11 July 2020) <https://bit.ly/3xnKF16>.
[3] See, e.g., Freedom on the Net: Ethiopia (2016, Freedom House) <https://bit.ly/2RV9pxo>.
[4] See U.S. Department of State Country Report on Human Rights Practices 2005: Ethiopia (8 March 2006) <https://bit.ly/2QosJD7>.
[5] Note that after this *Legal Guide* was finalized in May 2021, much of Tigray has fallen back to TDF but network disruption remains in place in all parts of the region to date (i.e., late July 2021). See How Local Guerrilla Fighters Routed Ethiopia's Powerful Army (The New York Times, 12 July 2021) <https://nyti.ms/3hY6eiY>.

nation's socio-economic systems. But with increasing access to the Internet and the overall drive towards digitization, the recurrence of network disruptions is bound to be a cause for concern among relevant actors. The other factor relates to the hitherto restrictive legal regime for the formation of civil society organizations which may have had a role in limiting the number of civil society groups working in the field of human rights, including on 'digital rights'. The recent change in the civil societies' law has, however, began to enable the formation of organizations with mandates on network disruptions.

Despite such promising developments, there is a persistent lack of clarity as to what could be done, and by who in addressing the problem of network disruptions in Ethiopia. For instance, it remains unclear whether Ethiopian law offers any defensible legal basis for network disruptions. Also unclear is whether legal grounds seldomly relied upon by the government to justify network disruptions stand up to closer scrutiny. The respective role of stakeholders in attending to the wide-ranging socio-economic and human rights impacts of network disruptions is also far from clear. This *Legal Guide* seeks to fill this gap in two ways.

First, it explores the current legal landscape relevant to network disruptions. In so doing, it considers whether, and the extent to which, the legal basis relied upon by the government, as well as emergent standards on network disruption, are pertinent. The *Legal Guide* then shows how the current cybercrime legislation offers a defensible legal basis for some forms of network disruptions in Ethiopia. This would prove particularly useful when one considers the impending liberalization (and partial privatization) of the telecom sector in Ethiopia. As the monopoly ends and new telecom operators enter the market, the government's appetite for disrupting communication networks to tackle problematic content such as disinformation is likely to grow exponentially. As access to the Internet increases, the volume of content problematic to the government would also increase — and hence calling for more episodes of network disruptions which are often used as measures against such content.

The *Legal Guide* would provide to new telecom operators as well as civil society groups legal guidance on the country's legal framework governing network disruptions. Beyond civil society actors that might wish to push litigation after the fact, the *Legal Guide* would bring clarity about when and how network disruptions may be legally justified. This would be beneficial in a number of ways, including in outlining the permissible grounds and preconditions for network disruptions. Second, the *Legal Guide* details the ways in which key stakeholders, namely, relevant government bodies, civil society groups and the private sector, may take steps in predicting, preventing and responding to network disruptions. Recurrent network disruptions in Ethiopia often cause outrage but there appears to be little awareness as to who should/could do what in attending to such a recurring problem. In this regard, the *Legal Guide* would bring some clarity on the respective institutional roles of key stakeholders.

Methodology

This Legal Guide adopts a mixed research approach combining desk research and interview with relevant stakeholders. First, a doctrinal desk research has been conducted to thoroughly analyse relevant laws, policies and the attendant jurisprudence on network disruption in

Ethiopia and beyond. Second, the desk research is supplemented by semi-structured interviews with relevant stakeholders, particularly civil society actors. Interviews with relevant civil society actors sought to gather information on two points: (a) to uncover steps being taken to address the recurrent problem of network disruptions, (b) to establish the nature and type of legal resources that civil society groups would like to have in their effort to predict, prevent and respond to network disruptions in Ethiopia, and (c) to understand the extent to which network disruptions impacted vulnerable groups, particularly women. In so doing, interviews were conducted with two categories of respondents.

The first category of respondents included representatives from civil society organizations. Three types of civil society organizations were interviewed: (a) those working particularly in the field of 'digital rights' namely the Center for the Advancement of Rights and Democracy (CARD) and the Network for Digital Rights in Ethiopia (NDRE); (b) a civil society group working on human rights generally, namely the Ethiopian Human Rights Council (EHRCO); and (c) civil society organizations working on the rights and welfare of women, namely Setawit and Siqqee Scholars. The first two organizations are picked because they are the main human rights civil society groups in the country. Whereas the third set of civil society groups are selected for their high profile advocacy work on the rights of women who are disproportionately affected by network disruptions. In the second category, interviews were held with undergraduate and graduate students at Addis Ababa University Law School — who are originally from the northern region of Tigray and the western province of Wollega in the Oromia region — with a view to get a sense of the impact of network disruptions on residents of places where there is still ongoing network disruption.

Setting the Scene: Network Disruptions in Ethiopia

Ethiopia is one of the few countries to introduce telecommunications in 1894 shortly after its invention, but it is one of the least connected countries in the world. According to data from Internet World Stats, the level of Internet penetration as of December 2020 has been around 18%.[6] But recent years have seen a growing drive towards digitalization at many levels. A growing number of technology companies are carving a budding tech industry in and around Addis Ababa.[7] Information and communication technologies are also increasingly being adopted by a number of organizations such as financial institutions. Indeed, successive national ICT policies of the government have long recognized information and communication technologies as enablers of development.[8] But the most recent policy iteration, the Digital Transformation Strategy, envisions building a vibrant digital economy that would catalyse Ethiopia's broader development vision.[9] Nevertheless, this multi-faceted drive towards digitalization and development of a digital economy is being undermined by network

[6] See details at <https://www.internetworldstats.com/africa.htm#et>. At the time of writing, Ethio-telcom claims that it has close to 55 million mobile service subscribers and over 25 million data and Internet users but these statistics do not reflect the level of Internet penetration in Ethiopia. See <https://www.ethiotelecom.et/>.
[7] See The Ethiopia Tech Ecosystem: A Sleeping Giant is Waking Up! (GSMA, 3 July 2019) <https://bit.ly/3aBSvKD>.
[8] See, e.g., National Information and Communication Technology Policy and Strategy of Ethiopia (2016).
[9] See Digital Ethiopia 2025: A Digital Strategy for Ethiopia's Inclusive Prosperity (2020).

disruptions. Not only are disruptions occurring frequently but also often for a longer duration. The nascent tech start-ups are particularly being impacted by the recurring and prolonged disruption of communication networks.[10] In what follows, the scope and nature of network disruption in Ethiopia are discussed with a view to providing a background to the subsequent analysis on its legal dimensions.

Nature and Scope of Network Disruptions in Ethiopia

For purposes of this *Legal Guide*, Global Network Initiative's (GNI) enunciation of 'network disruption' is followed. According to a GNI report, network disruption denotes 'the intentional, significant disruption of electronic communication within a given area and/or affecting a predetermined group of citizens'.[11] Unless the context dictates otherwise, cognate terms such as Internet shutdown and network shutdown are used interchangeably with network disruptions. Network disruptions vary on many levels. One concerns the scope of the information control it enables. In this sense, network disruptions range from complete Internet and telecom service blackout throughout a specific geographic area to blocking of specific websites and mobile applications. The other variation relates to the mental element driving the disruptions where most disruptions are carried out by telecom operators on the orders of the government. Whereas some disruptions are accidentally caused due to technical failures or damage caused to the network's physical infrastructure. The third point of variation concerns the time when measures disrupting the network are taken vis-à-vis the danger they seek to contain. While most disruptive measures are reactionary – i.e. taken once events triggering disruption began unfolding such as street protest or violence, some are preventive aimed at pre-emptively avoiding the role of, say social media, in triggering or fuelling violence. A further point of variation is the juridical means with which governments instruct network disruptions. Often, orders come in the form of executive instructions whereas a judicial warrant is rarely sought to have networks disrupted.

A number of rationales are provided by the Ethiopian government for network disruptions. The trigger factors may be grouped into three categories. The first and probably the commonest trigger factor relates to threats to national security and public safety. Since 2015, network disruptions have occurred multiple times during mass public protests and the ensuing violence[12] and in the aftermath of political assassinations.[13] The more recent iteration of the national security rationale has been deployed to justify the ongoing region-wide network shutdown in the Tigray regional state where there is a war. Network disruption is reportedly still in place in certain parts of the country such as several provinces in Oromia, Benishangul Gumuz and Amhara regional states where there is an intensifying insurgency.[14] By default, disrupting communication networks has become part and parcel of the

[10] Ethiopia's Tech Start-ups are Ready to Run the World, But the Internet Keeps Getting Blocked (Quartz Africa, 18 June 2019) <https://bit.ly/3aEKIMu>.
[11] Disconnected: A Human Rights-based Approach to Network Disruptions (GNI, 2020) 6.
[12] As Violence Flares in Ethiopia, Internet Goes Dark (VOA News, 17 December 2017) <https://bit.ly/3sRzElj>.
[13] Ethiopia's Government Shut down the Entire Country's Internet (Business Insider, 7 February 2020) <https://bit.ly/2PsfpwW>.
[14] Internet Disrupted in Ethiopia as Conflict Breaks out in Tigray Region (NetBlocks, 4 November 2020) <https://bit.ly/3dTS8gw>; Ongoing Internet and Phone Disruptions in Oromia as of January 8 (Garda World, 9 January 2020) <https://bit.ly/2SlqaSO>.

government's national security response. Incidents of political nature in the past five years tend to be followed by circulation of rumours, disinformation and conspiracy theories which — in turn — result in widespread violence and destruction. As a result, network disruption often is taken to pre-empt such street violence and destruction of property. But as several studies have shown, such measures add little in addressing the problem network disruptions seek to achieve.[15] Indeed, the fact that the country still is beset by multiple armed conflicts, further polarization of politics and the attendant prominence of online disinformation allude to the impertinence of network disruptions as a national security regulatory tool.

Preventing exam leaks is the second objective sought by network disruptions in Ethiopia. In June 2019 for instance, the government shut down certain social media platforms and mobile data services to prevent the circulation of leaked national exam scripts.[16] This pre-emptive measure is triggered by the scandalous exam leaks that occurred a year before. But in July 2016, the government had blocked popular social media platforms like Facebook, Instagram, WhatsApp and Viber to prevent students from being 'distracted' by rumours about leaked national high school leaving exams.[17] Similarly, a total Internet blackout was also imposed in June 2019 during the national high school leaving exams to prevent exam cheating.[18] This rationale has not since been presented to disrupt communication networks.

Thirdly, network disruptions have been triggered by alleged attacks on the physical and technical telecommunication infrastructure by what the government calls 'criminal elements'. But often such rationale was never presented as a freestanding cause for disruptions. For example, some government officials have blamed the actions of TDF, including through cyberattacks, for disruptions in parts of Tigray while — in truth — the region was in total network blackout since the beginning of the war in early November.[19] Similarly, the government blamed an insurgent group in Oromia, the Oromo Liberation Army (OLA), for causing damage to telecom infrastructure which led to network disruptions.[20] But a version of this rationale for network disruption is the claim that the Internet was shut down to fend off cyber-attacks against financial institutions.[21] While the notion of disrupting the network to respond to cyber-attacks sounds odd, network disruptions cannot be a sustainable solution to threats of cyber-attacks against critical infrastructures.

