



NAVIGATING  
LITIGATION DURING  
**INTERNET**  
**SHUTDOWNS IN**  
**SOUTHERN AFRICA**

2019  
June

## **REPORT: Navigating Litigation during Internet Shutdowns in Southern Africa**

© 2019 Southern Africa Litigation Centre, Media Institute of Southern Africa

ISBN: 978-0-6399321-8-7

ISBN: 978-0-6399321-9-4

Cover Photograph: Shutterstock

### **About the Southern Africa Litigation Centre (SALC)**

The Southern Africa Litigation Centre (SALC), established in 2005, envisions a Southern Africa in which human rights are respected, protected, promoted and fulfilled. SALC's mission is to promote and advance human rights, democratic governance, rule of law and access to justice in Southern Africa through strategic litigation, advocacy and capacity strengthening. SALC works in Angola, Botswana, Democratic Republic of Congo, Eswatini, Lesotho, Malawi, Mozambique, Namibia, South Africa, Zambia and Zimbabwe.

### **About the Media Institute of Southern Africa (MISA)**

The Media Institute of Southern Africa (MISA) works to promote and advocate for the unhindered enjoyment of freedom of expression, access to information and a free, independent, diverse and pluralistic media. MISA consists of vibrant national chapters in Lesotho, Malawi, Tanzania, Zambia and Zimbabwe.

### **Authorship and Acknowledgement**

This guide was researched and written by Tyler Walton, from SALC, with additional input from Kuda Hove, from MISA Zimbabwe, Otto Saki, from Ford Foundation, Anneke Meerkotter, Isabeau Steytler, Mariano Fanatico and Emma Heo from SALC. It was edited by Anneke Meerkotter.

This guide was preceded by a workshop, co-hosted by SALC and MISA, on litigating during internet shutdowns in Southern Africa, which was held in April 2019 with financial and technical assistance from the Ford Foundation. Printing of this guide has kindly been funded by Free Press Unlimited.

### **Southern Africa Litigation Centre**

Second Floor, President Place, 1 Hood Avenue, Rosebank, Johannesburg,  
South Africa, 2196, [info@salc.org.za](mailto:info@salc.org.za), +27 (0) 10 596 8538,  
[www.southernafricalitigationcentre.org](http://www.southernafricalitigationcentre.org), @follow\_SALC

### **Media Institute of Southern Africa Zimbabwe**

84 McChlery Avenue, Eastlea, Harare, Zimbabwe, [admin@misazim.co.zw](mailto:admin@misazim.co.zw),  
+263 242 776 165, <http://zimbabwe.misa.org>, @misazimbabwe

### **Electronic copies of this report can be found at**

[www.southernafricalitigationcentre.org](http://www.southernafricalitigationcentre.org) and <http://zimbabwe.misa.org>

The background of the page features a light gray field with a pattern of binary code (0s and 1s) in a slightly darker shade. In the lower-left corner, there is a faint, stylized silhouette of a city skyline with several buildings of varying heights.

# NAVIGATING LITIGATION DURING **INTERNET SHUTDOWNS IN SOUTHERN AFRICA**

# Foreword

**A**cross Southern Africa, at critical moments and times, such as elections or public protests governments have directed internet service providers to restrict or shut down the internet. These directives have affected economies, and enabled political predation to occur under the cover of internet blackouts. Accountability and legal liability is eviscerated through a web of unclear directives framed under already controversial and non-specific laws. Public interest lawyers and organisations continue to be the last line of defence against state and non-state actors' excesses. Litigation compliments other policy and advocacy efforts to expose these excesses, illegalities, and the unreasonable directives shutting down internet which is near-endemic in Southern Africa. This manual demonstrates opportunities available, shares strategies for challenging internet shutdowns and contributes to the development of a cadre of lawyers, internet policy activists, and public interest law organisations willing to hold state and private sector powers accountable and ending impunity. Freedom of expression, as well as access to imparting, receiving, or disseminating information are vital for any society. Even the most shocking and offensive information should not be subjected to arbitrary, unjustified and unreasonable limitations.

Censorship of information through closure of media houses, arrests of journalists, and redaction of published materials, remains prevalent. These brute approaches are now complimented by indiscriminate telecommunication networks disruptions and shutdowns. Justification for such practices have not changed; the need to maintain law and order, averting threats against national security, public order, health and morality. These justifications are repeated without shame and little restraint, especially in countries with weak or constrained judiciaries. The private sector is not entirely without blame, business decisions and shareholder interests trump rights. Because of their proximate relationship to the state, most internet service providers are quick to implement these directives. Those with little or no government shareholder interests carefully navigate these relationships including denial of having received directives to shut down the internet, or in other very brazen instances challenging these directives. These complexities necessitate using the law to challenge internet shutdowns. The instrumentalization of the law in internet shutdowns requires commensurate responses. Countries, whether defined or viewed as democratic or authoritarian justify all their actions in terms of the law, and shutdowns are no exception. Most laws in Southern Africa do not have specific reference to internet shutdowns, but governments invoke even the slightest relevant provisions from general cyber and telecommunications legislation. This places a premium on efforts that equally uses national, regional and international human rights law to debunk these excesses. This manual contributes to global efforts to *keep the internet on*, and advance rights, social, political and economic progression of Southern African nations. It is a noble cause.

**Otto Saki**  
**Programme Officer**  
**Ford Foundation Regional Office**  
**Southern Africa**

# CONTENTS

1

<i>Foreword</i>	<i>iv</i>
<i>Digital Acronyms</i>	<i>3</i>

<b>1</b>	<i>Introduction</i>	<i>4</i>
----------	---------------------	----------

<b>2</b>	<i>Technical Explanation</i>	<i>6</i>
----------	------------------------------	----------

<b>3</b>	<i>Recent Shutdowns in Southern Africa</i>	<i>8</i>
	Malawi	8
	Zimbabwe	8
	Democratic Republic of Congo	9
	Lesotho	9

<b>4</b>	<i>Socio-economic Impact of Internet Shutdowns</i>	<i>11</i>
	Economy	11
	Journalism and the Media	12
	Education	12
	Health	12
	Personal Security	13

<b>5</b>	<i>International Human Rights Framework and the Internet</i>	<i>14</i>
	Regional Law on Internet Rights and Freedoms	16
	Limitations on Fundamental Human Rights	17
	Necessity and Legality	18
	Prior Restraint	21
	Human Rights and National Emergencies	22

<b>6</b>	<i>Domestic Laws</i>	<i>24</i>
	Protection of Digital Rights	25
	Independence of Regulatory Authorities	26
	Ambiguity of Powers of Regulatory Authorities	28
	Legislated Authorisations for Suspension of Communications	33
	Legality of Executive Directives	34
	Communication Laws and Declarations of Emergency	35
	Contract Law	36

# 7

## *Internet Shutdowns during Elections* 38

Offences during Election Time	40
Reporting Obligations of the Media	40
Legislative Protections of Freedom of Expression	41

# 8

## *Constitutional Considerations* 42

Freedom of Expression Case Studies Constitutional Limitations on Telecommunications Regulations	43
Constitutional Limitations on Telecommunications Regulations	47

# 9

## *Thinking Through Litigation Strategy* 50

# 10

## *Conclusion* 52

## *Annex I*

## *Global Case Studies on Freedom of Expression and Technology* 53

## *Annex II*

## *Major Internet Providers in Southern Africa* 60

ANGOLA	60
BOTSWANA	61
DEMOCRATIC REPUBLIC OF CONGO	62
ESWATINI	63
LESOTHO	64
MALAWI	65
MOZAMBIQUE	66
NAMIBIA	67
TANZANIA	68
ZAMBIA	69
ZIMBABWE	70



## digital ACRONYMS

**asp**

**Application Service Provider**

A company that offers individuals or enterprises access to applications and related services over the internet. The term has largely been replaced by software as a service (SaaS) provider.

**cdn**

**Content Delivery Network**

A system of distributed servers (network) that deliver pages and other Web content to a user, based on the geographic locations of the user, the origin of the webpage and the content delivery server.

**dns**

**Domain Name System**

A decentralised naming system for computers, services and other resources connected to the internet or a private network.

**dpi**

**Deep Packet Inspection**

A form of computer network packet filtering that examines the data part of a packet as it passes an inspection point.

**hipssa**

**Support for the Harmonisation of the ICT Policies in Sub-Saharan Africa**

A project supported by ITU which aims to create the policy, legal and regulatory frameworks conducive to investments in ICT infrastructure in this region.

**https**

**Hyper Text Transfer Protocol Secure**

Secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. It means communications between your browser and the website are encrypted.

**ict**

**Information and Communications Technology**

Broader than information technology (IT). Stresses the integration of telecommunications (telephone lines and wireless signals) and computers, software, storage etc.

**igf**

**Internet Governance Forum**

A multi-stakeholder forum for policy dialogue on issues of Internet governance.

**ip**

**Internet Protocol**

IP address is an identifier to each computer or other device connected to the internet, to locate and identify the node in communications with other nodes on the network.

**isp**

**Internet Service Provider**

An organisation that provides services for accessing, using, or participating in the Internet.

**itu**

**International Telecommunications Union**

A specialised agency of the United Nations that is responsible for issues that concern information and communication technologies.

**ixp**

**Internet Exchange Point**

The physical infrastructure through which ISPs and CDNs exchange Internet traffic between their networks (autonomous systems).

**mno**

**Mobile Network Operator**

A wireless service provider, wireless carrier, cellular company, or mobile network carrier - a provider of wireless communications services that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure.

**ooni**

**Open Observatory of Network Interference**

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

**ssl**

**Secure Sockets Layer**

Cryptographic protocols that provide communications security over a computer network. Its predecessor is Transport Layer Security (TLS).

**tcp**

**Transmission Control Protocol**

A set of communication protocols used to interconnect network devices on the Internet.

**tor**

**The Onion Router**

A free, open-source software for anonymous communication by directing internet traffic through a free, worldwide, volunteer overlay network consisting of thousands of relays to conceal a user's location and usage from anyone conducting network surveillance.

**url**

**Uniform Resource Locator**

Web address - web resource that specifies its location on a computer network and a mechanism for retrieving it.

**vpn**

**Virtual Private Network**

Extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

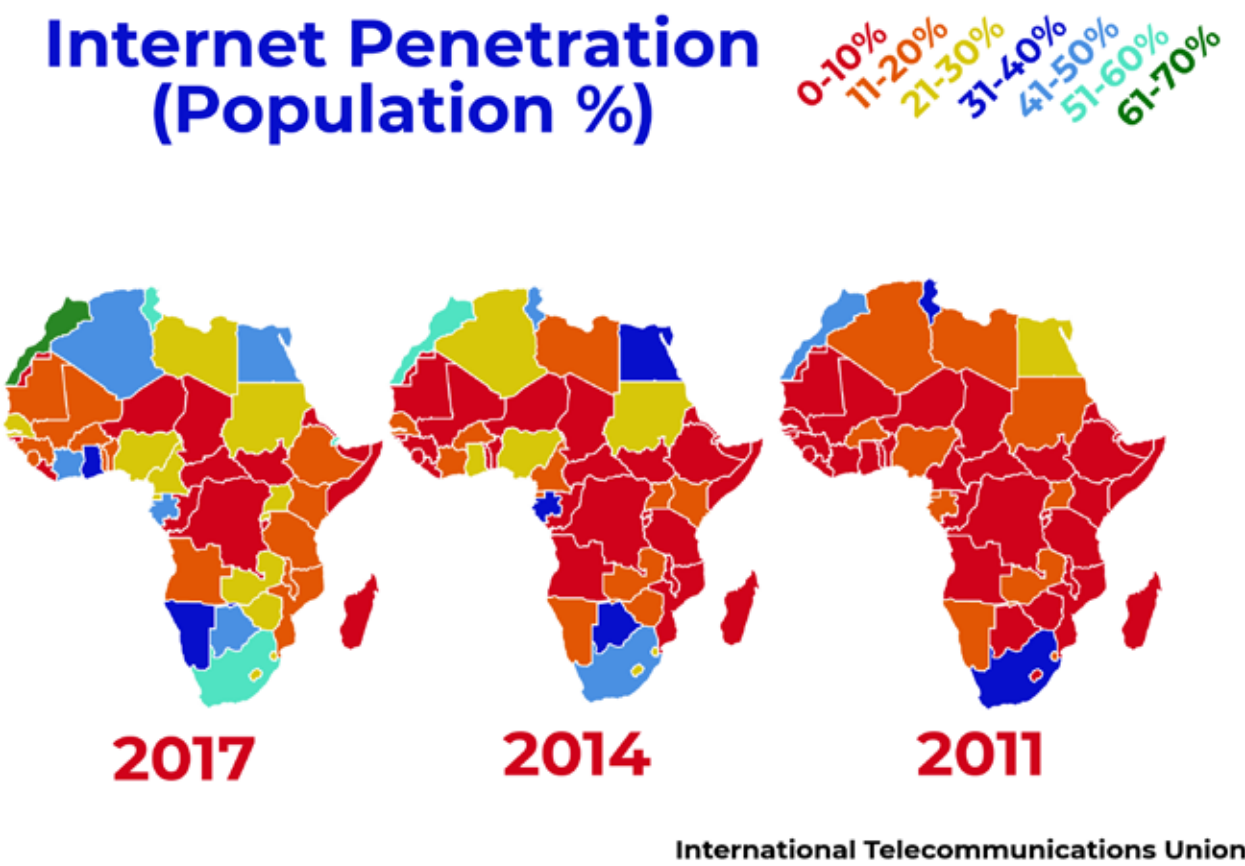
**www**

**World Wide Web**

The Web - an information space where documents and other web resources are identified by URLs and are accessible over the Internet and accessed through a software application called a web browser.