The scope of network disruptions in Ethiopia, including in terms of geographic coverage, varied over time. Total network shutdown occurred throughout the country, for instance in

[15] See, e.g., Shutting Down Social Media Does Not Reduce Violence, But Rather Fuels it (The Conversation, 29 April 2019) <https://bit.ly/3xsmCho>.
[16] See, e.g., Ethiopia Shuts Down the Internet to Prevent Exam Leaks (Digital Watch, 13 June 2019) <https://bit.ly/2S3FJ1k>.
[17] Ethiopia Shuts Down Social Media to Keep from 'Distracting' Students (The Washington Post, 13 July 2016) <https://wapo.st/3eslWjA>. Note, though, that exams were indeed leaked on Telegram and students had to retake national exams.
[18] Total Internet Outage Identified in Ethiopia (NetBlocks, 11 June 2019) <https://bit.ly/3vjffan>.
[19] See, e.g., Cyberattack Behind Tigray Blackout, Says Ethiopia (EU Observer, 14 December 2020) <https://bit.ly/32PmVFi>; see also the message of the federal government in its fact-checking platform set up following the Tigray war where it blames physical destruction by TDF at < https://bit.ly/3gL8VVf>.
[20] See, e.g., Ethiopian Government Lifts Telecom Ban on West Oromia Amid International Outcry (Ezega, 1 April 2020) <https://bit.ly/3eyVnJw>.
[21] Brief Internet Shutdown in Ethiopia as a Cyber Attack Hits (Digital Watch, 5 December 2019) <https://bit.ly/3aBV53q>.

the aftermath of the assassinations of political leaders in the Amhara region in June 2019[22] and a political activist-singer in June 2020.[23] As alluded to above, with a view to prevent exam cheating, total Internet blackout was in place for three days in June 2019 throughout the country. In the Tigray regional state for instance, Internet, mobile and fixed telephone lines as well as electricity have been disrupted since the beginning of the war in early November 2020, and Internet remains still shut. In other cases, the network disruption is restricted to specific geographic locations. For instance, several reports indicate that network disruptions are in place in a handful of provinces in Oromia, Amahara, and Benishangul Gumuz regional states.

The other variation of scope is the extent of the disruptions. While total blackout affecting Internet and telephone services are common, the government, on a few occasions, has disrupted parts of the network. For instance, the response to exam leaks has not been total Internet and phone service blackout but blocking of popular social networking and messaging services like Viber. In some instances — such as during the June 2017 network disruption, the aim was preventing exam leaks and targeted just social media platforms and mobile data services. As such, broadband Internet, fixed and mobile services were not disrupted. Whereas the December 2019 brief disruptions affected only Internet services, not other telecom services such voice and SMS services. As this brief overview suggests, the scope and nature of network disruptions varied by time and place in Ethiopia. It further signals that government network disruption measures followed no consistent and coherent standards or procedure. The arbitrary nature of network disruption measures emanates from this impulsive approach of the government.

Imperative of A Legal Guide for Network Disruptions in Ethiopia

A need assessment recently undertaken by Internews has underlined the need for country-specific mechanisms of pushing back against arbitrary network disruptions, including through advocacy efforts, raising public awareness and strategic litigation.[24] This *Legal Guide* is a direct response to this need for a country-specific legal resources for addressing network disruptions in Ethiopia. In what follows, the imperatives of a tailored *Legal Guide* for network disruptions in Ethiopia are outlined. Imperatives of this *Legal Guide* can be put into three broad categories.

Firstly, network disruption in Ethiopia occurs not only too often but also lacks a clear legal basis. Also unclear is the process through which disruptions are carried out. What law has been invoked to justify network disruptions? Who orders, requests or technically effects network disruptions? What processes are followed to effect disruptions? Who determines the scope and duration of network disruptions? Except for the legal basis casually invoked by the government, questions of the above sort find no clear answer. This confusion surrounding network disruptions, mainly its legal and procedural aspects, appears to have undermined — or at least may have delayed — legal responses to recurrent and prolonged network

[22] Internet Shutdown in Ethiopia Amid Reports of Attempted Coup (NetBlocks, 22 June 2019) <https://bit.ly/3gLegvL>.
[23] Internet Cut in Ethiopia Amid Unrest Following Killing of Singer (NetBlocks, 30 June 2020) < https://bit.ly/3veiD6i>.
[24] See Building Capacity for Internet Shutdown Advocacy: A Community Needs Assessment Report (Internews, November 2020) 4.

disruptions in Ethiopia. Relevant stakeholders, including emerging civil society organizations, lack clarity as to the possible ways of timely responding to network disruptions. These actors require a guideline that outlines legal means of responding to network disruptions in Ethiopia. This *Legal Guide* seeks to fill this void by providing a thorough but accessible analysis of the pertinent legal framework governing network disruptions in Ethiopia. In so doing, its aim is to enable relevant stakeholders to weigh ways of preventing or responding to network disruptions through legal means, including strategic litigation.

Secondly and related to the above is that the use of network disruption as a regulatory tool in Ethiopia is bound to increase. This is mainly because of the ever-growing polarization of politics fuelled by the ongoing civil war(s) and inter-communal conflicts engulfing the nations. Violent protests orchestrated via social media platforms have been common trigger factors for network disruptions in Ethiopia. Added to the impending — and already disputed national elections, the ruling partly is likely to resort to network disruptions to quell the inevitable violence after the elections. This *Legal Guide* would help stakeholders in taking proactive measures against network disruptions.

Thirdly, the role of stakeholders in addressing the problem of network disruptions is not entirely clear. While civil society groups working on digital rights have surfaced in the last few years, they lack clarity as to what they should do in addressing recurrent network disruptions. A survey of relevant stakeholders revealed that while most are yet to take the matter seriously and roll out strategies to address the wide-ranging impact of network disruptions. For instance, Setawit Movement, which seeks to advance the right of women, is yet to go beyond pushing the government to address the problem of gender-based violence, and address the impact of network disruptions in enabling it.[25] Similarly, EHRCO, a longstanding human rights civil society group in Ethiopia, is also yet to take steps beyond condemning arbitrary network disruptions.[26] Part of the reason for this reticence on the part of these stakeholders is lack of clarity as to what steps key stakeholders may take in response to network disruptions. This lack of awareness extends to other stakeholders including the government. With telecom liberalization now set to allow a new telecom operator,[27] the private sector would also be in need of legal guidance to address network disruptions. By outlining who is best-placed to do what in predicting, preventing and responding to network disruptions, this *Legal Guide* would help bring clarity on the respective role of relevant stakeholders. And this would, in turn, help avoid institutional rivalry or redundancy.

Further underlining the need for some form of legal guidance is the increasing impact of network disruptions in Ethiopia. Several studies have documented the cross-cutting impact of network disruption including human rights,[28] economic productivity[29] and social impacts.[30]

[25] Interview with Kalkidan Asmamaw, Digital Communications Manager at Setawit Movement, held on 5 April 2021.
[26] Interview with Tesfaye Gemechu, Coordinator at Ethiopian Human Rights Council, held on 6 April 2021.
[27] Note that in late May 2021 the government granted a telecom license to a global consortium of telecom operators. The government has also disclosed its intention to float another bid to license the second private operator. See Ethiopia Awards Telecom License to Safaricom-led Consortium (Al Jazeera, 22 May 2021) <https://bit.ly/3feS4bU>.
[28] See, e.g., GNI (n 11) 10.
[29] See, e.g., A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa (CIPESA, 2017); The Economic Impact of Disruptions to Internet Connectivity (Deloitte, 2016).
[30] See, e.g., Life Interrupted: Countering the Social Impacts of Network Disruptions in Advocacy in Africa (GNI, 2021).

While disrupting communication networks might offer tentative reprieve from the impugned content, the root causes of exam cheating, social unrest or recurrent political crisis could not be addressed by curbing the flow of information for a period of time. In that sense, network shutdown is an essentially ineffective regulatory tool. Although technological uptake in Ethiopia is still lower, preliminary reports have already shown the significant economic impacts of network disruption in Ethiopia. A recent report by Paradigm Initiative, for instance, has estimated that Ethiopia loses about $4 million daily due to Internet shutdowns.[31] As the Internet and allied technologies increasingly become essential in commerce and the provision of public services, the economic implications of network disruptions will be higher.

Interviews with relevant stakeholders have also revealed that network disruptions have considerably impacted vulnerable groups particularly minority groups and women in Ethiopia. The impact of network disruptions on women is recognized by civil society groups working on the rights and welfare of women. A participant outlined the two common ways in which network disruptions affect the rights and welfare of women as follows:

> First, during a network disruption, women subjected to a certain type of violence are unable to call the police or alert neighbours. Victims of intimate partner violence or domestic violence usually cope up from such trauma through a support system such as by calling a friend or loved ones. That there is network disruption would make such a support system difficult to access and might have a negative psychological effect on women. Second, network disruption affects the ability of women who are ill or are about to give birth, to gather information and medical advice, including on where to go.[32]

This account is supported by another interviewee, a law student at Addis Ababa University and who is from the Tigray region, where there is still network disruption in place.[33] According to him, pregnant women had to give birth in their homes, and on streets due to the unavailability of a network to call an ambulance. The participant described the impact in Tigray, where there has been compete network backout since 4 November,[34] as follows:

> First, because banks are closed – and still are in many places – and that electricity unavailable in many towns and cities, people were not able to withdraw cash to pay for basic items needed for survival. This meant we have been forced to eat 'Kolo' (a roasted cereal eaten often as a snack) for several weeks. I have 3 baby brothers of 3,4 and 6 years old who do not understand the situation so they used to beg our mom for proper meals. Now I am here in Addis Ababa for educational purposes but I have not

[31] Digital Rights in Africa 2019 (Paradigm Initiative, 2019) 17.
[32] Interview with Kalkidan Asmamaw, Digital Communications Manager at Setawit Movement, held on 5 April 2021.
[33] Interview with Kalayu Hagos, Third Year Law student at Addis Ababa University and who has been in Tigray for the first few months of the network disruption in the region, held on 2 April 2021.
[34] Note that while the Internet remains shut at the time of writing — i.e., late April 2021, mobile phone services were available intermittently in some parts of Tigray. See, e.g., Internet Disrupted in Ethiopia as Conflict Breaks out in Tigray Region (Net Blocks, 4 November 2020) <https://bit.ly/3snEdU4>; Ethiopia's War-scarred Tigray Region Regains Some Services (Reuters, 14 December 2020) <https://reut.rs/3e60jWe>.

> been able to meet my family through phone as there is still no network. My family is also not transferring me any money as banks remain closed.[35]

Participants from Siqqee Scholars, a women rights advocacy initiative in Ethiopia, highlighted a series of challenges presented to women by network disruptions.[36] These include impeding access to vital information, particularly on issues regarded as taboo, disrupting women's expression, mobilization and representation, and undermine their ability to make informed participation in political processes like elections and generally perpetuates inequalities.

Hardships caused by network shutdowns such as the inability to access banking services have also been experienced in Wollega, where there are still partial disruptions. Obsa Degabasa, who is a lecturer at Wollega University and a PhD student at Addis Ababa University, confirmed the ongoing challenge in obtaining banking services due to recurrent network disruptions in most parts of Wollega.[37] This is further reinforced by another participant from Wollega who not only stated his inability to contact his family for about six months but also unable to receive pocket money from his family due to lack of banking services.[38]

Network Disruptions in Ethiopia: In Search of a Legal Basis

Although the Ethiopian government resorts to network disruption often, it barely provided a coherent and plausible legal justification. As shall be highlighted in this section, the government provided a justification only recently – and rather in a passing – while it responded to a country visit report of the United Nations (UN) Special Rapporteur on Freedom of Expression, David Kaye. This disinterest in properly grounding a repetitive but far-reaching measure like network disruption is striking. A further reflection of this apathy is that relevant government departments never invoked the rather sensible legal basis for network disruptions provided in the Basic Texts of the International Telecommunication Union (ITU) to which Ethiopia has been a member since 1932.[39] ITU's Constitution recognizes the right of States to permanently 'cut off' or suspend international telecommunication services.[40]

Of course, two requirements should be fulfilled to cut off telecommunication services pursuant to this law. One is that that the measures must have a legal basis in national law, and second, the measure should be taken to avert national security threats, violations of national law or to protect public order or decency. Notable about this proviso is that there must exist a legal basis for the measure in national law which is currently lacking in Ethiopia.

[35] Interview with Kalayu Hagos, Third Year law student at Addis Ababa University and who has been in Tigray for the first few months of the network disruption in the region, held on 2 April 2021.
[36] Interview with Heran Birhanu, Administrative Lead at Siqqe Scholars, held on 12 April 2021.
[37] Interview with Obsa Degabasa, Lecturer at Wollega University and PhD Student at Addis Ababa University, held on 31 March 2021.
[38] Interview with Lami Tesfaye, Third Year Law student at Addis Ababa University and a resident of Kellem Wollega, held on 2 April 2021.
[39] See details at <https://www.itu.int/online/mm/scripts/gensel8>.
[40] Constitution of the International Telecommunication Union (1992, as amended) Arts 34(2), 35. See also International Telecommunication Regulations (2012) which, under Art 9, recognizes the right of member states to suspend international telecommunication services.

States may also suspend telecommunication services without invoking any national law or the necessity of guarding national security, in which case the state must notify the Secretary General of the ITU of the measure taken and when it would come to an end. Moreover, the scope of this measure is restricted to 'international telecommunication service', a service that connects more than one country.[41] This suggests that the envisaged power of cutting off or suspending telecom services does not extend to national telecom services. The International Telecommunication Regulations also require states to comply with their human rights obligations when implementing ITU instruments, including when exercising their power of cutting off or suspending international telecommunication services.[42] The upshot is that it would have made more argumentative sense had the Ethiopian government invoked ITU's instruments to justify network disruptions as opposed to its lumbering justification considered further below.

This section considers the questions of whether and to what extent that Ethiopian law provides a sound legal basis for network disruptions. It closely examines the government's recent legal justification offered for disrupting communications networks. It also considers recent attempts at introducing rules governing network disruptions in Ethiopia. Furthermore, this section discusses why and how the current cybercrime legislation provides a defensible legal basis for certain forms of network disruptions.

Legal Justifications of the Government for Network Disruptions— and Their Limits

As highlighted above, the Ethiopian government has rarely offered legal justifications for network disruptions. Under what legal basis the government restricted Internet access for several days, and sometimes, months is unclear. Often, the government presents lumbering defences for its opaque shutdown practices. One recalls here the claim that since the Internet is neither water nor air; it could be shut when the government deems there is a threat to national security.[43] Mainly because of international pressure, particularly human rights organizations, the government has recently attempted to put forward a legal justification for network disruptions. Legal grounds often relied upon to disrupt communication networks may be grouped into three. One is what may generally be referred to as national security legislation where the government invoked the powers of the Information Network Security Agency (INSA) to shutdown the Internet for addressing national security threats. The second legal basis concerns martial laws which have been enacted in Ethiopia multiple times for the past six years. While such laws provide a relatively explicit legal basis for communication disruption, the government has not invoked them publicly to defend network disruptions. Yet another potential legal basis for network disruption are conditions attached to telecom licenses which are used elsewhere to order network shutdowns. Now that a private telecom operator is awarded a license to enter the market – and the monopoly has essentially ended,[44] license conditions may be relied upon by the government to order and/or justify network

[41] See International Telecommunication Regulations (2012) Art 2.3.
[42] *Ibid*, Preamble.
[43] Twitter Backlash after Ethiopia PM's Internet 'Not Water or Air' Threat (Africa News, 3 August 2019) <https://bit.ly/3s3b7Jv>.
[44] See Press Release: Final License Issued (Ethiopian Communications Authority, 14 July 2021) <https://eca.et/2021/07/14/final-license-issued/>.

disruptions. What follows explores these possible grounds for network disruptions, and highlights their limits.

National Security Legislation

The first ever official legal justification for network disruptions is offered by Ethiopia's Federal Attorney General. This justification appears to be provided rather incidentally in its formal comments on a report of the UN Special Rapporteur on Freedom of Opinion and Expression that, *inter alia*, lamented government shutdown practices. In his post country visit report, the Special Rapporteur argued that Ethiopia continues to shut down the Internet without any apparent legal basis.[45] And shutdowns undertaken without any legal basis or pursuant to vaguely formulated laws – and often covertly, violate the requirement under Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR) — to which Ethiopia is a state party since 1993 — that restrictions be 'provided by law'.[46] Shutdowns must also be necessary to achieve aims specified in Article 19 (3) of the Covenant, and shutdowns often fail to meet this requirement.[47]

In Para 20 of the 'Comments by the State', the Attorney General provides the following:[48]

> Paragraph 51 and 52 — With respect to the statement that the government shuts internet without an obvious legal basis, we would kindly request the special rapporteur to observe to the following points. First, according to proclamation no 808/2013 which re-establishes Information Network Security Agency, the agency among others is vested with the power to keep the country safe from any threats against national security and it can take measures when the necessity arises. Further can be looked into article 6 of this proclamation which details the powers and functions of the agency. Second, the Ethiopian (sic) constitution is progressive in recognizing the right to freedom of information. Under article 29 (2), it has guaranteed a freedom to seek, receive and impart information and ideas of all kinds. Moreover, under the same article sub article 3, access to information of public interest is guaranteed. However, as it is enshrined under international law governing the subject whom Ethiopia is also a party to, clearly specified that these rights are not absolute and derogations with in the established scope are permissible. The limits Ethiopia have incorporated under article 29 (6) of the constitution are verbatim of those specified under article 19 of Universal Declaration of Human Rights and article 19 sub article 3 of ICCPR. In conclusion, we would like to reaffirm that these measures are exercised seldom with maximum restraint and are solely confined to the requirements of legality, legitimacy, necessity and proportionality.

This casual legal justification has two prongs. The Attorney General notes that the 2013 law which re-established INSA empowers the Agency to 'keep the country safe from any threats against national security and it can take measures when the necessity arises'. According to

[45] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Visit to Ethiopia, UN Doc A/HRC/44/49/Add.1 (29April 2020) Para 51.
[46] *Ibid*, Para 50.
[47] *Ibid*.
[48] Comments by the State on the Report of the Special Rapporteur on the Promotion and Protection of the Freedom of Opinion and Expression on His visit to Ethiopia, UN Doc A/HRC/44/49/Add.3 (15 April 2020).

the Office, this law provides a legal basis for Internet shutdowns. Read closely, this statement of the Attorney General also suggests that the law in question does not provide a legal basis for other forms of network disruption such as targeted blocking of websites, apps and throttling. And hence such measures of the government in the past have all along been admittedly unlawful. But a closer look at this law does not support the Attorney General's claims. Nowhere in this law the Agency's power of cutting Internet access for national security purposes is explicitly stated or remotely implied. The closest this law comes is when it empowers INSA to take 'counter-measures' for cyber-attacks. Among the powers and duties of the Agency include taking 'all necessary counter-measures to defend any cyber or electromagnetic attacks on information and computer-based infrastructures or systems or on citizens' psychology'.[49]

As the nation's cyber command, this proviso simply empowers INSA to take counter-measures – otherwise called 'strike-backs' – against perpetrators of cyber-attacks against the nation's critical infrastructures like power grids and 'citizens' psychology'. Cyber-attacks are defined broadly in the law to include 'destruction of computer-based critical infrastructures or disruption of their services or obliterating the confidentiality, integrity or availability of information or computer-based psychological attack on citizens or digital identity theft perpetrated by different techniques'.[50] Strike-backs are sort of 'in-kind' retaliations by resorting to proportionate cyber-attacks.[51] If the attack was – for instance – in the form of Distributed Denial of Services (DDoS) attacks, the Agency may retaliate with similar DDoS attacks or large-scale spreading of malware.

This then would mean two things. For one, when cutting Internet access, INSA would not be engaging in lawful strike-backs envisioned in its establishment law. Instead, it simply is unlawfully restricting the individual right to free expression, including to access information off the web. Second, most trigger factors for Internet shutdown in Ethiopia, such as social media disinformation or hate speech, do not really fall under the rubric of cyber-attacks imagined in the law. Online disinformation is a form of hybrid cyber threat but not quite a cyber-attack warranting lawful strike-backs. Even if it were, how would a State hit back proportionately against coordinated disinformation campaigns of non-State actors or loose youth online groups? How would INSA react to online attacks on 'citizens' psychology' regardless of what such attacks might mean? INSA had previously invoked a similar line of reasoning to justify the brief Internet blackout in December 2019. Then, INSA claimed the brief shutdown was needed to fend off active cyber-attacks against the nation, particularly financial institutions.[52] But this justification lacked any legal basis.

A subordinate piece of legislation meant to further INSA's re-establishment law does not use the term 'cyber attacks' but 'cyber operation'. INSA is empowered by this legislation to lead

[49] Information Network Security Agency Re-establishment Proclamation No 808/2013, *Federal Negarit Gazeta*, Art 6(4).
[50] *Ibid*, Art 2(5).
[51] See, e.g., Kenneth Himma, Ethical Issues Involving Computer Security: Hacking, Hacktivism and Counter-Hacking, in Kenneth Himma and Herman Tavani (eds), *The Handbook of Information and Computer Ethics* (Wiley, 2008) 206-207.
[52] Brief Internet shutdown in Ethiopia as a Cyber-attack Hits (Geneva Internet Platform, 5 December 2019) <https://cutt.ly/cc2qCnv>.

and coordinate cyber operations.[53] The Agency may carry out cyber operations on its own motion, based on a court order, orders of the federal government or request of regional governments.[54] But it is unclear whether cyber operations — not referred to in the INSA re-establishment legislation — are different from counter-measures. Cyber operation is defined as a 'technique' that is used to exploit cyber intelligence and digital forensic evidence, curb cyber activities that threaten national security and citizen's safety or defend state sovereignty from an attack by cyber and electromagnetic technologies.[55] This description suggests that cyber operations are not restricted to counter-measures, which are essentially retributions to earlier attacks, and include proactive measures such as the collection of signals intelligence. In that sense, cyber counter-measures fall into the Agency's broader power of engaging in cyber operations.