# 1.Introduction

As of 2018, ITU estimated that 51.2% of the global population was using the internet.<sup>1</sup> Much of the recent growth is occurring in Africa, which saw a 20% bump in internet users over the course of 2017. There are now half a billion users across the continent, with some of the highest percentage of connectivity occurring in Southern Africa. As people have become more connected, it has changed how citizens participate in civic life, as well as how governments respond to their citizens.



<sup>1</sup> "Statistics" ITU (2019) <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>



One of the troubling government responses to digital life has been internet shutdowns. Access Now is one international human rights organisation that focuses on human rights in the digital age who has been tracking internet shutdowns for a decade. They define internet shutdowns as:

**“An internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.”<sup>2</sup>**

Internet shutdowns violate human rights and can lead to many negative socio-economic impacts. In response to the growing number of internet shutdowns around the world and in the Southern Africa region, civil society has started advocating against internet and other communications disruptions. One important avenue that can be used to respond to internet shutdowns is litigation. Litigation is a way to challenge the laws used to justify internet shutdowns, and to achieve redress for economic damage caused and human rights violated. This report explains the legal considerations relevant for challenging internet shutdowns in courts in Southern Africa.

---

<sup>2</sup> “#KeepItOn Campaign” Access Now (2018) <https://www.accessnow.org/keepiton/>

## 2. Technical Explanation

For many total or partial internet shutdowns, government officials or security forces, such as military or police, tell internet service providers (ISPs) to shut down services. While sometimes, these orders are backed by a warrant or official written order, such as in the case of the recent Zimbabwe shutdown, there are also reports of verbal orders given without written justification.<sup>3</sup>

Sometimes shutdowns target specific websites or applications, such as Twitter, WhatsApp or Facebook. When shutdowns are only blocking certain sites, there are technical workarounds that can provide internet users with a way to still access sites. The most common method is through virtual private networks (VPNs). VPNs allow users to connect IP addresses that are hosted outside of the country of origin, and thus provide an avenue around national blockages to service. ISPs are also able to block access to VPN providers, so sometimes certain VPNs will also not be accessible during a partial internet shutdown.

VPNs also allow access when Internet access is throttled. Throttling is another way that is used to limit access to the Internet. This method involves the intentional reduction of Internet access speeds to a point where websites and Internet dependent applications are inaccessible or effectively unusable.

Other times, ISPs will completely shut off access to the internet. This involves a total blockage which cannot be circumvented through a VPN. Governments sometimes try to avoid complete shutdowns because they impact internet-based banking which has a higher economic impact and is more disruptive than partial blockages.

When civil society is considering a legal challenge to an internet shutdown, careful consideration should be given to which parties to join as defendants to the claim. In addition to the relevant government authorities, the ISPs implementing the order should also be included in the suit.

Often, governments give no public indication that they are behind an internet shutdown. In these cases, strategic selection of private companies, such as ISPs, for the defendants in a case can allow litigants to extract information from the private companies. This can be a way to get evidence that the government did in fact order the shutdown, especially if an ISP needs a defence for interrupting its services to paying customers.

An annex outlining the major ISPs in each country in Southern Africa can be found at the end of this report.

---

<sup>3</sup> "#NAMAPolicy: How do Internet shutdowns happen, and do they work?" MediaNama (21 December 2017) available at <https://www.medianama.com/2017/12/223-namapolicy-internet-shutdowns-happen-work/>

# Methods used to block internet content

SOURCE: INTERNET SOCIETY, PERSPECTIVES ON INTERNET CONTENT-BLOCKING: AN OVERVIEW

## IP and Protocol-based Blocking

How?

BLOCKS CONTENT

A DEVICE IS INSERTED IN THE NETWORK THAT BLOCKS BASED ON IP ADDRESS AND/OR APPLICATION (E.G. VPN)

What helps?

- CHANGE IP ADDRESS
- MIGRATE CONTENT
- USE CONTENT DELIVERY NETWORKS (CDN)
- HIDE IP ADDRESS BY USING VPN



The connection has timed out



## URL-based Blocking

How?

BLOCKS CONTENT

A DEVICE IS INSERTED IN THE NETWORK THAT INTERCEPTS WEB REQUESTS AND LOOKS UP URLS AGAINST A BLOCK LIST

This site has been blocked by the network administrator



- MULTIPLE LAYERS OF ENCRYPTION
- USE NON-STANDARD APPLICATION LAYER

What helps?

## Deep Packet Inspection-based Blocking

How?

BLOCKS CONTENT

A DEVICE IS INSERTED IN THE NETWORK THAT BLOCKS BASED ON KEY WORDS OR OTHER CONTENT



The connection was reset

What helps?

- MULTIPLE LAYERS OF ENCRYPTION
- SMALL CHANGES IN TEXT TO BYPASS BLOCKS



## Platform-based Blocking

ESPECIALLY SEARCH ENGINES

How?

WORKING WITH APPLICATION PROVIDERS (SUCH AS SEARCH ENGINES), CONTENT IS MODIFIED ACCORDING TO LOCAL REQUIREMENTS

No results found



What helps?

- USE ALTERNATIVE PLATFORM, SUCH AS DIFFERENT SEARCH ENGINE



## DNS-based Blocking

DISCOURAGES ACCESS

How?

AT NETWORK OR ISP LEVEL, DNS TRAFFIC IS FUNNELED TO A MODIFIED DNS SERVER THAT CAN BLOCK LOOKUPS OF CERTAIN DOMAIN NAMES

Server not found



What helps?

- SEND QUERIES THROUGH UNMODIFIED PUBLIC SERVER (VPN)

## 3. Recent Shutdowns in Southern Africa

### 3.1 Malawi

Leading up to the election on 21 May 2019, there were rumours swirling that the government of Malawi was considering shutting down the internet on the day of the election. Several meetings between the government, the Malawi Communications Regulatory Authority (MACRA), and civil society occurred during the weekend before the election. Lawyers from MACRA resisted efforts by the government to shut down the internet, and stated that while they believed Malawian law gave them the authority to shut off internet access, they did not think that it was necessary. There were also reports that the government was directly pressuring individual ISPs within the country to shut off access.

On the day of elections, there were reports that several of the major internet arteries between Blantyre and Lilongwe were cut. NetBlocks reported a 20% decrease in internet activity in the three hours following the closure of the polls.<sup>4</sup> The government stated both that there was no internet shutdown, and that vandals had cut lines that caused some services to be down temporarily.

### 3.2 Zimbabwe

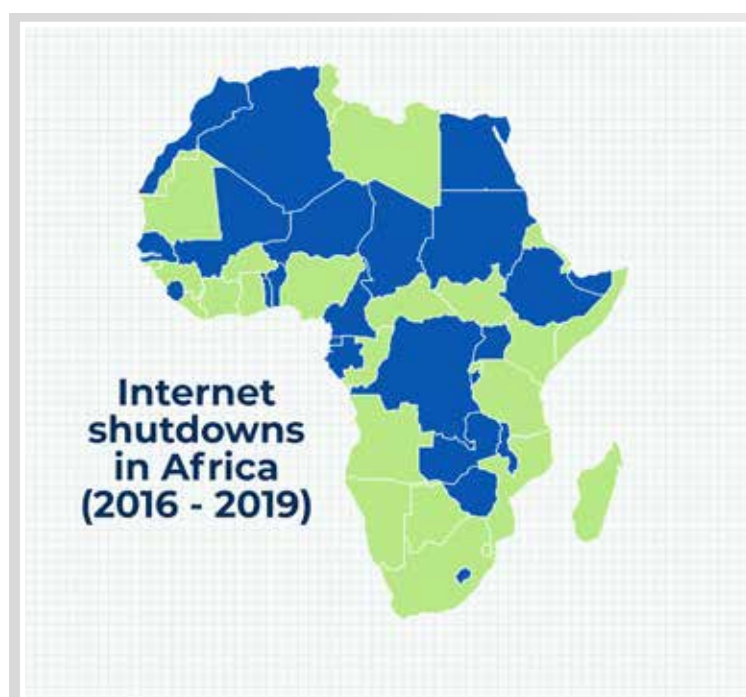
Beginning around 9 am local time on 16 January 2019, Zimbabwe internet users began being unable to access the internet, including social media apps like Facebook, Twitter, and WhatsApp. At first, Zimbabweans were able to use VPNs to get around the blockage, but by noon Wednesday, the majority of the country was experiencing a complete internet blackout.

The Internet shutdown was ordered by a warrant issued pursuant to the Interception of Communications Act, a 2007 law which provides the government with the right to lawfully intercept or monitor postal and telecommunications to fight crime and protect national security. The definition of interception in the Act states that it “means to listen to, record, or copy” a communication; nowhere in the Act is blocking or disrupting communication services even mentioned.

The Zimbabwean government has previously disrupted Internet-based communications without relying or referring to the Interception of Communications Act. On the morning of 6 July 2016, Zimbabwe experienced a partial shutdown targeting social media websites and applications such as Facebook, WhatsApp and Twitter. The partial shutdown lasted an estimated four hours. During that time, Zimbabwean users could access the restricted services and applications by means of VPNs.

---

<sup>4</sup> “Internet Disrupted in Malawi on Election Day” NetBlocks (2019) available at: <https://netblocks.org/reports/internet-disrupted-in-malawi-on-election-day-Q8oOrl8n>



### 3.3 Democratic Republic of Congo

The Democratic Republic of Congo has experienced many internet shutdowns over the past several years. These have ranged from complete country wide shutdowns to targeted regional shutdowns of social media platforms. The Telecommunication Law in the DRC contains sections which specifically mandate that license holders may be ordered to shut off access to their networks due to concerns of national security or public order.<sup>5</sup> The internet shutdowns are often accompanied by outages of SMS services, cuts to radio and television signals for independent broadcasters, and the implementation of roadblocks in population centres such as Kinshasa.

The first reported internet shutdown occurred in January 2015. This followed an earlier 25 day cut to SMS services in December of 2011. Again, on 19 December 2016, the government ordered the internet to be shut down on the day Joseph Kabila was set to step down as head of State. On 30 December 2017, the Democratic Republic of Congo's Telecommunications Minister, Emery Okundji, ordered the country's telecommunications providers to shutdown internet and SMS services across the country. There was another three-day internet blockage beginning 21 January 2018. Then on 25 February 2018 there was a ten-hour blockage. From 31 December 2018 to 6 January 2019, during the election count, internet users in the Democratic Republic of Congo were again shut off from the internet.

### 3.4 Lesotho

In July 2016, leading up to the 2017 election in Lesotho, the government of Lesotho proposed a social media shutdown over concerns that State secrets were being published. The regulatory body, the Lesotho Communications Authority (LCA), refused the proposal and demanded that the government give a lawful written order if they wanted to shut off access to social media. Later that year, in November 2016, the government again pursued a social media shutdown and asked LCA to send a letter to the two main mobile/internet providers to

<sup>5</sup> Loi sur les télécommunications en République démocratique du Congo, Act No. 13 of 2002, Article 46.



“provide information on whether a temporary restriction of access to Facebook and Twitter usage was possible”.<sup>6</sup> The government sent the letter the service providers, who subsequently leaked it to the public. LCA then held a meeting with officials from Facebook. The elections eventually happened on 3 June 2017, and there was no confirmed evidence of an internet shutdown. Because of a mixture of pressure from an independent regulator, civil society, and business interests, a likely internet shutdown was avoided.



<sup>6</sup> Arthur Gwagwa “When Governments Defriend Social Media” Centre for Intellectual Property and Information Technology Law (2017) p. 5.

## 4. Socio-economic Impact of Internet Shutdowns

When governments shut off access to the internet, it can lead to a plethora of negative socio-economic consequences. As was stated in a recent report by the Special Rapporteur on the rights to freedom of peaceful assembly and of association:

**“network shutdowns...generate a wide variety of harms to human rights, economic activity, public safety and emergency services that outweigh the purported benefits.”<sup>7</sup>**

When approaching litigation, considering the economic and societal costs are important, and can be used in addition to claims of human rights violations to bolster cases. These questions are also important in considering who the named applicants in a challenge to an internet shutdown should be. Covering a wide swath of experiences based on those who are impacted by the internet shutdown can be an important way to demonstrate to the court the high societal cost of upholding internet shutdowns. Many of the arguments against internet shutdowns will ultimately depend on a proportionality test. Is the limitation on rights justified by the harm attempting to be averted? Demonstrating more socio-economic costs will push the balance in favour of the shutdown not being proportional. Below are some examples of substantive areas which may be impacted by internet shutdowns.

### 4.1 Economy

A recent Brookings Institute report<sup>8</sup> documented the economic impact of 81 internet shutdowns that occurred in 19 countries from 1 July 2015 to 30 June 2016. The shutdowns led to a conservative estimate of US\$2.4 billion in economic damages, not counting loss of tax revenue or drops in investor confidence. Furthermore, CIPESA reports that internet shutdowns in Sub-Saharan Africa between January 2015 and September 2017 led to losses of at least US\$237 million.<sup>9</sup>

**NetBlocks** has developed a Cost of Shutdown Tool (COST) to estimate the hourly/daily economic impact of internet shutdowns. COST considers the GDP of a given country, the percent of GDP that is comprised of the digital economy, the duration of the shutdown, and the number and economic value of jobs supported by the internet and technology industry. For a 24-hour total shutdown in Zimbabwe, the estimated economic loss is US\$5.7 million, in the Democratic Republic of Congo it is US\$3.2 million.<sup>10</sup> For a partial shutdown of just social media in Zimbabwe, the daily cost is still upwards of US\$1 million.<sup>11</sup>

<sup>7</sup> “Rights to freedom of peaceful assembly and of association” Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (2019) A/HRC/41/41, paras. 52-53.

<sup>8</sup> Darrel M. West, “Internet shutdowns cost countries \$2.4 billion last year” *Brookings Institute* (October 2016) available at <https://www.brookings.edu/wp-content/uploads/2016/10/internet-shutdowns-v-3.pdf>

<sup>9</sup> “The Economic Impact of Internet Disruptions in Sub Saharan Africa” CIPESA (2017) [https://cipesa.org/?wpfb\\_dl=249](https://cipesa.org/?wpfb_dl=249)

<sup>10</sup> Cost of Shutdown Tool (COST), *NetBlocks*, (2019) tool available at <https://netblocks.org/cost/>

<sup>11</sup> If Facebook, Twitter, YouTube, Instagram and WhatsApp are blocked.

Economic costs can also be broken down to the individual level. For example, in Zimbabwe 97% of financial transactions in 2017 were mobile or electronic.<sup>12</sup> This means that small local businesses as well as large national corporations like banks suffer losses during an internet shutdown. Students who are attending school away from home cannot receive money transfers from their parents for daily living expenses. Families who rely on remittances from abroad cannot receive money. People who need to purchase medications from pharmacies may face difficulties in obtaining medicine.

In addition to the economic damages that occur during internet shutdowns, there are many societal and rights-based costs borne by citizens during a shutdown.

## 4.2 Journalism and the Media

Journalism and the media are greatly restricted during an internet shutdown. Shutdowns impact both their ability to receive newsworthy information, as well as their ability to share essential information with society. This violates the right to a free press and restricts both the right to access information as well as the right to freedom of expression.

## 4.3 Education

The internet is a portal to vast amounts of information and is becoming more and more essential for modern education. As part of the Sustainable Development Goals, the percentage of schools with access to the internet for pedagogical uses is one of the indicators that measures Goal 4: Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.<sup>13</sup> Internet shutdowns slow progress towards reaching these goals. The negative educational effects of an internet shutdown on tertiary education is also evident. Recently, Massive Open Online Courses (MOOCs) have been increasingly accessed by students in Africa. These free courses from universities such as Harvard and University of Witwatersrand allow students to learn subjects without the fees associated with attending college.<sup>14</sup> The growth of these services is matched with anecdotal evidence of students being unable to access them during internet shutdowns.<sup>15</sup>

## 4.4 Health

Internet shutdowns can have negative impacts on the health care system. Research on health impacts of internet shutdowns is limited, but anecdotal evidence points to negative impacts. For example, in Cameroon, health care apps such as GiftedMom connect rural women to doctors for health care advice for young children, such as immunisation scheduling.<sup>16</sup> These apps are unavailable during protracted internet shutdowns, such as the ones in Anglophone Cameroon which lasted for months. Furthermore, Cameroon was unable to submit 85% of its health-performance data to the District Health Information System data set DHIS2, which is used to guide

<sup>12</sup> Tawanda Karombo "Zimbabwe: 96% of total transactions in 2017 were electronic, mobile" IT Web Africa (18 February 2018) available at <http://www.itwebafrica.com/e-commerce/703-zimbabwe/242752-zimbabwe-96-of-total-transactions-in-2017-were-electronic-mobile>

<sup>13</sup> Global indicator framework for the Sustainable Development Goals and targets of the 2030 Agenda for Sustainable Development, A/RES/71/313 E/CN.3/2018/2.

<sup>14</sup> Eleni Mourdoukoutas "Why online courses are trending" (2017) available at <https://www.un.org/africarenewal/magazine/special-edition-youth-2017/why-online-courses-are-trending>

<sup>15</sup> James Jeffrey "Internet blackout forces young Ethiopians to go retro" DW (2016) available at <https://www.dw.com/en/internet-blackout-forces-young-ethiopians-to-go-retro/a-36490982>

<sup>16</sup> Okwen Mbah, Miriam Nkangu, & Zak Rogoff "Don't ignore health-care impacts of Internet shutdowns" *Nature* (2018) available at <https://www.nature.com/articles/d41586-018-05797-4>



funding decisions. This led to disruptions in funding flows and loss of wages for health care workers.<sup>17</sup> Internet shutdowns can also disrupt communication with doctors during emergencies. In Pakistan, a gynaecologist reported that an internet shutdown led a pregnant patient to not call her when she was feeling unwell. After the shutdown was over, the doctor found that the foetus was dead, and prior care may have been able to save the pregnancy.<sup>18</sup>

#### 4.5 Personal Security

Many people use messaging services to alert friends and family of dangerous security situations. Personal security may decline during an internet shutdown. This is especially true for people who belong to marginalised groups, such as Human Rights Defenders, the LGBTI community or those who participate in sex work.



<sup>17</sup> Okwen Mbah, Miriam Nkangu, & Zak Rogoff "Don't ignore health-care impacts of Internet shutdowns" *Nature* (2018) available at <https://www.nature.com/articles/d41586-018-05797-4>

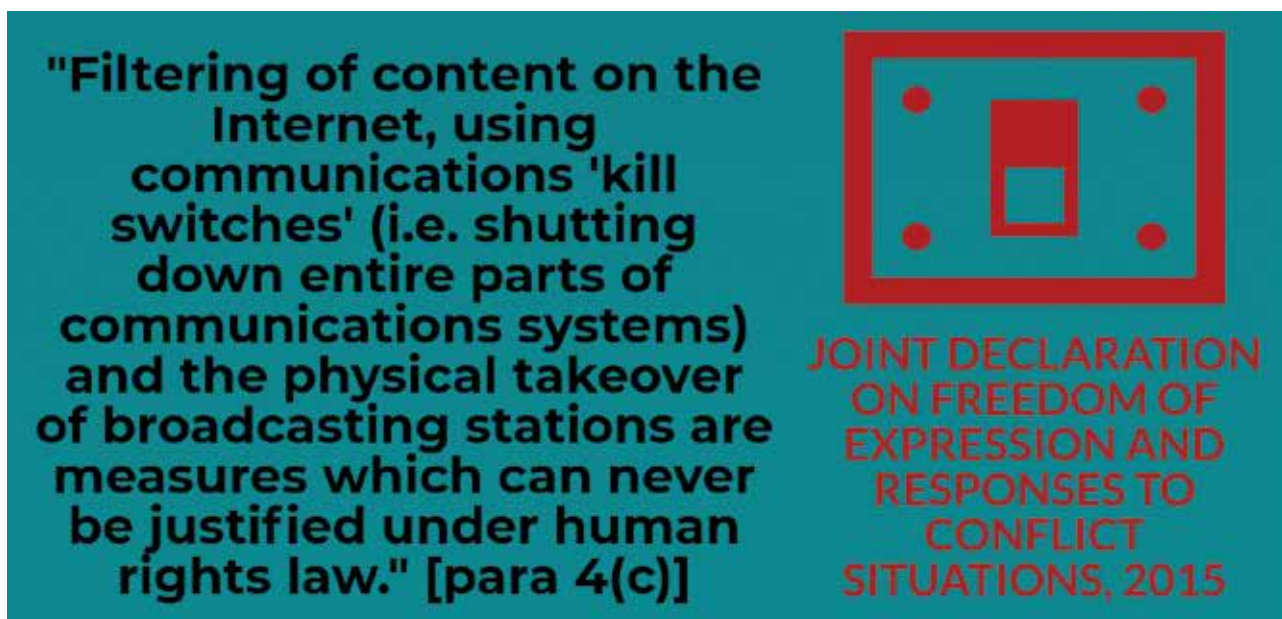
<sup>18</sup> "Pakistanis question government's use of bans on cell phones, other tech" PRI (2013) <https://www.pri.org/stories/2013-01-03/pakistanis-question-governments-use-bans-cell-phones-other-tech>

## 5. International Human Rights Framework and the Internet

In a report to the Human Rights Council, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression found that:

**"cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights."<sup>19</sup>**

Just a month later, a group of special representatives from the international and regional human rights bodies, including the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, issued the Joint Declaration on Freedom of Expression and the Internet.<sup>20</sup> The Joint Declaration recognised the "transformative nature of the Internet in terms of giving voice to billions of people around the world, of significantly enhancing their ability to access information and of enhancing pluralism and reporting" and recognised "the power of the Internet to promote the realisation of other rights and public participation, as well as to facilitate access



<sup>19</sup> Para. 78.

<sup>20</sup> Joint Declaration on Freedom of Expression and the Internet, adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission's Special Rapporteur on Freedom of Expression and Access to Information in Africa, (01 June 2011).

to goods and services”.<sup>21</sup> The Joint Declaration was concerned, however, that “some governments have taken action or put in place measures with the specific intention of unduly restricting freedom of expression on the Internet, contrary to international law”.<sup>22</sup>

The Joint Declaration lays out a clear framework for the intersection between human rights and the internet. This includes the foundational statement that:

**“Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognised under international law”.**<sup>23</sup>

The Joint Declaration also tied access to the internet to a plethora of other rights which States have an obligation to protect:

**“Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.”**<sup>24</sup>

The Joint Declaration was followed by a 2012 Resolution of the United Nations Human Rights Council,<sup>25</sup> which recognises “the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms” and affirms that “the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice,” and calls upon all States “to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries”.

In addition to freedom of expression, the internet is also integral to the modern exercise of the rights to freedom of association and freedom of assembly. In May of 2019, the Special Rapporteur on the rights to freedom of peaceful assembly and of association issued a report outlining the human rights implications of digital spaces for the exercise of freedom of association and assembly. The Special Rapporteur highlighted:

**“Technology serves both as a means to facilitate the exercise of the rights of assembly and association offline, and as virtual spaces where the rights themselves can be actively exercised.”**<sup>26</sup>

<sup>21</sup> Preamble.

<sup>22</sup> Preamble.

<sup>23</sup> 1(a).

<sup>24</sup> 6(a).

<sup>25</sup> “The promotion, protection and enjoyment of human rights on the Internet” HRC/RES/20/8 (2012).

<sup>26</sup> “Rights to freedom of peaceful assembly and of association” Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (2019) A/HRC/41/41, Para. 11

Furthermore, he pointed out that:

**“By serving both as tools through which these rights can be exercised “offline” and as spaces where individuals can actively form online assemblies and associations, digital technologies have vastly expanded the capacities of individuals and civil society groups to organize and mobilize, to advance human rights and to innovate for social change.”<sup>27</sup>**

Importantly, the Special Rapporteur confirms the conclusion that freedom of assembly and association are protected under international law both online and off:

**“Simply stated, international law protects the rights of freedom of peaceful assembly and of association, whether exercised in person, or through the technologies of today, or through technologies that will be invented in the future.”<sup>28</sup>**

## 5.1 Regional Law on Internet Rights and Freedoms

On 4 November 2016, the African Commission set down the Resolution on the Right to Freedom of Information and Expression on the Internet in Africa.<sup>29</sup> The Resolution was based on the recognition of “the importance of the Internet in advancing human and peoples’ rights in Africa, particularly the right to freedom of information and expression” and the recognition that “privacy online is important for the realisation of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association”.

The resolution was motivated by concern for “the emerging practice of State Parties ... interrupting or limiting access to telecommunication services such as the Internet, social media and messaging services, increasingly during elections”. The resolution “[c]alls on States Parties to respect and take legislative and other measures to guarantee, respect and protect citizen’s right to freedom of information and expression through access to Internet services”.