Now the question of whether disrupting communication networks falls within INSA's mandate to launch cyber operations, including counter-measures remains. Ethiopian law describes cyber operation as a 'technique' but it does not state what such techniques include. Could cutting off Internet access, blocking of websites/apps or throttling be taken as a technique? But more questionable is whether common trigger factors for network disruption in Ethiopia such as disinformation, hate speech, exam leaks or cheating are among factors warranting cyber operations. None of the grounds warranting cyber operations provided by law seems to capture these factors often mentioned as reasons for network disruptions. Cyber operations may be taken to achieve the following objectives: (a) to collect cyber information and digital forensic evidence, (b) to prevent cyber and electromagnetic attacks targeting national sovereignty, or (c) to prevent cyber actions that threaten national security or citizen's security.[56]

That a cyber operation is a 'technique' which probably only INSA has the capability to launch suggests that it does not include network disruption. Ethio-telecom is a state monopoly but it is still a (state) commercial enterprise. This would ordinarily mean that requests to disrupt networks would be sent/submitted to Ethio-telecom by the relevant government department. Often, Ethio-telecom redirects media and public queries about network disruptions to security and law enforcement departments.[57] When the impending telecom liberalization happens, similar requests or orders would be submitted by the government to the new operator. This would mean that network disruption is not probably the type of 'technique' considered cyber operation by the drafters of the law. A cyber operation is a measure that only INSA — and probably other government bodies — are able to engage in. So, this raises the question of what role INSA could have in the continuum of disrupting communication networks — is it submitting the shutdown/blocking instructions to telecom

[53] See Information Network Security Agency Re-establishment Proclamation Execution Council of Ministers Regulation No 320/2014, *Federal Negarit Gazeta*, Art 9 cum Art 2(5).
[54] *Ibid*, Art 9(2).
[55] *Ibid*, Art 2(5).
[56] *Ibid*, Art 9(1).
[57] See, e.g., Ethiopian Authorities Crack Down on Opposition Supporters with Mass Arrests: Amnesty (Addis Standard, 27 January 2020) <https://bit.ly/3wJDVdw>. Regarding the May 2021 blocking of Facebook, Instagram and WhatsApp, an unnamed official at Ethio-telecom stated to the media that the disruption was 'beyond the control of Ethio-telecom'. See, e.g., a tweet by the popular online media outlet in Ethiopia TIKVAH-ETHIOPIA at https://bit.ly/2SqjF0O [Tweet in Amharic: Author's translation].

operators or does it have the technical capability to 'kill the switch' itself? Its claim of carrying out the Internet shutdown in December 2019 suggests that it did/does still have the technical capability to kill the switch, but without the legal authority to do so.

Reading INSA's power of disrupting communication networks under its broader cyber operation mandate is also problematic in and of itself. This is mainly because of the way in which Ethiopian law frames the Agency's powers which raises human rights concerns. Except in the case where the cyber operation is based on a court order, an operation may be taken anytime based on mere instructions/request of the government (either federal or regional governments) or by the Agency on its own motion. This opens the door for arbitrary network disruption. Of course, the Agency is required not to disclose information obtained through cyber operations to third parties other than the requesting body.[58] But this does not sufficiently address the privacy concern raised by cyber operations. For one, the Agency may undertake invasive cyber operations without any oversight. Even though court warrant should be sought by the Attorney General to have cyber operations taken by the Agency, the fact that the federal government can still 'instruct' the Agency to carry out cyber-attacks without a court warrant renders the mandated judicial oversight nigh meaningless. This is another reason why 'cyber operations' are problematic avenues for disrupting communication networks.

The second part of the Federal Attorney General's legal justification is that Internet shutdowns are taken seldom with maximum restraint, and in line with international human rights and national constitutional standards of 'legality, legitimacy, necessity and proportionality'. But not only are Internet shutdowns occurring often — and at times, for an extended period of time thereby proving to be a disproportionate response — but they also lack clear legal basis thus failing to meet the requirements of 'legality'. This makes it immaterial to consider whether the other requirements of necessity and proportionality are fulfilled.

In sum, the national security legislation invoked to justify network disruptions does not hold up to closer scrutiny. That this law does not provide a tenable legal basis for deliberate disruption of communication networks highlights the need to introduce a pertinent legal framework governing network disruption.

Martial Laws

Martial laws, often enacted to 'suppress an invasion and restore law and order', traditionally empowered governments to disrupt communication services.[59] A 1934 statute in the United States, for instance, empowers the President to order the shutting down of communication during times of public peril and national emergency.[60] But martial laws are inherently intrusive, cumbersome and hence disproportionately restrict human rights and other legitimate interests. In the past few years, a Bill meant to curb this far-reaching power of the President has been tabled before the US Congress.[61] While never publicly invoked by the

[58] Regulation No 320/2014 (n 53) Art 9(4).
[59] See, e.g., Osborn's Concise Law Dictionary (12th Ed, Sweet Maxwell, 2013) 273.
[60] See Communications Act of 1934 (47 U.S.C. 606) Section 606.
[61] See Preventing Unwarranted Communication Shutdowns Act 2020, 116th Congress 2nd Session.

Ethiopian government to justify network disruptions, laws imposing State of Emergency (SoE) — also called 'martial laws' — provide a tentative legal basis for network shutdowns.

In the past few years, network disruptions in Ethiopia often followed declarations of state of emergency by the federal government. And decrees proclaiming a state of emergency — be it for defending the 'constitutional order' or ensuring public security — often empower a 'Command Post' instituted to enforce the decrees, including to order the shutdown of communication networks. A 2018 SoE Decree, for instance, empowers the Command Post to 'cause the closure or termination of any means of communication' should doing so be deemed necessary to protect the 'Constitution and constitutional order, maintain public and citizens' peace and security'.[62] The more recent SoE law was enacted after war broke out between TDF and the federal government in early November. This law institutes a SoE Task Force, a new term for 'Command Post', that is empowered to 'cause the closure or termination of any means of communication' when it is necessary to maintain the Constitution and constitutional order.[63]

The reliance on martial laws as a legal basis for network disruption raises a number of concerns. One is that SoE decrees permit sweeping human rights derogations. Except for a few sets of rights such as the rights to self-determination and protection against cruel, inhuman, degrading treatment or punishment, all other rights guaranteed under the Ethiopian Constitution may be derogated during the SoE.[64] This means that fundamental human rights such as freedom of expression would be derogated, including by measures like network disruptions. Because of the persistent security challenges the country has been experiencing since 2016, the government has proclaimed SoE several times, sometimes extending beyond the initial period of 6 months required by the Ethiopian Constitution. At the time of writing in late April 2021, a state of emergency is in place in the Tigray regional state where there is an ongoing war.[65] Most provinces of the Oromia regional state as well as the Benishangul Gumuz regional state are also being ruled by a Command Post while it is not clear if these administrative re-arrangements are based on a SoE decree. On 19 April 2021, the federal government declared a SoE in the 'special' Oromo provinces in Amhara regional state to address the growing violence.[66] The recurrent declaration of SoEs has essentially made them the norm while they are meant to be exceptional measures.

[62] See State of Emergency Proclamation Issued to Defend the Constitution and Constitutional Order from Threat Council of Ministers Proclamation No 2/2018, *Federal Negarit Gazeta*, Art 4(2) cum State of Emergency Proclamation Issued to Defend the Constitution and Constitutional Order from Threat Council of Ministers Proclamation No 1/2016, *Federal Negarit Gazeta*, Art 4(2).

[63] State of Emergency for the Protection of the Constitution and Constitutional Order Proclamation No 4/2020, *Federal Negarit Gazeta*, Art 4(5) cum State of Emergency Proclamation for the Prevention of Constitution and Constitutional Order No 4/2020 Ratification Proclamation No 1228/2020, *Federal Negarit Gazeta*.

[64] See Ethiopian Constitution, Proclamation No 1/1995, *Federal Negarit Gazeta*, Art 93(4).

[65] See Ethiopia Declares State of Emergency in Opposition-ruled Tigray (Al Jazeera, 4 November) <https://bit.ly/3v21g8F>. Note that the SoE was declared for a period of six months starting from 4 November 2020, and hence the decree should come to an end on 4 May 2021. It is unclear whether the SoE has been formally renewed but reports from the region indicated that prohibitions originally mandated in the SoE decree remained, to a degree, until the federal, Eritrean and Amahara militia were routed from much of the region.

[66] See Amid Violence, Ethiopia Declares State of Emergency in Amhara (Al Jazeera, 19 April 2021) <https://bit.ly/2Qi3Tof>.

Further complicating matters, SoE laws are not subject to any meaningful oversight to avert possible abuse in the course of implementation. The Ethiopian Constitution mandates the federal Parliament to institute a State of Emergency Inquiry Board to oversee the implementation of SoE decrees.[67] However, the Inquiry Board has largely advisory roles, its most significant but vague power being ensuring the prosecution of 'inhuman' acts committed in the course of enforcing the decree.[68] The Ethiopian Human Rights Commission (EHRC) has been recently empowered by law to 'monitor the human rights situation during a state of emergency'.[69] But it is unclear to what extent the Commission may see to it that human rights abuses are held to account during SoE. Its lacklustre response to the widespread, systematic and gross allegations of human rights violations in Tigray, which had been under martial law since early November 2020, appears to have undercut its credibility.[70]

Added to the recurrence of SoEs in Ethiopia, the reliance on martial laws as a legal basis for justifying network disruptions is worrisome. SoE is meant to be the exception but the multiple times that the government resorts to martial laws to address national security threats appear to be making them the rule. Even more worrisome is that SoE laws impose a strict duty to cooperate on 'any person' with SoE Task Force or Command Post.[71] This means that telecom operators, for instance, would have no room to resist orders of the SoE Task Force to disrupt communication networks. Failing or refusing to obey orders of the Task Force are subject to imprisonment of up to three years.[72]

Indeed, unlike national security laws, SoE laws provide not only clear provisions authorizing network disruptions but also indicate government entities meant to enforce them. For instance, the Task Force established to oversee the SoE in Tigray is led by the General Chief of Staff of the National Defence Forces.[73] In that sense, it may be taking to be relatively transparent. But besides the concerns highlighted above, martial laws offer only tentative reprieve from threats triggering SoE. That makes them impertinent legal basis for network disruptions.

Telecom License Conditions

In jurisdictions where no legal basis exists for ordering network disruptions — at least during peacetime, provisions in license conditions are often invoked to oblige telecom operators to disrupt communication networks. In Chad, Uganda and Cameroon for instance, national security clauses in license conditions that mandate 'cooperation' were invoked as legal basis by regulators to order shutdowns.[74] License conditions are compulsory terms, and often operators have little wriggle room to negotiate license conditions. Often, telecom laws

[67] See Ethiopian Constitution (n 64) Art 93(5) [Note, though, that while the Ministry of Defense did announce the decree to the media, it remains unclear if the decree was proclaimed, as constitutionally mandated, by the Council of Ministers].
[68] *Id*, Art 93(6(d)) cum Proclamation No 1228/2020 (n 63) Art 4(4).
[69] See Ethiopian Human Rights Commission Establishment (Amendment) Proclamation No. 1224/2020, *Federal Negarit Gazeta*, Art 2.
[70] See, e.g., Ethiopia's Human Rights Chief as War Rages in Tigray: 'We Get Accused by All Ethnic Groups' (The Guardian, 2 June 2021) <https://bit.ly/3znLtDw>.
[71] See, e.g., Proclamation No 4/2020 (n 63) Art 9.
[72] *Ibid*, Art 10(2).
[73] *Ibid*, Art 7(1).
[74] See How Telecom Companies in Africa Can Respond Better to Internet Disruptions (CIPESA Policy Brief, 2021) 2.

governing authorization and licensing provide that failing to comply with the conditions attached to the license would lead to the revocation of license. With their business interests at stake, telecom operators are likely to comply with network disruption orders based on license conditions.