Following the string of internet shutdowns in late 2018 and early 2019 across the continent, the Special Rapporteur on Freedom of Expression and Access to Information in Africa issued a statement condemning the shutdowns. In his statement, he reiterated:

**“The internet and social media shutdowns violate the right to freedom of expression and access to information contrary to Article 9 of the African Charter on Human and Peoples’ Rights. The internet and social media have given voice to the people of Africa who may now discourse on social, economic and political issues far more than ever before, and states should not take away that voice. Citizens should not be penalised through shutdowns when they demonstrate calling for economic or political reforms or indeed during contested electoral campaigns or polling”.<sup>30</sup>**

<sup>27</sup> A/HRC/41/41, para. 21.

<sup>28</sup> A/HRC/41/41, para. 28.

<sup>29</sup> ACHPR/Res. 362(LIX) (2016).

<sup>30</sup> “Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa”, Banjul, Gambia (29 January 2019).

## 5.2 Limitations on Fundamental Human Rights

If freedom of expression applies on the internet in the same way that it applies off the internet, then limiting access to the internet will also have impacts on the exercise of freedom of expression. International human rights law includes boundaries on how governments can limit fundamental freedoms like the freedom of expression. For example, when the ICCPR protects the freedom of expression in Article 19, it states that there may be restrictions to that rights but only allows for restrictions that:

**“are provided by law and are necessary:**

**(a) For respect of the rights or reputations of others;**

**(b) For the protection of national security or of public order (ordre public), or of public health or morals.”<sup>31</sup>**

A similar standard is accepted by the African Commission on Human and Peoples’ Rights. In the Declaration of Principles on Freedom of Expression in Africa, the Commission states:

**“Any restrictions on freedom of expression shall be provided by law, serve a legitimate interest and be necessary and in a democratic society.”<sup>32</sup>**

These restrictions, however, cannot extinguish the right to expression. As the Human Rights Committee states in General Comment 34, “when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself...the relation between right and restriction and between norm and exception must not be reversed.”<sup>33</sup>

This principle applies to other human rights which are exercised online, such as freedom of assembly and association. As the Special Rapporteur on the rights to freedom of peaceful assembly and of association stated:

**“the freedom to access and use digital technologies for the exercise of peaceful assembly and association rights should be viewed as the rule, and the limitations as the exception.”<sup>34</sup>**

The ICCPR reiterates this principle:

**“Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant.”<sup>35</sup>**

So while restrictions on rights are permitted to preserve national security or public order, these restrictions must be narrow, proportionate, and must not defeat the ability to exercise one's right altogether.

<sup>31</sup> ICCPR, Art. 19(3).

<sup>32</sup> Declaration of Principles on Freedom of Expression in Africa, ACHPR, Done in Banjul, 23 October 2002.

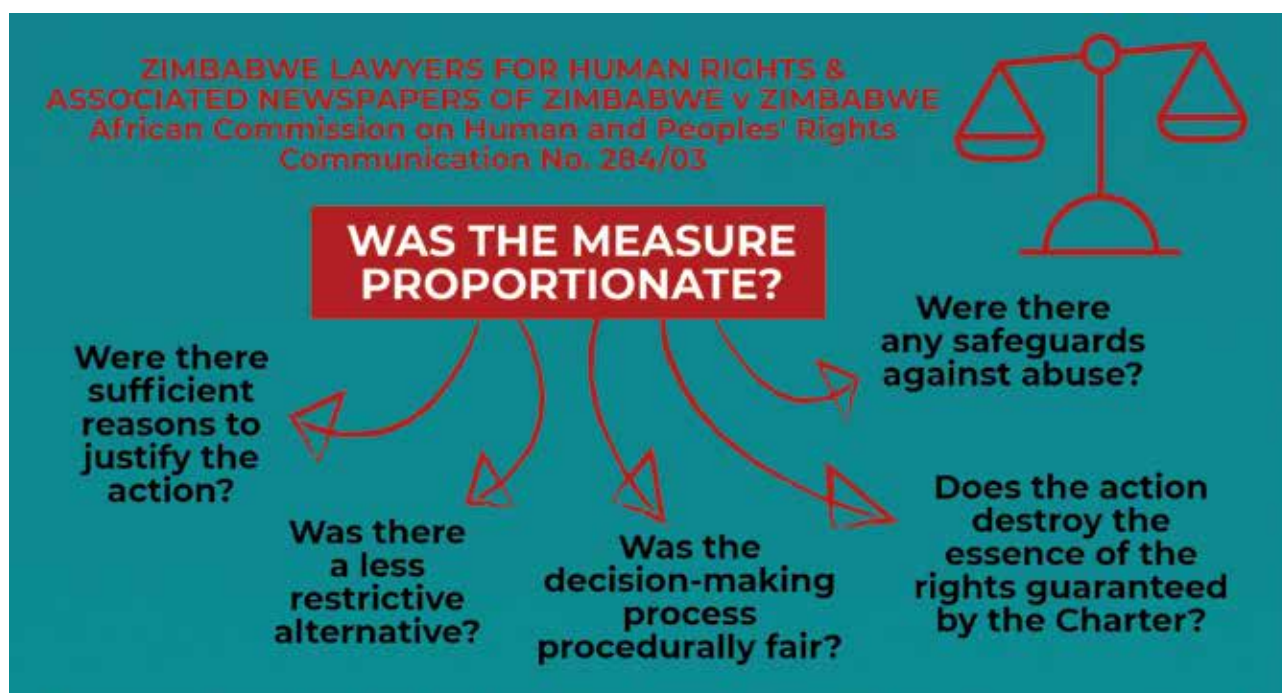
<sup>33</sup> General Comment 34, para. 21.

<sup>34</sup> “Rights to freedom of peaceful assembly and of association” Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (2019) A/HRC/41/41, para. 12.

<sup>35</sup> ICCPR Article 5(1).



### 5.3 Necessity and Legality



The narrowness of restrictions is further informed by the two requirements set out above: necessary and provided by law. Additionally, the necessity must tie back to the specified permitted categories. For example, the Committee states that, “[i]t is not compatible with paragraph 3...to invoke...laws to suppress or withhold from the public information of legitimate public interest that does not harm national security”.<sup>36</sup> Any internet shutdown that occurs that claims to protect public order or national security must actually target expression that is harming public order or national security.

A case before the Human Rights Committee, *Womah Mukong v Cameroon*, clarifies this point.<sup>37</sup> Womah Mukong was an author and advocate of multi-party democracy in Cameroon who was jailed and had his book banned in the country, among other abuses. The Committee found that there was a violation of Article 19 of the ICCPR. In making this determination it stated that:

**“the legitimate objective of safeguarding and indeed strengthening national unity under difficult political circumstances cannot be achieved by attempting to muzzle advocacy of multi-party democracy, democratic tenets and human rights; in this regard, the question of deciding which measures might meet the ‘necessity’ test in such situations does not arise.”<sup>38</sup>**

Many internet shutdowns occur during elections and periods of national protests. If the government gives a justification for the shutdown, they often point towards the necessity of maintaining order and national unity and wanting to prevent protests which may get out of control. Muzzling protesters, advocates, and opposition parties cannot achieve the aims of national unity in a democratic society that cares about human rights. Therefore, it is an impermissible justification, before even getting to the question of necessity and proportionality.

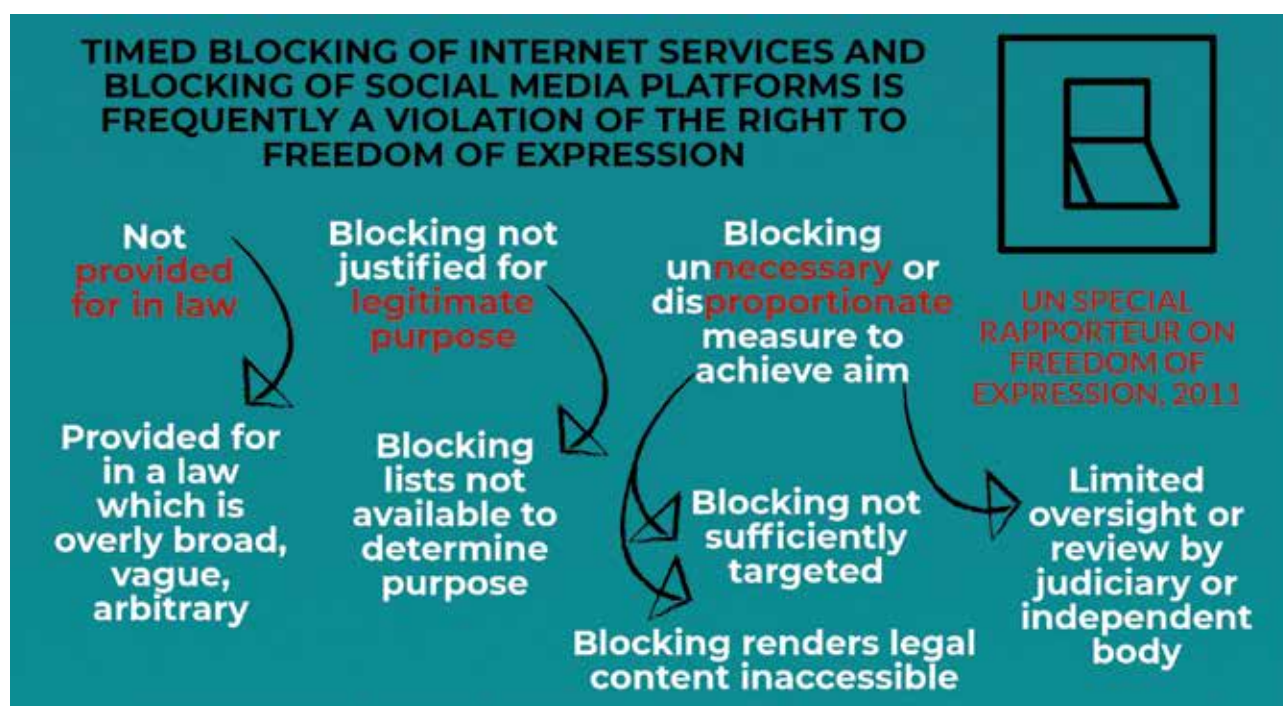
<sup>36</sup> General Comment 34, para. 30.

<sup>37</sup> *Womah Mukong v Cameroon*, U.N. Doc. CCPR/C/51/D/458/1991 (1994).

<sup>38</sup> *Womah Mukong v Cameroon*, U.N. Doc. CCPR/C/51/D/458/1991 (1994) para. 9.7.

Furthermore, a simple tenuous tie to national security or public order is not enough, because the measure of whether something is necessary or not is also one of proportionality. This idea was further expounded on by the committee:

**“The principle of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.”<sup>39</sup>**



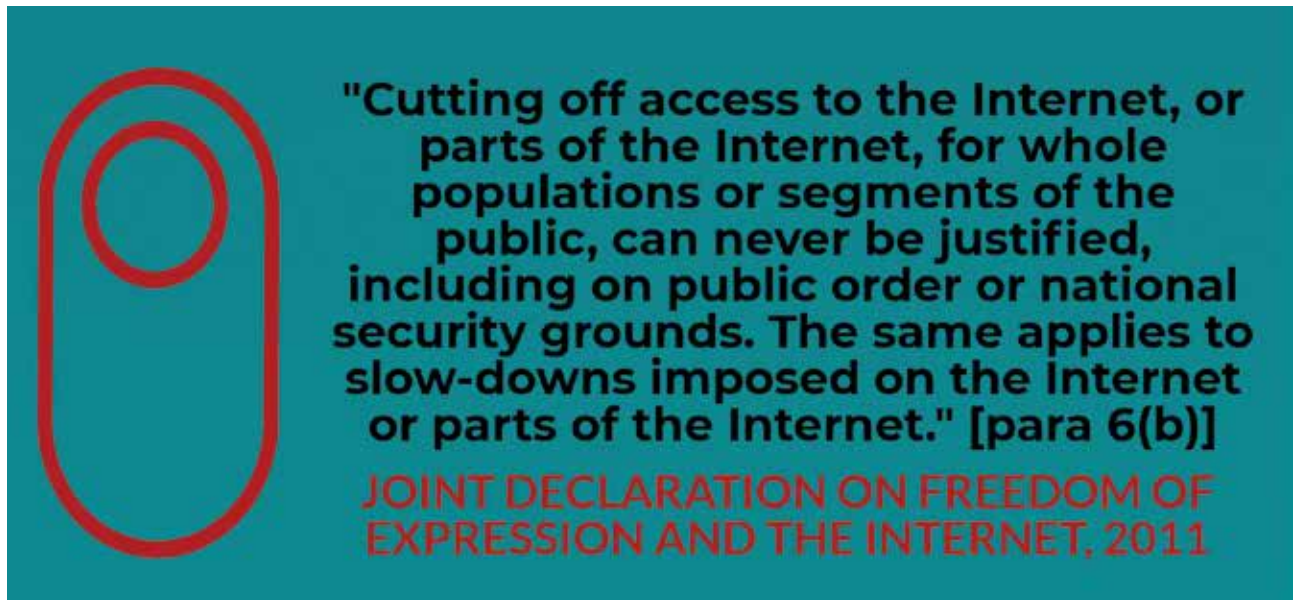
With human rights bodies recognising the integral role that internet plays in people's ability to exercise the freedoms of expression, association, assembly and ability to access information, access to its platforms must be given their proper weight in the proportionality test. The internet is a unique and important means of dissemination. Not only that, because of the plethora of ideas and opinions shared in digital spaces, some of the most important forms of expression, such as public and political debate, occur regularly online and on social media platforms.