Thus far, the fact that the communications sector has been a monopoly means the Ethiopian government did not have to rely on license conditions to compel Ethio-telecom to shut down the communication services. This is, of course, without losing sight of the fact that other government bodies like INSA may have the actual technical capability to 'kill the switch' without necessarily requiring the participation of Ethio-telcom. At least in one instance, as noted above, INSA has claimed to have briefly shut down the Internet. And this essentially means that license conditions are currently irrelevant to the Ethiopian case, at least for now. This situation would change soon as the new private telecom operator enters the market. Obviously unable to kill the switch off itself — unless it does switch it at a 'gateway' level[75] — and if it is not during a SoE, the government might resort to license conditions to order network disruptions.

Under Ethiopian telecommunications law, one of the grounds for the revocation of telecom license is failure to comply with license conditions. Revocation will take effect when a licensee fails to rectify the breach within fourteen (14) days after the sector regulator — the Ethiopian Communications Authority (ECA) — notified the licensee of the breach.[76] Another broader ground is when licensees act in a way that is in conflict with public interest.[77] This provision is framed in such a broad way that ECA may invoke it to revoke a license for failing to comply with shutdown orders. The law also vaguely empowers the Communications Authority to set any license conditions that may help achieve its legislative objectives.[78] And the prime objective of the law is to help deliver high quality, efficient, reliable and affordable communication services throughout the nation.[79] This might mean that license conditions that undermine, for instance, human rights of users, might be introduced by ECA so long as the economic rationales of the law outweigh. Moreover, ECA is empowered to amend license conditions only within a month of notice, during which telecom operators may submit non-binding feedback.[80]

There are, of course, two instances where such expansive powers of the ECA appear to be mitigated. One relates to the development of license conditions. The Communications Service Proclamation provides that the development of license conditions should be guided by principles of transparency, fairness and non-discrimination, among other considerations.[81]This signals the possibility for relevant stakeholders, including civil society groups and telecom operators, to take part in the development of license conditions. This might help ensure that license conditions uphold the rule of law and fundamental human

[75] *Ibid*, 4 (Reporting that in Guinea the sector regulator had cut Internet connection at the international gateway).
[76] See Communications Service Proclamation No 1148/2019, *Federal Negarit Gazeta*, Art 34(2(b)).
[77] *Ibid*, Art 34(2(i)).
[78] *Ibid*, Art 21.
[79] *Ibid*, Art 5.
[80] See Telecommunications Licensing Directive No 792/2021 (ECA, 2020) Art 9.
[81] *Ibid*, Art 20(4).

rights. The other instance is the possibility of offering feedback to ECA during the revision of license conditions. The views of telecom operators offered during such a process are non-binding, but it offers an opportune occasion to help shape the development of fair and clear license conditions, including when and how they may be requested to take network disruption measures. As shall be highlighted in the next section, this is an area where civil society groups as well as (future) telecom operators may play an active role as part of their broader effort against arbitrary practices of network disruption.

As the above sketch of the legal landscape suggests, Ethiopian law does not provide a sound and firm legal basis for network disruptions. But recent years have seen efforts of introducing rules governing network disruptions in Ethiopia. What follows considers one such development, namely network disruption standards envisaged in the draft cybercrime legislation, and highlight their limits.

Emergent Legal Standards on Network Disruptions—and Their Limits

The cybercrime Bill (2020), which is slated to replace the current Computer Crime Proclamation (2016) introduces a legal framework for three forms of network disruption; namely Internet shutdowns, blocking and filtering.[82] Tucked in Part III of the Bill that deals with content-related crimes, it stipulates that such measures should be: (a) undertaken in a transparent manner, (b) subject to legal challenge by affected persons, (c) based on prior court order and (d) taken to achieve specific legitimate aims such as national security and public health. The Bill further requires service providers to notify users and the general public of an impending network disruption.[83] The initiative to ground network disruptions on a firm legal basis — and with some human rights safeguards is commendable, though it brings along a number of questions.

One such concern is that it is not entirely clear how network disruption is related to cybercrime law. The legislative objective of any cybercrime legislation is to lay out rules for the criminalization, investigation and prosecution of crimes committed through the use of or against computer systems.[84] It goes well beyond the scope of cybercrime legislation to institute a legal framework for network disruptions. Perhaps, the best way forward is to relocate this provision – with appropriate changes – elsewhere, probably in a subordinate legislation to INSA's establishment legislation, or a new freestanding piece of legislation. In countries such as India, rules authorizing network disruptions are enshrined in secondary legislation.[85] As shall be discussed in the following section, the current cybercrime legislation provides a defensible legal basis for certain forms of network disruptions. But the question of formal pertience will remain.

[82] See Draft Computer Crime Proclamation (2020) Art 22 cum Art 2(15-17).
[83] The term 'service provider' is defined in the cybercrime Bill broadly as 'a person who provides technical data processing, storage or communication service or alternative infrastructure to users by means of computer system', and arguably includes telecom operators. See *Id*, Art 2(20).
[84] See, e.g., Understanding Cybercrime: Phenomena, Challenges and Legal Response (ITU, 2012) 3.
[85] See Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 [Enacted by the Central/Union government of India pursuant with section 7 of the Indian Telegraph Act, 1885].

Beyond the question of formal pertinence, the rule governing network disruption is beset by further conceptual ambiguities. First, it states that network disruption measures would be taken when orders are given by a 'competent body' to service providers.[86] But it is not clear which department of government is given this far-reaching power – is it INSA, the Office of the Attorney General, National Intelligence and Security Service (NISS) or the Federal Police? Art 22(3) of the Bill suggests that the envisioned competent body is not a single government department but several bodies: 'service providers, the agency [INSA] or any other government body'. While leaving this discretion to a number of bodies is problematic in and of itself, it is also odd how 'service providers' are seen as decision-makers vis-à-vis network disruptions. What is clear, however, is that the envisioned 'competent body' is not the judiciary. This is a major misstep for a revision project whose prime goal is entrenching human rights protection in cybercrime prevention, investigation and prosecution. Orders for network disruption should always be given by an independent and impartial tribunal. Otherwise, the incidence of such orders would continue unabated, and *post facto* options of judicial recourse to challenge the measures would do little to remedy damages already sustained. Perhaps, the requirement of court order might be waived in exceptional circumstances that dictate immediate measures but judicial review should be mandated at a later stage – e.g. within 48 hours.

Second, the provision stipulates that 'any affected party' may challenge before courts 'decisions of service providers, the Agency or any other government body'.[87] At least two questions arise here. For one, does this right to institute a legal challenge apply before the measures are taken or only after the fact? The term 'decision' suggests that the legal challenge may be launched before the decision to, for instance, shutdown the Internet is implemented by service providers. And this reading of the provision also finds support from the duty of notification, discussed further below, on service providers regarding impending measures. But it is still vital to clarify this point. Secondly, what constitutes being 'affected', and who would be considered an 'affected party' in the context of network disruptions is not also straightforward. Would ordinary Internet users whose access to the Internet is cut due to Internet shutdowns be considered an 'affected party' that may lodge a legal challenge? Would businesses such as banks whose services rely on the availability of network be able to legally challenge network disruptions? How about civil society groups – would they have a standing for judicial recourse? Such questions remain unanswered. In light of the recurrence of network disruptions in Ethiopia, it is vital that civil society groups are bestowed a legal standing on behalf of ordinary users and the public.

Third, the provision envisages a notification regime by which service providers 'should notify their users accordingly and should provide sufficient information to the public about the order and action taken'.[88] Ambiguous about this proviso concerns as to when the notice should be provided – is it before or after the network disruption? The terms 'order and action taken' suggest it is *post facto* notification, after the service provider cut the Internet, blocked websites or began filtering content. If the notice were to be provided before the fact, it would

[86] Draft Computer Crime Proclamation (2020) Art 22(4).
[87] *Id*, Art 22(3).
[88] *Id*, Art 22(4).

allow 'affected parties' to launch a legal challenge to prevent the impending network disruption. But the notice regime would offer little if the notification comes after the fact, especially when the measures would cause irreparable losses, be it material or otherwise. *Ex post* notices would be useful only if the loss sustained due to the network disruption can be recuperated, for example through damages/compensation. To make the notice rules more effective, the best way forward is to envisage a two-pronged notification regime. *Ex ante* notices should be provided to users before measures are taken and *ex post* notices only for urgent cases. In the latter case, the relevant government body may seek a court order and have network disruptions taken in exceptional cases, which should be followed by ex-ante notices.

Apart from these substantive lapses, these standards provide the baseline for a freestanding legal framework for network disruptions, however. As highlighted above, cybercrime legislation is not where such standards belong. The best way forward then is to relocate these standards to a freestanding legislation, probably in a freestanding subsidiary piece of law. If INSA plays the central role — as it claims it does — in the network disruption continuum, such a secondary legislation may be enacted as a Directive by the Agency. But till such legislation is introduced, a sensible legal basis for certain forms of network disruption can be found in the currently operative cybercrime legislation, as the next section illustrates.

The Cybercrime Legislation as a Defensible Legal Basis for Network Disruptions

Ethiopia's current cybercrime law arguably offers a defensible legal basis for network disruptions. Article 32(5) of the legislation which is located in the evidentiary and procedural parts of the law, provides as follows:

> Where the investigatory organ finds the functioning of a computer system or computer data is in violation of the provisions of (sic) this Proclamation or other relevant laws, it may request the court to order for such computer data or computer system to be rendered inaccessible or restricted or blocked. The court shall give the appropriate order within 48 hours after the request is presented. [Emphasis added]

The 'investigatory organ' envisaged in this provision is the Executive Task Force that is led by the Federal Attorney General, and includes the Federal Police Commission and INSA.[89] Its power includes having a given 'computer system' or 'computer data' rendered inaccessible or blocked based on a court order where its functioning violates the cybercrime law or any other relevant legislation. The first key question is whether disrupting communication networks like the Internet would fall under this provision. The law defines 'network' as the 'interconnection of two or more computer systems by which data processing service can be provided or received',[90] and this clearly captures the Internet. The law further defines the term 'computer system' together with 'computer' and hence is not entirely instructive.[91] In light of the fact the interconnection of 'computer systems' essentially creates a 'network', it

[89] Computer Crime Proclamation No 958/2016, *Federal Negarit Gazeta*, Art 41 cum Arts 38-39.
[90] *Ibid*, Art 2(8).
[91] *Id*, Art 2(3).

can be argued that the power of seeking the blocking, restriction or making computer systems inaccessible would include networks like the Internet. But the same cannot definitively be said for other telecommunication services because the definitions center around computers. In that sense, the scope of permissible network disruption is narrower. Likewise, the definition of 'computer data' essentially captures web content, thereby allowing blocking of specific websites found to be disseminating problematic content.[92]

A key point in this provision is that it allows measures of blocking or blackout even when violations of not just the cybercrime legislation, but also other Ethiopian laws occur. That means when the alleged infringement concerns, say the recent hate speech and disinformation legislation, investigators could seek a court order to have delinquent websites blocked and arguably have Internet access restricted. What makes this plausible is that the Office of the Federal Attorney General, the lead 'investigatory organ' under the cybercrime law, is also tasked to investigate and prosecute hate speech and disinformation.[93] This would potentially meet the requirement of legality by providing some legal basis for Internet shutdowns, among other modes of network disruption.