**“When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.”<sup>40</sup>**

<sup>39</sup> General Comment 34, para. 34.

<sup>40</sup> General Comment 34, para. 35.

Total internet shutdowns, and even social media blockages, are a blunt tool, which wipe out access to an almost innumerable amount of conversations which represent important avenues of expression. Shutdowns are neither specific nor individualised. There is no justification for internet shutdowns that respects human rights. This opinion is shared by the Special Procedures who joined the Joint Declaration on Freedom of Expression and the Internet.<sup>41</sup>



The Joint Declaration's statements make it clear that shutting down the internet cannot be justified under any human rights-based approach to governance.

Lastly, any limitation to freedom of expression, association or assembly must be written in law. The legal regimes regulating telecommunications and ISPs in the countries in the region vary widely. The following section will explore the state of domestic laws. What is important is that many of the countries have no laws which explicitly authorise the government to order an internet shutdown. Without a clear statement in law, the order of an internet shutdown is a violation of the right to freedom of expression.

Another important aspect of legality, is that in addition to being written down, the order must carry the force of law. Legality questions both the authority backing a given order and the character of the law. Certain government directives, such as presidential declarations, may not carry the force of law. Laws which have been passed by a legislative body, and assented to by the executive carry the greatest force of law, and can authorise subsequent directives. The question of legality, however should be explored for the specific directives relied on in internet shutdowns.

<sup>41</sup> Joint Declaration on Freedom of Expression and the Internet, adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission's Special Rapporteur on Freedom of Expression and Access to Information in Africa, (01 June 2011)6(b).



Furthermore, the character of the law/order in question must also be “lawful”. General Comment 34 describes this as follows:

**“For the purposes of paragraph 3, a norm, to be characterized as a “law”, must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.”<sup>42</sup>**

For laws which contain provisions that allow for “any other” circumstance, this is often an indication of unfettered discretion. Provisions such as this should have their legality challenged.

## 5.4 Prior Restraint

The doctrine of prior restraint or prior censorship is a concept which restricts permissible limitations on freedom of expression. The presumption against prior restraint implies that the government should not suppress information before publication. If there is impermissible expression, such as incitement to violence, it should be penalised after the fact, rather than potentially impermissible or limitable expression being censored before publication. In the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, which have been repeatedly endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression and the United Nations Commission on Human Rights, Principle 23 reads:

### **“Principle 23: Prior Censorship**

**Expression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country under the conditions stated in Principle 3.”<sup>43</sup>**

The principle is also stated expressly in American Convention on Human Rights:

**“The exercise of [freedom of expression and opinion] shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:**

- a. respect for the rights or reputations of others; or**
- b. the protection of national security, public order, or public health or morals.”<sup>44</sup>**

Courts in the region have also relied on the doctrine of prior restraint. For example, the Constitutional Court of South Africa has affirmed Lord Scarman’s assertion:

<sup>42</sup> General Comment 34, para. 25.

<sup>43</sup> “The Johannesburg Principles on National Security, Freedom of Expression and Access to Information” Article 19 (November 1996).

<sup>44</sup> American Convention on Human Rights, adopted at the Inter-American Specialised Conference on Human Rights, San José, Costa Rica (22 November 1969), Article 13(2).

**“The prior restraint of publication, though occasionally necessary in serious cases, is a drastic interference with freedom of speech and should only be ordered where there is a substantial risk of grave injustice.”<sup>45</sup>**

When the government shuts down the internet, all online expression is subjected to prior restraint. This is a drastic interference of expression, and cannot be justified to apply to such sweeping categories as all online publications, or all publications on social media.

## 5.5 Human Rights and National Emergencies

Sometimes, nations face existential threats such as armed conflict or natural disaster which create circumstances which may allow for extraordinary restrictions on human rights. Article 4 of the ICCPR lays out the standard for these extraordinary derogations:

**“In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.”<sup>46</sup>**

The Human Rights Committee expounded on Article 4 in General Comment 29. The Committee highlighted that, “two fundamental conditions must be met: the situation must amount to a public emergency which threatens the life of the nation, and the State party must have officially proclaimed a state of emergency.”<sup>47</sup> The latter principle keeps intact the rule of legality for all restrictions on fundamental rights.

The first standard, “a public emergency which threatens the life of a nation”, is a high threshold, and typically signifies armed conflict. The Committee goes on to say that, “in other situations than an armed conflict, [States] should carefully consider the justification and why such a measure is necessary and legitimate in the circumstances”.<sup>48</sup> The Committee is concerned about both Constitutional thresholds which establish a lower standard,<sup>49</sup> as well as changes in circumstances which no longer rise to the level of public emergencies which threaten the life of a nation.<sup>50</sup>

<sup>45</sup> *Print Media South Africa and Another v Minister of Home Affairs and Another* (CCT 113/11) [2012] ZACC 22; 2012 (6) SA 443 (CC); 2012 (12) BCLR 1346 (CC) (28 September 2012) quoting with approval *Attorney-General v British Broadcasting Corporation*, the Court of Appeal of England and Wales [1981] AC 303 (CA) at 362.

<sup>46</sup> ICCPR, Article 4.

<sup>47</sup> CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency CCPR/C/21/Rev.1/Add.11 (2001) Para. 2.

<sup>48</sup> CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency CCPR/C/21/Rev.1/Add.11 (2001) Para. 3.

<sup>49</sup> See e.g. *United Republic of Tanzania* (1992), CCPR/C/79/Add.12, para. 7 (“The Committee is concerned over the unclear position of the Covenant in national law, particularly in cases where conflicts could arise between the Covenant and the Constitution. In this regard, article 32 of the Constitution regarding emergencies is clearly not in conformity with the international obligations of the State party under article 4 of the Covenant. Under that provision no derogation is permissible from certain fundamental rights, among which is the right to life. The Committee is concerned that the grounds for declaring a state of emergency are too broad and that the extraordinary powers of the President in an emergency are too sweeping. Other concerns of the Committee in regard to specific provisions of the Constitution which are incompatible with the Covenant include article 30 (1) which provides a wide scope for limitations of rights and freedoms and article 25 which provides for the possibility of forced labour.”)

<sup>50</sup> See e.g. *United Kingdom of Great Britain and Northern Ireland* (1995), CCPR/C/79/Add.55, para. 23.

The Covenant requires states to report when they declare national emergencies to the Secretary General of the United Nations.<sup>51</sup> This provides opportunities to review whether the two fundamental conditions are met.

If States use a public emergency to justify an internet shutdown, they must comply with all of the provisions of the ICCPR. In addition to demonstrating that conditions in a country are serious enough to rise to an existential threat, the State must also show that shutting down the internet is strictly required to address the emergency. These must be coupled with an official declaration of an emergency as provided for under the Constitution of the State in question, as well as a communication to the UN Secretary General.

---

<sup>51</sup> ICCPR, Article 4(3).

## 6. Domestic Laws

Typically, ISPs are regulated through the communication laws of a country. These laws usually cover radio, broadcast networks, telecommunication providers, and sometimes postal services. Examples of these include the Angola Law of Electronic Communication and Information Society Services,<sup>52</sup> the Botswana Communications Regulatory Authority Act,<sup>53</sup> the Malawi Communications Act,<sup>54</sup> or the Democratic Republic of Congo's Telecommunications Law.<sup>55</sup> In addition to communication laws, ISPs are also sometimes impacted by cyber security laws, laws providing for government surveillance, and penal codes.

COUNTRY	LAW
Angola	Lei das Comunicações Electrónicas e dos Serviços da Sociedade de Informação No. 23 of 2011 Regulamento Geral das Comunicações Electrónicas Decreto Presidencial No. 225 of 2011 Cria o INACOM Decreto Presidencial No. 243 of 2014
Botswana	Electronic Communications and Transactions Act No. 38 of 2016 Communications Regulatory Authority Act No. 15 of 1996 (commence 2013)
Democratic Republic of Congo	Act No. 13 of 2002 Postal and Telecommunications Regulatory Authority Act No. 14 of 2002
Eswatini	Swaziland Communication Commission Act No. 10 of 2013
Lesotho	Communications Act No. 4 of 2012
Madagascar	Act No. 23 of 2005
Malawi	Electronic Transactions and Cybersecurity Act No. 33 of 2016 Communications Act No. 34 of 2016
Mauritius	Information and Communications Technologies Act No. 44 of 2001
Mozambique	Lei das Telecomunicações No. 8 of 2004 Regulamento de Partilha de Infra – Estrutura de Telecomunicações e outros Recursos de Rede Decreto No. 65 of 2018 Aprova o Regulamento de Homologação de Equipamentos de Telecomunicações e Radiocomunicação Decreto No. 66 of 2018
Namibia	Communications Act No. 8 of 2009
Seychelles	Seychelles Media Commission Act No. 89 of 2011
South Africa	Electronic Communications Act No. 36 of 2005 Independent Communications Authority Act No. 13 of 2000
Tanzania	Electronic and Postal Communications Act No. 3 of 2010 Tanzania Telecommunications Corporation Act No. 12 of 2017 Media Services Act No. 12 of 2016
Zambia	Electronic Communications and Transactions Act No. 21 of 2009 Information and Communications Technology Act No. 15 of 2009
Zimbabwe	Postal and Telecommunications Act No. 4 of 2000

<sup>52</sup> Lei Quadro das Comunicações Electrónicas e dos Serviços da Sociedade da Informação, Act No. 23 of 2011.

<sup>53</sup> Botswana, Communications Regulatory Authority Act, Act No. 19 of 2012.

<sup>54</sup> Act No. 34 of 2016.

<sup>55</sup> Loi sur les télécommunications en République démocratique du Congo, Act No. 13 of 2002.

## 6.1 Protection of Digital Rights

Oftentimes, the communication laws specifically set out to protect the rights and security of consumers who use electronic communication networks (i.e. the internet). For example, the Angolan Law of Electronic Communications and Information Society Services specifically seeks to protect the rights and security of those who use electronic communication networks, including the internet.<sup>56</sup> This includes through Article 36 on the principle of electronic democracy.<sup>57</sup> Language like this in the communications law can be used to argue that shutting off the internet defeats the intent of the legislature, which passed these Acts to better realise the right to freedom of expression.

In Botswana, the Communications Regulatory Authority Act<sup>58</sup> establishes the Communications Regulatory Authority and also contains positive language about promoting access to communication services. The Board oversees broadcasting licenses, radio communication, postal services and telecommunication services.<sup>59</sup> The Board is charged to, “ensure, that so far as is practicable there are provided throughout Botswana, safe, reliable, efficient and affordable services”, including internet services. In the long list of delineated authorities given to the board, there is no mention of the right to shut off internet services. The Act further states:

**“Any person who...without lawful excuse, by any means interferes with or obstructs the provision or operation of a telecommunications, broadcasting or postal service... or does any act with intent to, or knowing that it is likely that such act will impair the usefulness or efficiency or prevent or impede the working of, any such equipment, commits an offence...”<sup>60</sup>**

A similar provision is found in the new Cybercrime and Computer Related Acts,<sup>61</sup> a law used to better regulate the internet in Botswana. This Act does not contain any provisions which authorize the government to shut down the internet, but it does provide legal prohibitions on interfering with the internet. Section 8 of the Act states:

**“A person who intentionally, without lawful excuse or justification-**

**(a) Hinders or interferes with the functioning of a computer or computer system; or**

**(b) Hinders or interferes with a person who is lawfully using or operating a computer or computer system,**

**Commits an offence...”<sup>62</sup>**

<sup>56</sup> Lei Quadro das Comunicações Electrónicas e dos Serviços da Sociedade da Informação, Act No. 23 of 2011, Articles 4 & 15(1)(g).

<sup>57</sup> Lei Quadro das Comunicações Electrónicas e dos Serviços da Sociedade da Informação, Act No. 23 of 2011, Article 36.

<sup>58</sup> Botswana, Communications Regulatory Authority Act, Act No. 19 of 2012.