A virtue of this proviso, though, is that it embodies an important safeguard against potential arbitrariness. Any measure of restricting Internet access or blocking particular websites requires a prior court warrant. Before deciding whether to grant the request, the relevant court should establish whether the sought measure is necessary and proportionate in light of international human rights standards and the Ethiopian Constitution. In undertaking the balancing, the Court would/should consider at least two issues: (a) whether, for instance cutting Internet access, is necessary to fulfil a certain legitimate aim (for instance, maintaining public order); (b) whether taking that measure would be proportionate to the objective. This rigorous balancing exercise would not only help prevent arbitrary shutdowns but also keep the recurrence of the measures to the minimum.

Established jurisprudence elsewhere suggests that in addition to the requirement of a prior court order, other additional safeguards are needed to upend the wide-ranging impact of network disruption. In a series of recent decisions against Russia, the European Court of Human Rights held that beyond judicial warrant, network disruptions like website blocking warrant further safeguards.[94] One such safeguard is the need to provide in advance notice of the impending measures to parties whose interest might be affected by the blocking order. With the Internet becoming increasingly a critical utility for the provision of public services and commercial activities, the importance of a heads up on planned network disruption cannot be overemphasized. No such safeguards are provided in the cybercrime legislation, further reinforcing the need for tailored rules governing network disruptions.

[92] Id, 2(4) ['computer data' is defined as any content data, traffic data, computer program, or any other subscriber information in a form suitable for processing by means of a computer system].
[93] See Hate Speech and Disinformation Prevention and Suppression Proclamation No 1185/2020, *Federal Negarit Gazeta* cum Federal Attorney General Establishment Proclamation No 943/2016, *Federal Negarit Gazeta*, Art 6(3).
[94] See *Vladimir Kharitonov v. Russia* (application no. 10795/14), *OOO Flavus and Others v. Russia* (application nos. 12468/15, 23489/15, and 19074/16), *Bulgakov v. Russia* (application no. 20159/15), and *Engels v. Russia* (application no. 61919/16).

As the above discussion illustrated, the current cybercrime legislation provides a legal basis for certain types of network disruptions. But it also has limitations. At the most basic level, the question of formal pertinence arises – is cybercrime legislation where such standards belong? But more importantly, the cybercrime legislation does not envisage circumstances where third parties such as civil society groups may take legal actions against arbitrary network disruptions. This is exacerbated by the 48 hours period limit within which courts must respond to investigators' request for an order making it harder for intervention by interested parties. In terms of scope, the legislation applies only in scenarios where there was a legal violation. In that sense, it comes after the fact. This set of limitations of the cybercrime legislation reinforces the need for a fully-fledged legal framework on network disruptions.

Network Disruptions and the Role of Stakeholders in Ethiopia

The arbitrary nature of network disruptions — and their considerable impact in Ethiopia — is yet to be properly recognized. Thus far, international human rights organizations have been at the forefront of condemning network disruptions and highlighting their cross-cutting impacts.[95] With increasing access to the Internet — and its role in the nation's economy, local actors including the growing tech sector have begun to feel the brunt of network disruptions.[96] This may also help raise awareness about and the need for addressing the arbitrariness in routine disruption of communication networks. The formation of NDRE for instance, is directly motivated by the problem of recurrent and arbitrary network disruptions.[97] Despite this rise in awareness — and the drive to meet the challenge, there is a lack of clarity as to who should do what and when in dealing with network disruptions. In particular, the respective role of government institutions, civil society groups and the private sector in predicting, preventing and responding to network disruptions is not entirely clear. In an attempt to address this lacuna, this section considers the respective role of relevant government institutions, civil society groups and the nascent private sector vis-à-vis network disruptions in light of either their statutory mandate or organizational mission.

The Role of Government Institutions

The frequent resort to network disruptions in Ethiopia suggests that the government has seen value in it as a tool of addressing national security threats. But the failure to provide a clear legal basis or any explanations has been scandalous. Government departments issuing network disruption orders need to do so publicly with clear justification. This would require them to invoke some legal ground to justify the measure, and why that measure is necessary to achieve a particular objective. More such transparency would be beneficial in at least three ways. First, that the government would be pressured to explain its actions means its recurrence may diminish overtime. Second, that the reasons for and legal basis of the shutdown are known means stakeholders may orient their responses accordingly, including

[95] See, e.g., Ethiopia: Communications Shutdown Takes Heavy Toll: Restore Internet, Phone Services in Oromia (Human Rights Watch, 9 March 2020) <https://bit.ly/3aNihM3>.
[96] See, e.g., Ethiopia's Tech Start-ups are Ready to Run the World, But the Internet Keeps Getting Blocked (Quartz Africa, 18 June 2019) <https://bit.ly/3aEKIMu>.
[97] See details at NDRE's websites <https://ndrethiopia.org/>.

through legal means. The arbitrary nature of network disruptions may have played a part in undermining the role of civil society groups in Ethiopia to take strategic measures. Third, providing an explanation would reduce reputational damage as well as the socio-economic and rights implications of network disruptions. What follows lays out specific steps that may be taken by government departments that are directly involved in or whose statutory mandate is directly engaged in arbitrary network disruptions.

Information Network Security Agency

INSA is a federal body tasked with a wide-ranging responsibility of enhancing and ensuring the nation's cyber security. The Agency is often associated with network shutdowns in Ethiopia, and indeed it has at least in one occasion claimed responsibility for killing the switch. However, the question of whether — as shown above — INSA has, indeed, such power of disrupting communication networks remains. Despite the arguments of the government, no law in Ethiopia empowers the Agency to take such a far-reaching measure. Of course, it would be straying away from the Agency's prime legislative objective of securing the nation's cyber infrastructure (and citizens' psychology) from malicious cyber-attacks. This legal ambiguity aside, it is vital that the role of the Agency in the overall continuum of disrupting communication networks is properly defined. The principle of legality in international law and the Ethiopian Constitution dictates that measures that restrict human rights such as freedom of expression are envisaged in a clear and accessible law. The reliance on a vague legal basis like INSA's re-establishment legislation would, therefore, fail this standard. To address this lapse, INSA should adopt a subordinate piece of legislation that outlines how and when it may legitimately disrupt communication networks. Such legislation should also envisage mechanisms by which stakeholders may lodge protests against network disruptions. Indeed, INSA is already empowered by its re-establishment law to issue directives, subordinate pieces of legislation in the hierarchy of laws in Ethiopia, to further its statutory functions.[98] Perhaps the plausible way forward is to relocate the network disruption legal framework envisaged in the cybercrime Bill (2020), with further amendments, to a future Directive to be issued by INSA.

Government Ministries with Specific Mandates

Government ministries and commissions such as the Ministry of Innovation and Technology, Ministry of Revenue, Ministry of Women, Children and Youth, EHRC and Planning and Development Commission are among government bodies whose mandate relate in one way or another to the incidence of network disruptions in Ethiopia. It thus is critical that these entities take certain steps so that network shutdowns do not continue to undermine their statutory responsibilities and mission. This is quite vital for two interrelated reasons:

Firstly, these government entities are tasked with supporting the nation's socio-political and economic transformation through and by ICTs. But the recurrence of network disruptions in Ethiopia undermines the statutory mission of these institutions. Network disruptions impact the economy, trade, provision of essential services such as emergency health care and financial services. Among government departments with a specific mandate concerning the

[98] Proclamation No 808/2013 (n 49) Art 11(2); Regulation No 320/2014 (n 53) Art 22.

economy is the National Planning and Development Commission. The Commission, for instance, has recently launched an ambitious 10-year development plan which hopes to transform the nation's economy, including its nascent digital economy.[99] The Ministry of Innovation and Technology is another ministry that has assumed the specific statutory responsibility of nurturing a digital economy.[100] With the increasing reliance on communication technologies for the provision of health and financial services, Ministries of Health and Finance should direct their attention to the impact of arbitrary and recurrent network shutdown.

As the nation moves to embrace technology in both modernizing the administration of taxes, and as a potential revenue base, the Ministry of Revenue should also be concerned by the long-term public finance implications of network shutdowns. The Ministry of Education should also be alarmed by the impact of network disruptions — often triggered by exam leaks — especially the signficant finacial loses as well as disruption on the normal teaching-learning process. In attending to the counter-productive effects of network disruptions, these government bodies should bring more attention to the problem internally within the ranks of government. In particular, they should engage with other departments of the government that are directly involved in ordering or effecting network disruptions. In so doing, the concrete cross-cutting impacts of network disruptions particularly on the economy, should be communicated. This would go a long way in shifting the government's misguided attitude about network disruption to deal with the underlying socio-political problems.

Secondly, a number of government organs are tasked to protect the rights and welfare of citizens, including vulnerable groups such as women, children and persons with disabilities. For instance, the Ministry of Labour and Social Affairs is tasked with ensuring the socio-economic well-being of persons with disabilities, whereas the Ministry of Women, Children and Youth has a statutory responsibility to improve the welfare of women and children.[101] Thus far, these ministries do not appear to officially recognize the impact of network disruptions on the welfare and wellbeing of vulnerable groups under their mandates. As highlighted above, network disruptions seriously affect, *inter alia*, the ability of women to get emergency health services. One step that these bodies can take is to properly recognize the impact of network disruptions, and reorient their operations. Raising the impact of arbitrary and recurrent network shutdowns at the highest levels of government, e.g. Cabinet, would also be crucial in changing the overall governmental attitude towards the utility of network disruptions.

Thirdly, EHRC is the national human rights institution tasked to promote and protect human rights. As a government human rights body, the Commission hardly enjoyed a modicum of public trust and confidence. One of the lauded but quickly diminishing legal reforms in the country launched since mid-2018 has been to enhance the Commission's institutional autonomy and credibility. While questions of independence persist, the Commission appears

[99] See Ten-Year Development Plan of Ethiopia: 2020/21 – 2030/31 (Planning and Development Commission, 2020) 32, 144.
[100] E-transaction Proclamation No 1205/2020, *Federal Negarit Gazeta*, Arts 5-6; Definition of Powers and Duties of the Executive
Organs of the Federal Democratic Republic of Ethiopia Proclamation No 1097/2018, *Federal Negarit Gazeta*, Art 20.
[101] Proclamation No 1097/2018 (n 100) Arts 28, 29.

to have become more active in promoting and monitoring human rights. But upholding human rights in the digital context is yet to come within the Commission's radar. In part, this is because of the countless human rights violations occurring in the country due to armed conflicts in different corners of the country. As a result, EHRC is yet to comment or seek justification from the government on network disruptions. Network disruptions impact a broad range of rights, with its recurrence in the past few years — and counting, the Commission should recognize network disruptions as a human rights problem and retool its human rights response mechanisms to address the problem.

Added to the effort of other stakeholders, the Commission should address the problem of network disruption in at least the following three ways:

- Before network disruptions occur, it should put in place ways in which impending network disruptions are prevented. As part of its core human rights monitoring role, the Commission should pay closer attention to events that often trigger network disruptions such as political violence, and take steps towards averting network disruptions;
- After network disruptions start taking place, it should seek legal justification from the relevant government department. As a government human rights body, its engagements with the government are more likely to receive favourable response from the government; and
- The Commission should collaborate with other stakeholders such as civil society groups in challenging before courts arbitrary network disruptions.