<sup>59</sup> See Botswana, Communications Regulatory Authority Act, Act No. 19 of 2012, Section 2 Interpretation, “telecommunications service’ means the emission, transmission or reception of information, including voice, sound, data, internet and electronic communication, text, video, animation, visual images, moving images and pictures, signal or a combination thereof by means of magnetism, radio or other electronic waves, optical, electromagnetic system whether with or without the aid of tangible conduct, but does not include content service, and includes any service ancillary thereto...” (emphasis added).

<sup>60</sup> Botswana, Communications Regulatory Authority Act, Act No. 19 of 2012, Section 56.

<sup>61</sup> Act 18 of 2018.

<sup>62</sup> Cybercrime and Computer Related Acts, Act 18 of 2018, Botswana, Section 8(1).

The definition of “computer or computer system” is “an electronic, magnetic or optical device or a group of interconnected or related devices, *including the Internet*, one or more of which, pursuant to a programme, performs the automatic processing of data.”<sup>63</sup>

Provisions like these within domestic laws can be used to combat internet shutdowns. If a government official orders an internet shutdown and cannot point to a legal basis for the order, then that government official could be liable for an offence, such as the one above. Provisions such as this one can be used as leverage to get official statements of why and under what authority an order to shut off the internet is coming from, which should provide an avenue to challenge that order in court.

In a similar fashion, the Malawi Communications Act contains section 179 which states:

**“A person who, without lawful cause, interferes with or obstructs the transmission or reception of any electronic communications, commits an offence...”<sup>64</sup>**

Zambia’s Electronic Communications and Transactions Act<sup>65</sup> also provides:

**“A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users commits an offence...”<sup>66</sup>**

## 6.2 Independence of Regulatory Authorities

During internet shutdowns, the question of whether the regulating authorities operate independently from the government is raised. Oftentimes, communication statutes dictate that the commission should be independent. However, sometimes governments exert control over the commission to get them to order the internet shutdown, even when a shutdown contradicts the mandate of the commission to provide internet access to citizens. In other cases, like Zimbabwe, the government unilaterally shuts down the Internet without involving/consulting the national regulatory authority. Independence of the regulating authority also depends on the powers of the executive to control appointments to the authority.

The Malawi Communication Act dictates that the Malawi Communications Regulatory Authority should be independent.<sup>67</sup> This could provide a litigation avenue should there be evidence of Executive orchestration of an internet shutdown, which is ordered through the auspices of the Authority.

In a similar fashion, the Eswatini Communications Commission is established under the Eswatini Communications Commission Act<sup>68</sup> and states that “[n]otwithstanding the other provisions of this Act, the Commission shall carry out functions entrusted to the Commission by or under this Act or any other law in an objective, transparent, proportionate and non-discriminatory manner.”

<sup>63</sup> Cybercrime and Computer Related Acts, Act 18 of 2018, Botswana, Section 2.

<sup>64</sup> Malawi Communications Act, Act No. 34 of 2016, Section 179.

<sup>65</sup> Zambia Electronic Communications and Transactions Act, Act No. 21 of 2009.

<sup>66</sup> Zambia Electronic Communications and Transactions Act, Act No. 21 of 2009, Section 99(5).

<sup>67</sup> Malawi Communications Act, Act No. 34 of 2016, Section 5(3).

<sup>68</sup> Act No. 10 of 2013.



In the Democratic Republic of Congo, the Loi portant création de l'Autorité de régularisation de la poste et des télécommunications (ARPTC Law)<sup>69</sup> creates the Regulatory Authority of the Post and Telecommunications of Congo (ARPTC). The ARPTC is charged to be an independent body under the law.<sup>70</sup> The actual independence of the ARPTC is questionable. The recent internet shutdown in the Democratic Republic of Congo was ordered by the ARPTC through letters to telecommunication providers, assumedly in reference to Article 46 of the Telecommunications Law.

## Appointment of regulatory authority board



**Parliamentary control  
over appointments**

**Minister appoints but  
in consultation**

**Minister appoints  
most or all members**

**President appoints  
most or all of  
members**

## Independence of regulatory authorities



**Requirements for  
transparency,  
parliamentary oversight**

**Legally Independent**

**Ministers can guide**

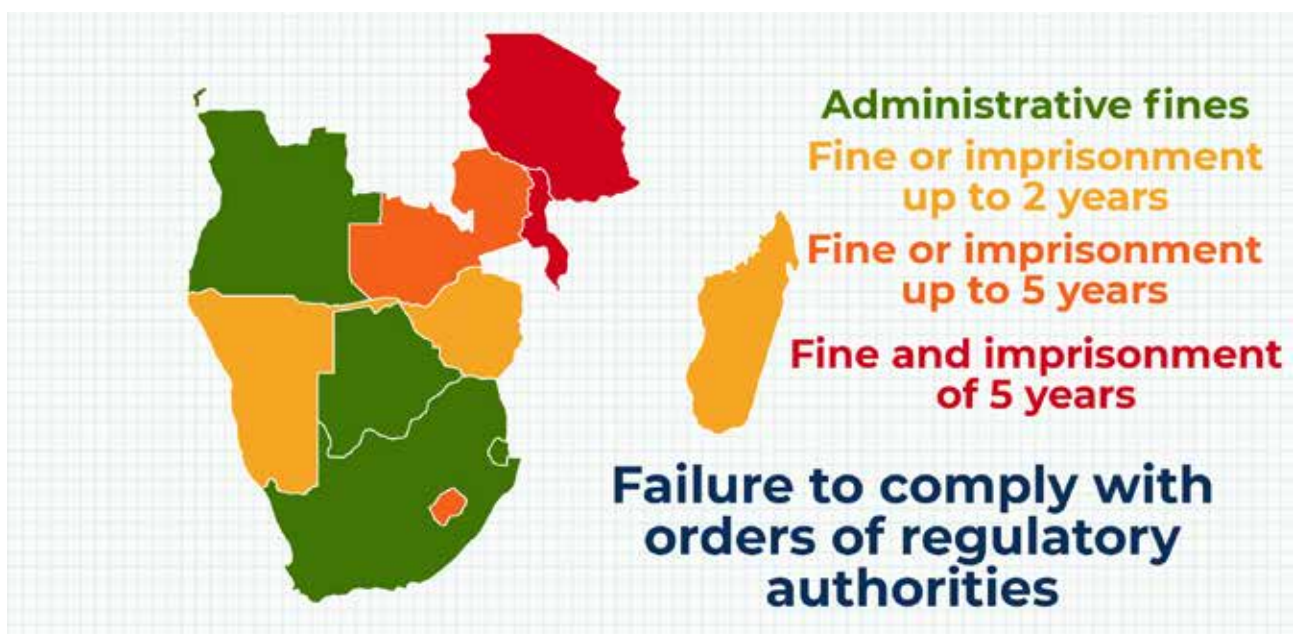
**Ministers can instruct**

<sup>69</sup> Loi portant création de l'Autorité de régularisation de la poste et des télécommunications, Act No. 14 of 2002, Democratic Republic of Congo.

<sup>70</sup> Loi portant création de l'Autorité de régularisation de la poste et des télécommunications, Act No. 14 of 2002, Democratic Republic of Congo, Article 14.

### 6.3 Ambiguity of Powers of Regulatory Authorities

Some Communication Acts provide broad powers to regulatory authorities. For example, the Malawi Communications Act,<sup>71</sup> establishes the Malawi Communications Regulatory Authority. In a list of enumerated powers, the Authority is charged to “protect public health and safety.”<sup>72</sup> Section 86 of the Act allows for search and seizure of license holders. This includes the power to “take any other action that it deems necessary”,<sup>73</sup> if it finds that an offence under the Act has occurred. This language is concerning, as it could be used by the government to justify an order of a shutdown due to concerns around public health and safety. More so, since under section 189, a licensee who fails to comply with an order issued by the Authority under the Act can be held liable of an offence which could attract a fine or imprisonment up to five years. Long prison sentences such as this one provide leverage for governments over communication license holders. When failure to follow an order from the ministry or regulatory authority may lead to loss of license, that is a strong enough penalty to exact obedience. The stakes are raised higher when long custodial sentences are in play.



In 2016, Malawi passed the Electronic Transactions and Cyber Security Act. The Act exercises primary jurisdiction over electronic transactions. Section 100 reads:

**“Where any inconsistency arises between a provision of this Act and a provision of any other written law relating to the regulation of electronic transactions, the provisions of this Act shall prevail to the extent of the inconsistency.”<sup>74</sup>**

While the Act prohibits the unlawful interference with access to an information system,<sup>75</sup> the Act also authorises the Minister to:

**“come up with specific cases where unauthorized access to, or interception of, or interference with, data may be permitted in specific conditions set out in the regulations.”**

<sup>71</sup> Act No. 34 of 2016.

<sup>72</sup> Malawi Communications Act, Act No. 34 of 2016, Section 6(2)(s).

<sup>73</sup> Malawi Communications Act, Act No. 34 of 2016, Section 86(3)(d).

<sup>74</sup> Malawi Electronic Transactions and Cyber Security Act, Act No. 23 of 2016, Section 100.

<sup>75</sup> Malawi Electronic Transactions and Cyber Security Act, Act No. 23 of 2016, Section 84(7).

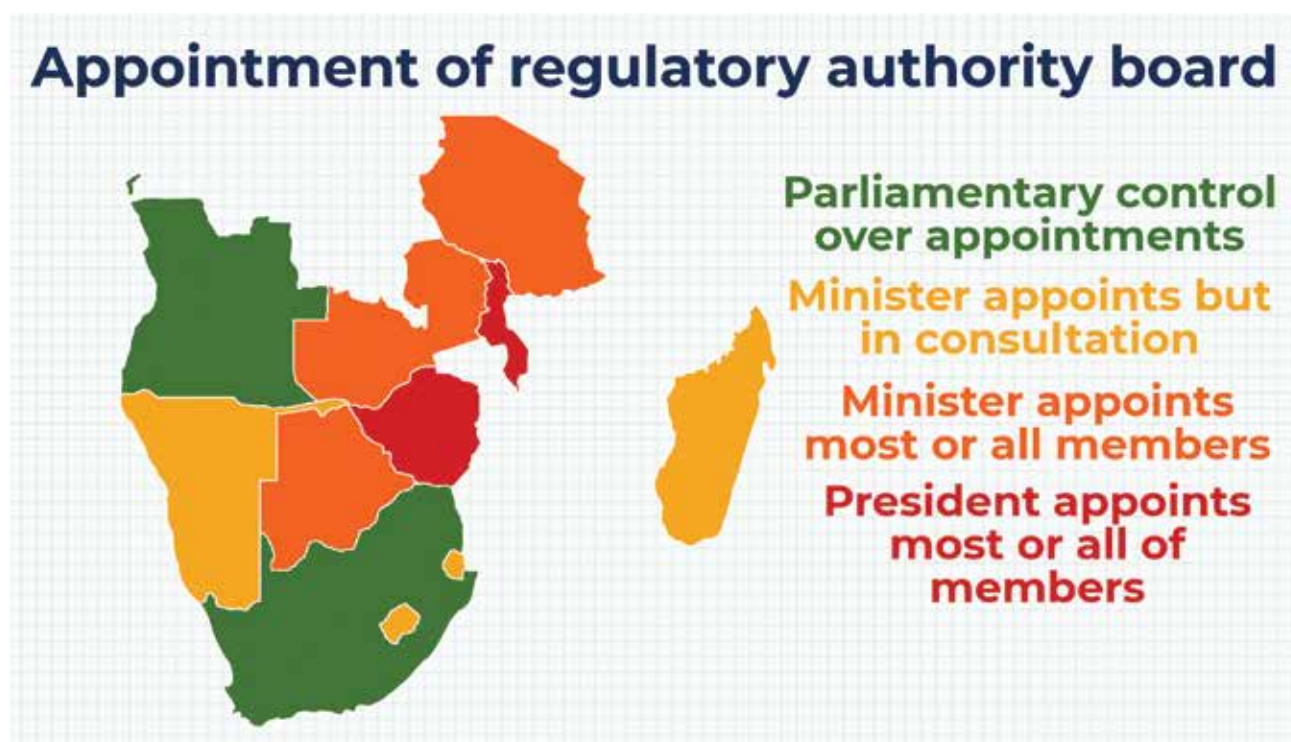


This provision continues to carve out space for the Minister to enact more explicit regulations authorising internet shutdowns.

In 2012, Lesotho passed the Communications Act, an “Act to provide for the regulation of the telecommunications, broadcasting and postal sectors, and for related matters.”<sup>76</sup> Under the Act, the Lesotho Communications Authority is authorised to act on matters dealing with the regulation of communication industries in Lesotho, and also “take any other action, not expressly prohibited by law that is necessary and proper to perform its duties and exercise its powers under this Act”.<sup>77</sup> The Lesotho Communications Authority (Administrative) Rules state:

**“A licensee shall comply with all regulatory requirements and obligations applicable to its type of license as may be stipulated in the Act, rules, licenses or any directives as may be issued by the Authority.”<sup>78</sup>**

This regulation creates liability should there be an order given by the Authority to shut down the internet.



Additionally, Zambia’s Electronic Communications and Transactions Act includes provisions which reserve the right of laws or courts to issue orders over ISPs and other licensees:

**“This Act does not limit the operation of any law that expressly authorises, prohibits or regulates the use of data messages, including any requirements, or under, any law for information to be posted or displayed in a specified manner, or for any information or document to be transmitted by a specified method.”<sup>79</sup>**

<sup>76</sup> Lesotho Communications Act, Act No. 4 of 2012, Preamble.

<sup>77</sup> Lesotho Communications Act, Act No. 4 of 2012, Section 5(1)(y).

<sup>78</sup> Lesotho Communications Authority (Administrative) Rules, Legal Notice 77 of 2016, Section 44(1).

<sup>79</sup> Zambia Electronic Communications and Transactions Act, Act No. 21 of 2009, Section 3(6).

This is repeated in section 63:

**“This Part does not affect...any obligation imposed by law or by a court, to remove, block, or deny access to any data message”.<sup>80</sup>**

While no express authorisations are outlined in these sections, they create ambiguities which could be raised by the government or courts to justify orders to switch off the internet.

These provisions are especially concerning because it was a provision like this that was used to authorise the 2019 internet shutdown in Zimbabwe. The preamble for Zimbabwe’s Interception of Communications Act<sup>81</sup> states that the purpose of the Act is “[t]o provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe; to provide for the establishment of a monitoring centre; and to provide for any other matters connected with or incidental to the foregoing.”<sup>82</sup>

Nowhere does it mention blocking or removing access to or the use of any postal service or telecommunication service. The Act goes on to explicitly state that the term “intercept” is defined “in relation to any communication which is sent— (a) by means of a telecommunication system or radio communication system, means to listen to, record, or copy, whether in whole or in part; (b) by post, means to read or copy the contents, whether in whole or part.”<sup>83</sup>

The Act clearly states reasons for which a warrant to intercept information may be given. In part, the Act reads that:

**“A warrant shall be issued ... if there are reasonable grounds for the Minister<sup>84</sup> to believe that—**

**...**

**(b) the gathering of information concerning an actual threat to national security or to any compelling national economic interest is necessary; or**

**(c) the gathering of information concerning a potential threat to public safety or national security is necessary.”<sup>85</sup>**

However, the Act goes on to give the Minister broader power than that to issue a warrant. In part 2, of Section 6, the Act states:

**“The Minister may, if he or she is of the opinion that the circumstances so require**

**(a) upon an application being made in terms of this Part, issue instead of a warrant any directive to a service provider not involving any interception or monitoring of communications...”<sup>86</sup>**

<sup>80</sup> Zambia Electronic Communications and Transactions Act, Act No. 21 of 2009, Section 63(b).

<sup>81</sup> Interception of Communication Act, Cap. 11:20.

<sup>82</sup> Interception of Communication Act, Cap. 11:20, Introduction.

<sup>83</sup> Interception of Communication Act, Cap. 11:20, Section 2(1).

<sup>84</sup> Initially, the Interception of Communications Act was administered by the office of a designated government/ cabinet Minister, typically the Minister of Information Communication Technologies, Postal and Courier Services. However, in 2018 administration of the Interception of Telecommunications Act was assigned directly to the President of Zimbabwe. Statutory Instrument 212 of 2018 as read with section 104(1) of the Constitution of Zimbabwe. The designation “Minister” in the Act therefore, currently refers to the President of Zimbabwe.

<sup>85</sup> Interception of Communication Act, Cap. 11:20, Sections 6(1)(b) and (6)(1)(c).

<sup>86</sup> Interception of Communication Act, Cap. 11:20, Sections 6(2).

The power to issue any directive to a service provider, which must be obeyed under the threat of imprisonment,<sup>87</sup> is an extremely broad power which has the opportunity to unconstitutionally limit the fundamental rights of Zimbabweans. And indeed, it unconstitutionally limited the freedom of expression of millions of Zimbabweans during the internet shutdown.

LEGISLATIVE AUTHORISATIONS FOR COMMUNICATION INTERCEPTION OR TAKE DOWN NOTICES					
	LEGISLATION	REQUEST	AUTHORISATION	SCOPE OF THE AUTHORISATION	BROAD POWERS
Angola	Lei das Comunicações Electrónicas e dos Serviços da Sociedade de Informação No. 23 of 2011	Lei No. 23 of 2011 § 55	Lei No. 23 of 2011 § 55	Decreto Presidencial No. 243 of 2014	Lei No. 23 of 2011 § 55
Botswana	Electronic Communications and Transactions Act No. 38 of 2016	§§ 44(1) & 45(2)	§§ 44(1) & 45(2)	§§ 44(2) & 45(2)	
Eswatini	Electronic Communications Act No. 9 of 2013	§ 15(j)	§ 15(j)	§ 15(j)	§§ 15(a) & (j)
Lesotho	Criminal Procedure and Evidence Act, 1981; Communications Act No. 4 of 2012	Crim. Proc. Act §§ 46-49	Crim. Proc. Act §§ 46-49	Crim. Proc. Act §§ 46-49	Com. Act § 20
Malawi	Electronic Transactions and Cyber Security Act No. 33 of 2016	§ 70(1)	§ 70(1)(c)	§ 70(1)	§ 70(1)(b)(ii)
Mauritius	Information and Communication Technologies Act No. 44 of 2001 (last amended 2018)	§ 25(3)	§ 25(3)	§ 25(3)	§§ 3(2) & 19
Mozambique	Código de Process Penal, 1931 (last amended 1993); Lei das Telecomunicações No. 8 of 2004	Crim. Proc. Act § 229	Crim. Proc. Act §§ 29 & 229	Crim. Proc. Act § 229	Com. Act, § 59
Namibia	Communications Act No. 8 of 2009	§ 70(2)	§ 70(8)	§ 70(8)	
South Africa	Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 (last amended 2008)	§§ 16-25	§§ 16-25	§§ 2-15	
Tanzania	Electronic and Postal Communications Act No. 3 of 2010; Cybercrimes Act No. 14 of 2015	Com. Act § 163(1); Cyber. Act § 31(1)	Com. Act § 163(6); Cyber. Act § 31(1)	Com. Act § 163(1); Cyber. Act § 31(1)	Com. Act §§ 114 & 124
Zambia	Electronic Communications and Transactions Act No. 21 of 2009	§§ 66(1) & 95	§§ 66(2), 66(3), & 96(1)	§§ 66(3), 67, 68 & 96(2)	
Zimbabwe	Interception of Communications Act No. 6 of 2007	§ 5	§ 6	§ 7	§ 6(2)

<sup>87</sup> Interception of Communication Act, Cap. 11:20. Section 9(2).

The Supreme Court of Zimbabwe held a similar provision unconstitutional in *Law Society of Zimbabwe v Minister of Transport and Communications and Another*.<sup>88</sup> In a now repealed section of the Postal and Telecommunications Act<sup>89</sup> it stated in part:

**“If, in the opinion of the President it is necessary in the interests of national security or the maintenance of law and order, he may give a direction that ...**

**(a) any cellular telecommunication or telecommunication service established, maintained or worked by a cellular telecommunication or telecommunication licensee or any class of such services shall be suspended or that such service shall be suspended in respect of a person named in the direction.”<sup>90</sup>**

The provision, along with a similar section 103, were declared unconstitutional, and were later repealed. In holding that the provisions were unconstitutional, the Court stated:

**“The net effect of the failure to provide statutory mechanisms to control or limit the exercise of the power conferred by the Act on the President leads to an unfettered discretion to intercept mail and communication. The impugned sections provide no guidance as to what a citizen should not do to avoid conduct that might lead to the exercise of the powers conferred by the impugned sections. The Act provides no legal recourse or safeguard for the innocent. The Act does not provide any mechanisms for accountability. Similar legislation in other jurisdictions provides or is required to provide, for prior scrutiny, independent supervision of the exercise of such powers and effective remedies for possible abuse of the powers. The Act provides for no such safeguards.**

**The issue here is not that the powers have been abused or are likely to be abused by the President but rather that there are no mechanisms in the Act to prevent such an abuse. In the absence of such limitations and control mechanisms the powers conferred on the President are too broad and overreaching to be reasonably justified in a democratic society. The impugned sections, as I have already stated, are so vague that the citizen is unable to regulate his conduct in such a way as to avoid the interception of his mail or communication. Thus, in this regard, the impugned sections of the Act are too vague and do not satisfy the constitutional requirement of ‘provided by law’.”<sup>91</sup>**

Similar concerns remain when the Minister may issue “any directive” to holders of telecommunication licenses. This section of the Interception of Communication Act allows “unfettered discretion” on what an allowable directive is. Without statutory limitations, the limitation is overly broad and cannot be said to be “provided by law” as is required for limitations on fundamental rights such as freedom of expression.

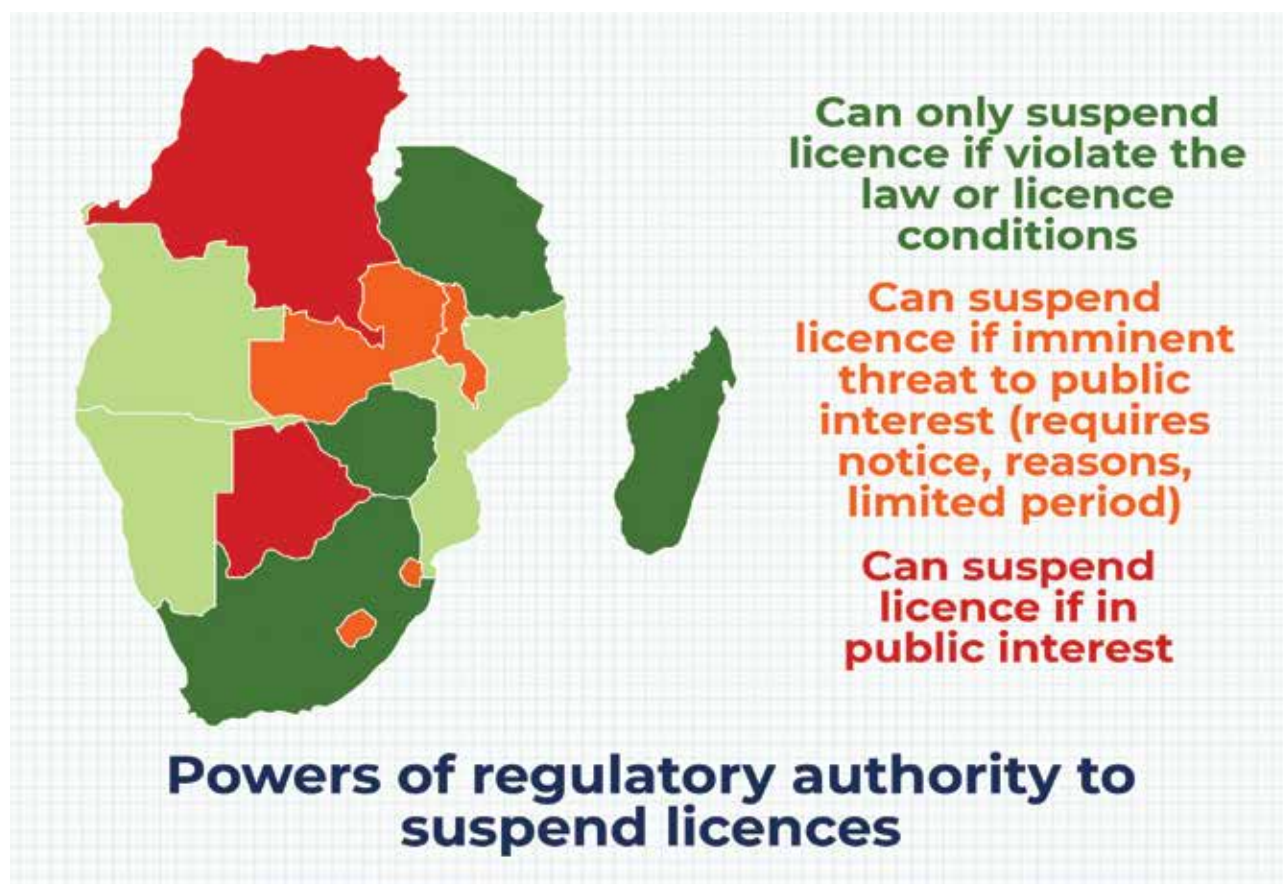
<sup>88</sup> *Law Society of Zimbabwe v Minister of Transport and Communications and Another* (28/02) ZWSC 127 (02 March 2004).

<sup>89</sup> Cap. 12:05.

<sup>90</sup> 98(2)

<sup>91</sup> *Law Society of Zimbabwe v Minister of Transport and Communications and Another* (28/02) ZWSC 127 (02 March 2004).