The Role of Civil Society Groups

Civil society groups hold a unique position in influencing or shaping public policy, including government-sanctioned network disruption measures. However, civil society groups in Ethiopia with specific missions in this arena are few and far between. Much of the advocacy work against network disruption in Ethiopia has been undertaken by regional and international organizations.[102] In part, this is because of the restrictive civil society law that has been in place until recently. With the enactment in 2019 of a new civil society legislation that widens the possibilities of forming and operating human rights advocacy groups,[103] civil society groups working in the field of digital rights are emerging. But both such domain-specific human rights groups and those with broader mandates — as the interviews with key respondents from local civil society groups revealed — are yet to take steps in preventing and responding to network disruptions.

One factor for this has been the lack of clarity as to what, and when that they could take pertinent measures. NDRE, a network of human rights, media, and digital rights advocacy civic groups and individuals, is one of the few groups seeking to take up the challenge of digital rights advocacy. But the interview with the Chair of the NDRE revealed that it is yet to be formally registered as a civil society organization, and has taken limited steps in addressing

[102] See, e.g., Paradigm Initiative (n 31); Good News, Bad News: A Story of Internet Shutdowns in Togo and Ethiopia (CIPESA, 2020) <https://bit.ly/3aUFzQe>.
[103] See Organizations of Civil Societies Proclamation No 1113/2019, *Federal Negarit Gazeta*.

network disruptions. Among the initial steps it took include the preparation and submission to the government of a position paper on network disruptions and running digital literacy programs.[104] This suggests that a lot more is expected from local civil society organizations.

Local civil society groups should take at least the following three major steps in addressing the problem of network disruptions:

- Civil society groups may pursue two key measures before disruptions occur. One is raising awareness of various stakeholders, particularly relevant government departments, on the impact as well as the ineffectiveness of network disruptions; particularly highlighting its economic impacts. The second feasible pre-disruption measure is for civil society groups to put in place an 'early warning system' by which impending network disruptions may be predicted based on ongoing political events.[105] Of course, in building and then operating such a system, collaborating with other stakeholders, especially with organizations working in the field of peace and security nationally and regionally, would be quite useful. Such organizations would often have conflict surveillance systems or knowledge-base that help inform the early warning system. The early warning system would ideally allow relevant stakeholders to prepare in advance for an impending or planned disruption and take all the relevant measures, including court injunctions.

- Providing digital security/literacy training that equip individuals with skills of circumventing network disruptions is the second possible strategy.[106] Such training would help primarily in circumventing small-scale disruptions like targeted blocking of websites and apps, not total Internet shutdowns. The only two ways in which complete network blackouts may be circumvented are through the use of international SIM cards on roaming and use of satellite links. Both options are very expensive options and hence not scalable. The provision of training is not also always scalable to a wider audience. Therefore, the best way forward is to raise public awareness about digital security tools through different platforms. In an interview, a representative from CARD — a recently established civil society organization working in digital rights — stated that raising awareness, including running digital literacy programs has been one of its digital rights work.[107] Part of the program, according to the interviewee, is a 'keep it safe' campaign by which they lobby the government to refrain from disrupting communication networks.[108] Building on such initiatives, local civil society groups should join forces with international organizations such as Access Now to launch sustainable and tailored digital literacy programs.

[104] Interview with Ameha Mekonnen, Chair of the Network for Digital Rights in Ethiopia and Executive Director of Lawyers for Human Rights, held on 7 April 2021.
[105] Of a related point, see GNI (n 30) 25-26.
[106] *Ibid*, 27-28.
[107] Interview with Atnafu Berhane, Program Director at Center for the Advancement of Rights and Democracy, held on 8 April 2021.
[108] *Ibid*.

- Challenging arbitrary network shutdowns before courts is another avenue for civil society groups to take. There is currently no firm and clear legal basis for network disruptions making litigation all the more vital. Of course, the existence of a firm legal basis *per se* is not a guarantee against arbitrary practices. It all hinges on a number of factors, including the independence of the judiciary and the will to legally challenge arbitrary measures. Part of the reason why the government never bothered to properly justify its frequent shutdown measures is because there was little internal legal challenge. Apart from vocal reports of global rights organizations, no meaningful pressure came from local stakeholders, including civil society groups. With the government-owned Ethio-telecom as the only Internet access provider, it was tempting to shut the Internet without the pain of seeking a court order. In this respect, recent measures towards the liberalization of the telecom sector will factor in positively. As new private telecom operators with extensive global experience enter the market, days of warrantless Internet shutdown may come to an end. This will, of course, hinge on the extent to which stakeholders such as civil society groups pursue legal action before courts. Civil society-led legal actions are bearing fruit elsewhere in Africa. More recent examples are decisions of the Economic Community of West African States' (ECOWAS) Community Court of Justice which found Togo's 2017 Internet shutdown unlawful and Zimbabwe's High Court, which set aside shutdown orders of a government ministry.[109] With now civil society groups working on 'digital rights' in the offing, it is high time to challenge Internet shutdowns before Ethiopian courts. In an interview, a participant from Lawyers for Human Rights: Ethiopia (LHR) — a human rights civil society organization — revealed that LHR plans to launch strategic litigation against network disruptions.[110] This would be an encouraging step, more so when one considers the fact that one of the plaintiffs in the successful litigation before the High Court of Zimbabwe was LHR: Zimbabwe.[111]

The Role of the Private Sector

Ethiopia's tech sector is at a nascent stage. Partly because of the nation's poor ICT infrastructure – and lack of an enabling environment, it is only recently that the nation's tech sector is picking up. The past few years have seen the establishment of dozens of tech start-ups and incubation centers. It is also only recently that the process of transitioning from state monopoly to a liberalized (and privatized) communication sector has begun. This means two things. One is that the impact of network disruptions has not been as debilitating as it could have been to the tech sector. But with more digitization and ongoing reforms to create an enabling environment for a vibrant digital economy, network disruption's impact is bound to be significant. Second, until the telecom sector becomes liberalized and privatized, concerns for and measures against arbitrary network disruptions from the sole telecom operator are almost unthinkable.

[109] See *Amnesty International Togo et al v Republic of Togo*, ECOWAS Community Court of Justice, ECW/CCJ/JUD/09/20 (25 June 2020); High Court Sets Aside Internet Shutdown Directives (MISA Zimbabwe, 21 January 2019) <https://bit.ly/3t4LnNh>.

[110] Interview with Ameha Mekonnen, Chair of the Network for Digital Rights in Ethiopia and Executive Director of Lawyers for Human Rights, held on 7 April 2021.

[111] See High Court Sets Aside Internet Shutdown Directives (MISA Zimbabwe, 21 January 2019) <https://bit.ly/3t4LnNh>.

With a private telecom operator now awarded a license, the era of arbitrary and frequent shutdowns may come to an end. Prospects Ethio-telecom's partial privatization by which 40% and 5% of its share will be sold to private telcos and the public respectively may also make hitherto practices of arbitrary shutdowns slightly difficult.[112] But what specific steps should the private sector, including prospective telecom operators, take to deal with the network disruption problem? What follows attempts to address this question. A caveat is, however, in order. Because the privatization of Ethio-telecom would bring in private telcos, the role of telecom operators detailed in this section will also apply to new telecom operators that may enter the market through privatization as well as the liberalization process.

Telecom Operators

Telecom operators should respond to requests for network disruption in at least four ways:

- Telecom Operators can bring more light to the process by disclosing to the public the nature, scope and content of orders submitted by the government. This would allow other stakeholders to know which department of the government is behind the (impending) disruption, and what legal basis is invoked to justify the request. Civil society groups would then be able to weigh options of responding to the request, including through litigation.

- Telecom operators may decline the request for a lack of clear legal basis for the disruption. In Africa, while most telecom operators outright obey shutdown orders – obviously due to their business interests and stringent license conditions, MTN Benin, Orange Guinea and Lesotho's Econeth have successfully pushed back against government requests for network disruptions.[113] A useful lesson from international best practices is that telecom operators resist disruption orders that lack clear legal basis and seek legal justifications.[114] Often, governments rely on vague provisions of national security law or license conditions to have networks disrupted. But companies should always seek explicit legal basis that warrant taking far-reaching measures like total network blackout or blocking of a popular website.

- The more diplomatic response is for telecom operators to dissuade the government from resorting to network disruptions as means of addressing a perceived national security threat.[115]

- Telecom companies should form alliances with civil society groups to collaboratively address network disruptions.[116]

[112] See Ministry to Avail 5pc of Ethio Telecom to Public (Fortune, 23 May 2020) <https://bit.ly/3hXcnN8>.
[113] See CIPESA Policy Brief (n 74) 3.
[114] See GNI (n 11) 10.
[115] *Ibid*.
[116] See Five Ways Telecommunications Companies Can Fight Internet Shutdowns (Lawfare, 23 August 2020) <https://bit.ly/3e5LVP1>.

- One of the grounds for revoking telecom licenses, as alluded to above, is failure to comply with conditions attached to telecom licenses. But the ECA is required to provide a 15 days notice to licensees within which they may present arguments against the revocation decision.[117] Moreover, ECA is required to take into consideration arguments of the licensee before reaching a final decision. This procedure provides an opportunity for a telecom operator that, for instance failed to comply with shutdown orders, to persuade why it has to decline the order.

- Another avenue is appealing to the Tribunal envisaged in the Draft Dispute Resolution Directive. The Tribunal is, of course, designed to hear appeals against decisions of ECA over disputes that arise between licensees, between licensees and consumers and other third parties such as advertisers.[118] But a closer reading of the Communications Service Proclamation suggests that all decisions of the ECA, probably including orders to disrupt telecom networks, may be appealed to the (future) Tribunal.[119] This means that part of telecom operators' effort of resisting arbitrary network shutdowns could be approaching the Tribunal.

- Seeking a public hearing is the other way in which telecom operators may seek to bring the problem of network disruptions to the spotlight. Per the Communications Service Proclamation, any 'interested parties' may by a written letter request the Authority to initiate a public hearing on any 'substantive matter within its jurisdiction'.[120] Such a public consultation may culminate later in the taking of binding decisions, including adoption of a subordinate legislation or submission of legislative proposals to the Parliament.[121] Following this path, telecom operators may push against requests for network disruptions that lack legal basis. This may have the effect of pressuring the government to introduce some legal basis for network disruptions.

Technology Companies[122]

Ethiopia's tech sector is at a nascent stage, and has been largely fragmented which has —thus far —limited its role in collectively voicing concerns about arbitrary network disruption. Established in 2010, the Information and Communication Technology Association of Ethiopia (ICT-ET) is a sectoral association whose membership includes national private technology companies operating in the information, communication and broadcasting technology sectors.[123] One of its foundational objectives is 'representing the interests of ICT companies in national dialogues'.[124] As highlighted above, one of the impacts of network disruptions is on the nation's budding ICT sector. In the past decade, a number of local technology

[117] See Telecommunications Licensing Directive (n 80) Art 34(3).
[118] See Telecommunications Dispute Resolution Directive No796/2021 (ECA, 2020) Arts 3 cum 20.
[119] See Proclamation No 1148/2019 (n 76) Art 40(1).
[120] *Ibid*, Art 34(1).
[121] *Ibid*, Art 35(4-5).
[122] For purposes of this *Legal Guide*, the reference 'technology companies' is meant to capture private companies in the technology sector other than telecom operators.
[123] See details at the Association's website here: <https://ictet.org/about/>.
[124] *Ibid*; see also Interview with Seyoum Beredid, President of Information and Communication Technology Association of Ethiopia, held on 16 April 2021.

companies, taxi hailing companies and start-ups have emerged in Ethiopia. But the recurrence of network disruptions has undermined the growth of the sector. As a sectoral association, ICT-ET should take steps towards preventing and responding to network disruptions. Among other things, it may for instance document the extent of impact on its member companies, propose a joint response, engage with relevant authorities and forge collaboration with civil society groups in addressing the problem of network disruptions.

Concluding Observations

Episodes of network disruption have become commonplace in Ethiopia since 2016.[125] While guarding national security has been a recurring rationale, other factors such as preventing exam leaks and cheating have been presented to justify network disruptions. The precise extent to which network disruptions impacted the enjoyment of human rights and the economy generally, and vulnerable groups in particular, is little known. But the incidence of network disruptions is bound to increase in the months and years ahead. So would their impact. With a highly polarized and bitter political climate shaped up and mediated by social media discourse, the usual trigger factors for network disruptions are pervasively present.

In spite of this state of affairs, no meaningful steps are being taken by relevant stakeholders to address the persistent problem of network disruption. Because there has never been any concrete push back from these stakeholders, especially civil society groups, the government hardly bothered to ground its disruption measures on a sound legal basis. Some commentators suggest that the recurrence of network disruptions in Africa is attributable to the failure of social media platforms in attending to the content moderation needs of the continent.[126] But this does not quite explain the case in Ethiopia where the government rarely sought such measures from technology companies. In jurisdictions where network disruption is considered a tenable regulatory tool such as India, laws are enacted not only to put the measure in a relatively firm legal basis but also to prevent arbitrariness. In the face of little resistance from civil society and private actors – and aided by state monopoly of the communications sector, the government disrupts communication networks often and at times for a long period of time.

But recent years have seen the formation of 'digital rights' civil society organizations with the potential to play a role in predicting, preventing and responding to network disruptions. As the interviews with some of these organizations revealed, there is an interest to challenge and respond to network disruptions. The prospect of telecom liberalization means the ease with which the government effects network disruptions through its state enterprise, Ethio-telecom, may be no more. And these two developments would be instrumental in bringing an end to the days of recurrent, arbitrary and unlawful network disruptions. Nevertheless, this potential local effort in addressing the problem of network disruptions cannot be marshalled without pertinent guidance on the legal aspects of network disruptions in

[125] While this *Legal Guide* was being finalized, Facebook, WhatsApp and Instagram were blocked for several hours on 17 May 2021 for which no explanation has been provided by the government. See Ethiopia Blocks Access to Social Media Platforms, Netblocks Says (Bloomberg, 17 May 2021) <https://bloom.bg/3fdNJpu>.
[126] See GNI (n 30) 16; CIPESA Policy Brief (n 74) 4.

Ethiopia. Currently there is no such guidance with which stakeholders may take steps against network disruptions.

This *Legal Guide* is a modest attempt to fill this void which it sought to fill in two respects. First, it explored the current legal landscape on network disruptions. In so doing, the aim is to put to the test whether the government's recent casual justification to network disruptions holds water. As shown in this *Legal Guide*, this legal position of the government does not stand up to closer scrutiny. Going further, the *Legal Guide* has shown how the current cybercrime proclamation probably offers a defensible legal basis for network disruptions while at the same time providing safeguards against arbitrariness. Relevant stakeholders such as civil society groups and telecom operators may rely on this legal analysis to prevent and respond to aribitrary network disruptions through legal means. Second, it considered the respective role of relevant government institutions, civil society groups and the private sector. As the research for this *Legal Guide* illustrated, there is a lack of clarity as to who is best-placed to do what in responding to network disruptions. Informed by considerations such as their statutory responsibilities and organizational mission, this *Legal Guide* has outlined the role of government institutions, civil society organizations and the private sector.

This *Legal Guide* closes with a series of recommendations to the government, civil society groups and the private sector.

To the Government

- The government should introduce legislation that mandates network disruption along with a robust oversight mechanism. Network shutdown standards misplaced in the cybercrime Bill – with proper amendments – should be enacted, preferably in a subsidiary legislation. Useful lessons in this regard may be drawn from India's Temporary Suspension of the Telcom Services (Public Emergency and Public Safety) Rules of 2017. While India's Supreme Court has raised reservations about this legislation – and recommended the government to amend it,[127] it doubtless offers one form in which a freestanding network disruption legislation may be fashioned;

- The role of INSA in ordering or effecting network disruption should be clarified. As shown in the *Legal Guide*, the Agency appears to have invisible technical capabilities of disrupting communication networks without the involvement of Ethio-telecom. With the entry of new telecom operators, when and how – or whether – INSA should be able to unilaterally 'kill the switch' in a lawful and orderly manner should clearly be spelled out by law;

- The government should properly recognize the cross-cutting impacts and counter-productive nature of recurrent network disruptions, and explore alternative ways of addressing the trigger factors, including through inclusive political processes;

[127] See SC's Kashmir Communication Shutdown Judgement is Just the Beginning of a Long Uphill Campaign (Internet Freedom Foundation, 10 January 2020) <https://bit.ly/3ysOhiS>.

- Government entities whose organizational missions are being undermined by network disruptions should engage in an 'internal' mission of persuading or dissuading the government from repeated, arbitrary and prolonged network disruptions.

To civil society groups

- Emerging as well as longstanding civil society groups working on human rights, and vulnerable groups should properly recognize the problem of network disruption. This should be followed by a concrete strategy where a bundle of measures to be taken before, during and after network disruptions occur;

- Civil society-led measures should be multi-pronged, combining awareness raising programs, collaborative advocacy and strategic litigation.

To the private sector

- The private sector, especially technology companies, should collectively voice their concerns on the impact of network disruptions. ICT-ET which represents major tech companies in Ethiopia should take the lead in this regard. Part of this effort should be to engage with relevant government departments;

- The private sector should collaborate with and support the efforts of civil society groups towards predicting, preventing and responding to network disruptions. The support could take various forms, be it technical or financial.

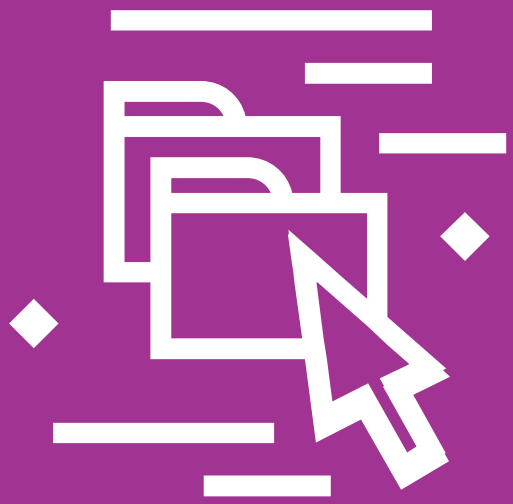
References

1. A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa (CIPESA, 2017).
2. Amnesty International Togo *et al* v Republic of Togo, ECOWAS Community Court of Justice, ECW/CCJ/JUD/09/20 (25 June 2020).
3. Building Capacity for Internet Shutdown Advocacy: A Community Needs Assessment Report (Internews, November 2020).
4. Comments by the State on the Report of the Special Rapporteur on the Promotion and Protection of the Freedom of Opinion and Expression on His visit to Ethiopia, UN Doc A/HRC/44/49/Add.3 (15 April 2020).
5. Communications Service Proclamation No 1148/2019, *Federal Negarit Gazeta*.
6. Computer Crime Proclamation No 958/2016, *Federal Negarit Gazeta*.
7. Constitution of the International Telecommunication Union (1992, as amended).
8. Digital Ethiopia 2025: A Digital Strategy for Ethiopia's Inclusive Prosperity (2020).
9. Digital Rights in Africa 2019 (Paradigm Initiative, 2019).
10. Disconnected: A Human Rights-based Approach to Network Disruptions (GNI, 2020).
11. Draft Computer Crime Proclamation (2020).
12. Draft Dispute Resolution Directive No 4 (ECA, 2020).
13. Draft Telecommunications License Directive No 1 (ECA, 2020).
14. Ethiopian Constitution, Proclamation No 1/1995, *Federal Negarit Gazeta*.
15. E-transaction Proclamation No 1205/2020, *Federal Negarit Gazeta*.
16. Freedom on the Net: Ethiopia (2016, Freedom House).
17. Hate Speech and Disinformation Prevention and Suppression Proclamation No 1185/2020, *Federal Negarit Gazeta*.
18. Information Network Security Agency Re-establishment Proclamation No 808/2013, *Federal Negarit Gazeta*.
19. Information Network Security Agency Re-establishment Proclamation Execution Council of Ministers Regulation No 320/2014, *Federal Negarit Gazeta*.
20. International Telecommunication Regulations (2012).
21. Kenneth Himma, Ethical Issues Involving Computer Security: Hacking, Hacktivism and Counter-Hacking, in Kenneth Himma and Herman Tavani (eds), *The Handbook of Information and Computer Ethics* (Wiley, 2008).
22. Life Interrupted: Countering the Social Impacts of Network Disruptions in Advocacy in Africa (GNI, 2021).
23. Media Sustainability Index: Ethiopia (2010, IREX).
24. National Information and Communication Technology Policy and Strategy of Ethiopia (2016).
25. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Visit to Ethiopia, UN Doc A/HRC/44/49/Add.1 (29April 2020).
26. State of Emergency for the Protection of the Constitution and Constitutional Order Proclamation No 4/2020, *Federal Negarit Gazeta*.
27. State of Emergency Proclamation Issued to Defend the Constitution and Constitutional Order from Threat Council of Ministers Proclamation No 2/2018, *Federal Negarit Gazeta*.
28. State of Emergency Proclamation Issued to Defend the Constitution and Constitutional Order from Threat Council of Ministers Proclamation No 1/2016, *Federal Negarit Gazeta*.
29. Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017.
30. Ten-Year Development Plan of Ethiopia: 2020/21 – 2030/31 (Planning and Development Commission, 2020).
31. The Economic Impact of Disruptions to Internet Connectivity (Deloitte, 2016).

32. U.S. Department of State Country Report on Human Rights Practices 2005: Ethiopia (8 March 2006).

About Kinfe Michael Yilma (PhD)

Kinfe Yilma is an assistant professor of law at Addis Ababa University School of Law in Ethiopia. His research interests are in the fields of Internet law, human rights law, and digital constitutionalism. Kinfe holds a PhD in Information Technology Law from the University of Melbourne (Austraila), LLM in International Human Rights Law from Brunel University London (UK), LLM in Information Technology Law from the University of Oslo (Norway), and LLB from Addis Ababa University (Ethiopia). He has rendered consultancy services to a number of international organizations including the Intergovernmental Authority on Development, Internet Society, the Association for Progressive Communication, the African Digital Rights and Freedoms Coalition, and the African Union Commission as well as the governments of Ethiopia and Lesotho. Before returning to his post at Addis Ababa University, Kinfe has taught at Melbourne Law School in Australia.



Contextualizing Your Data

This is a sample paragraph text that can be edited. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt.

This is a sample paragraph text that can be edited. Lorem ipsum dolor sit