## 6.4 Legislated Authorisations for Suspension of Communications



The laws of the Democratic Republic of Congo provide some of the clearest authorisations for shutting down the internet. In the Democratic Republic of Congo's Telecommunications Law,<sup>92</sup> the Minister is charged with the general supervision and policing of the telecommunication sector, in collaboration with the ministries of justice, interior, defence and security.<sup>93</sup> Article 46 of the Telecommunications Law states:

**"The State may, either for reasons of public security or defence of the territory, whether it is in the interest of the public service telecommunication or for any other reason, prohibit in whole or in part, and during the time determined, the use of telecommunications facilities.**

**The State may also, in the cases referred to in the first paragraph of this section, requisition the telecommunications facilities.**

**The people usually serving these facilities may be required to render their services to the competent authority if they so require it."**<sup>94</sup>

<sup>92</sup> Loi sur les télécommunications en République démocratique du Congo, Act No. 13 of 2002.

<sup>93</sup> Loi sur les télécommunications en République démocratique du Congo, Act No. 13 of 2002, Article 6(e)

<sup>94</sup> Loi sur les télécommunications en République démocratique du Congo, Act No. 13 of 2002, Article 46, ("L'Etat peut, soit pour des raisons de sécurité publique ou de la défense du territoire soit dans l'intérêt du service public de télécommunications soit pour tout autre motif, interdire en tout ou en partie, et durant le temps qu'il détermine, l'usage des installations de télécommunications.

L'Etat peut également, dans les cas visés au premier alinéa du présent article, réquisitionner ou faire réquisitionner par les fonctionnaires désignés par lui, les installations de télécommunications.

Les personnes desservant habituellement ces installations peuvent être tenues de prêter leurs services à l'autorité compétente si elles en sont requises par celle-ci.")



Another law that is concerning in that it could be interpreted to authorise government blockages of the internet is found within the Zambia Penal Code:

**“If the President is of the opinion that there is in any publication or series of publications published within or without Zambia by any person or association of persons matter which is contrary to the public interest, he may, in his absolute discretion, by order published in the Gazette and in such local newspapers as he may consider necessary, declare that that particular publication or series of publications, or all publications or any class of publication specified in the order published by that person or association of persons, shall be a prohibited publication or prohibited publications, as the case may be.”<sup>95</sup>**

While this law was passed in reference to published materials, it could be interpreted by government to include any published websites. Especially the provision which targets “any class of publication” could be used to target large swaths of the internet such as all Facebook pages, or all social media. Similar provisions can be found in the Penal Codes of Botswana<sup>96</sup> and Malawi.<sup>97</sup>

## 6.5 Legality of Executive Directives

Many times the orders which are given to ISPs to shut down the internet are Presidential Directives or Executive Directives. While these directives carry some legally binding authority, they cannot always be considered to carry the force of law. This point was highlighted by the Botswana Court of Appeals in *Attorney General and Others v Tapela*. The Court stated:

**“Counsel for the appellant sought, but without much conviction, to categorize a Presidential Directive as a law, so as to bring it within the compass of section 15(1) as read with 15(4)(b) of the constitution, but that argument cannot be sustained. First, neither of the Presidential Directives referred to has been produced, and so no informed discussion of these is possible. Before us is only an administrative direction given by the Permanent Secretary by means of a savingram. Certainly that does not amount to a law. Secondly, and in any event, Presidential Directives convey government decisions, taken by the President acting on the advice of the Cabinet. These are an exercise of executive power under section 47(1) of the Constitution as read with section 50(1) and (2). They are binding on public officers but do not amount to a law. The exercise of executive power is subject to the Constitution and subject to the laws of the land. That is the essence of the rule of law, to which Botswana is a proud adherent. The discrimination practiced here, far from being authorized by any law, flies in the face of the Prisons Act and the Regulations made under it (both of which are clearly laws).”<sup>98</sup>**

The court referenced section 15(4)(b) of the Constitution of Botswana which is a section outlining permissible limitations on the fundamental right prohibiting discrimination. As was outlined above in the section on the need for proportionality and legality in limitations to fundamental rights, those same principles apply

<sup>95</sup> Zambia Penal Code, Section 53(1).

<sup>96</sup> Botswana Penal Code, Cap. 08:01, Section 47.

<sup>97</sup> Malawi Penal Code, Cap. 07:01, Section 46.

<sup>98</sup> *Attorney General and Others v Tapela*, Botswana Court of Appeals, Judgment in Civil Case No. CACGB-096-14 and Civil Case No. CACGB-076-15, para. 60.

to limitations on constitutional rights. What is important about the *Tapela* decision is that it outlines how presidential directives fail to meet the legality prong of that test. Just because a directive is written down, it does not mean that that directive carries the force of law. Without the force of law, it cannot be used as a proper justification to limit constitutional rights. This argument can be used to challenge executive directives ordering internet shutdowns.

## 6.6 Communication Laws and Declarations of Emergency

Some communication laws contain explicit authorisations to shut off the internet during national emergencies. For example, the Lesotho Communication Act contains the following provision:

### **“20. Prior restraint**

**(1) No licensee shall be prevented or impeded, either directly or indirectly, from providing service, unless either—**

**(a) the Authority has suspended or revoked the licensee’s licence; or**

**(b) the Minister issues an emergency suspension order.**

**(2) The Minister shall only issue an emergency suspension order if the Minister has a reasonable basis to conclude that continued operation by a licensee poses a substantial, direct and imminent threat to national security or public order and that there is no other way to forestall the threat other than to act in the manner provided for in this subsection.**

**(3) Any emergency suspension order shall—**

**(a) be in writing;**

**(b) explain the basis for the suspension; and**

**(c) remain in effect for no more than 72 hours, unless extended by a court of competent jurisdiction.”<sup>99</sup>**

This law carefully follows the standards established under international human rights law for permissible limitations to freedom of expression: it is contained in law, it references allowable bases (national security and public order), and its language requires it to be necessary and proportional. Should litigation be brought to challenge this provision, it would most likely need to challenge its application. As was stated above, special rapporteurs on freedom of expression, including the African Commission’s Special Rapporteur on Freedom of Expression, have stated that an internet shutdown can never be justified by national security or public order. A factual argument on necessity and proportionality would need to be determined by the courts.

Furthermore, other communication laws contain provision for national emergencies that do not include authorisation for shutting off the internet. For example, the Botswana Communications Regulatory Authority Act states:

**“The Authority may, during any emergency, require any service provider to give priority to the transmission of the messages of Government or of any person, and to intercept messages transmitted under such circumstances.”<sup>100</sup>**

<sup>99</sup> Lesotho Communications Act, Act No. 4 of 2012, Section 20.

<sup>100</sup> Botswana, Communications Regulatory Authority Act, Act No. 19 of 2012, Section 53(1).

This guaranteed access for government officials to telecommunication systems during emergencies points to the extreme importance of their function. The absence of authorisation to shut off telecommunications, even during pre-considered “emergency conditions”, should point to the legislature’s purposeful exclusion of that authority. It also is evidence that should a shutdown occur in a country with a similar provision, it is likely not authorised by law, therefore it should fail the legality test required under the ICCPR.

## 6.7 Contract Law

One of the difficulties in challenging internet shutdowns is the dearth of information available when they happen. Often, government will verbally order ISPs to cut off access to the internet, and following a break in connectivity, the government will not acknowledge any involvement in the interruption to services, and the ISPs will not acknowledge any government participation. If this situation occurs, a successful challenge to the internet shutdown will first require the disclosure of who authorised the shutdown.

One strategy that can be pursued is to bring a lawsuit against service providers based on provisions within the service contract. For example, within the service provider contract for MIC Tanzania, the following provision is included:

**“On activation, the CUSTOMER will be entitled to the quality of service generally provided by a competent mobile telecommunications service provider exercising reasonable skill and care and pursuant to the applicable requirements under the licence to MIC.”<sup>101</sup>**

Should the internet be disrupted, a customer of MIC could bring a suit alleging the inability to access the internet evidences that the service is NOT the “quality of service generally provided” when reasonable skill and care is exercised. If MIC wants to raise the defence that the breakdown in service was reasonable due to a government order, this will provide access to information regarding government participation, which can then be used to indemnify the government. This information can also be used to bring a separate suit against the government challenging the legality of the order.

Challenges based on contract law, however, are dependent on the terms of the contract, and the jurisprudence on contract interpretation. In an example of a service contract from Botswana, the contract states that:

**“Orange will use reasonable efforts to make the Services available to the Subscriber at all times.”<sup>102</sup>**

However, the contract’s limited liability clause includes the following language:

**“Orange Botswana shall not be liable to the Subscriber for any loss or damage suffered by the...subscriber whether same is direct or consequential, if...[t]he network Services are interrupted, suspended or terminated, for whatsoever reason.”<sup>103</sup>**

<sup>101</sup> “Subscriber/Customer Terms & Condition” MIC Tanzania Ltd. (2019) para. 3.7, available at <https://www.tigo.co.tz/mic-tanzania-ltd-subscriber-customer-terms-and-conditions>.

<sup>102</sup> “Orange Postpaid Terms and Conditions” Orange Botswana (2019) Para. 3.1.

<sup>103</sup> “Orange Postpaid Terms and Conditions” Orange Botswana (2019) Para. 16.1.



Orange might raise the defence that they are not liable for network interruptions, and thus stave off the need to raise a defence of reasonableness based on obeying a government order. The provision of the Orange Botswana contract stands in contrast to the liability limitation in the previously referenced MIC Tanzania contract:

**“unless occasioned negligently, The CUSTOMER indemnifies and holds MIC harmless against all and any loss, liability, actions, suites, proceedings, costs, demands and damages of all and every kind, (including direct, indirect, special or consequential damages), arising out of or in connection with the failure or delay in the performance of Services offered or the use of Services.”<sup>104</sup>**

The opening caveat of negligence preserves the reasonableness standard demarcated in the service quality provision, and makes it more likely that a court will require the company to show that service interruptions were reasonable.

<sup>104</sup> “Subscriber/Customer Terms & Condition” MIC Tanzania Ltd. (2019) para. 4.13, available at <https://www.tigo.co.tz/mic-tanzania-ltd-subscriber-customer-terms-and-conditions>.

## 7. Internet Shutdowns during Elections

Free and fair elections are an essential part of a participatory democracy. Internet shutdowns have been occurring with increasing frequency during elections, or between elections and the release of the results. States have passed specific laws which govern how elections should be conducted in order to protect the will of the people in electing the government. Oftentimes these laws provide additional protection for avenues of communication and freedom of expression, which could be violated during an internet shutdown.

ELECTION LAWS AND REGULATIONS					
	ELECTORAL ACT	REGULATIONS	MEDIA REGULATIONS AND FREEDOM OF EXPRESSION	POWER OF THE ELECTORAL COMMISSION	ELECTION OFFENCES
Angola	Electoral Act No. 6 of 2005; Law of the President of the Republic Decree No. 319-A of 1976 (last amended 2018)	Codigo de Conduta Eleitoral (da Assembleia Nacional) Resolucao No. 7 of 2012	Electoral Act § 78; Decree § 48; Lei De Imprensa No. 1 of 2017	Constitution of Angola, Art. 107	Electoral Act §§ 80-83; Acordao No. 412 of 2016; Lei do Registo Eleitoral Oficioso. Acordao No. 462 of 2017
Botswana	Electoral Act, Cap. 02:09 (last amended 2012)	National Broadcast Board, Code of Conduct for Broadcasters During Elections (Code of Conduct)	Code of Conduct	Constitution of Botswana, Art. 65A & 66	Electoral Act §§ 90-115, 141-149;
Eswatini	Elections Act No. 10 of 2013; Voter Registration Act, 2013; The Elections and Boundaries Commission Act No. 3 of 2013		Elections Act § 16(6)	Constitution of Eswatini, Art. 90; Elections and Boundaries Commission Act § 7	Elections Act §§ 42, 75-88
Lesotho	National Assembly Electoral Act No. 1 of 2011	Schedule 2 - Electoral Code of Conduct	Electoral Act §§ 62, 67; Code of Conduct, paras. 3 & 4	Electoral Act §§ 134-152	Electoral Act §§ 156-182

Malawi	Parliamentary and Presidential Elections Act, Cap. 2:01 (last amended 1998); Electoral Commission Act, Cap. 2:03 (last amended 2010)	Electoral Code of Conduct for Political Parties and Candidates (2019)	Elections Act §§ 59, 63; Code of Conduct §§ 4, 8 & 10	Electoral Commission Act § 8	Elections Act §§ 61, 115; Code of Conduct § 7
Mauritius	Representation of the People Act, 1968 (last amended 2005)	National Assembly Elections Regulations, No. 12 of 1968; Code of Conduct for the National Assembly Elections 2014	Code of Conduct, Article 3	Representation Act § 3; Constitution of Mauritius Art. 38-41	Representation Act §§ 58-74
Namibia	Electoral Act, No. 5 of 2014	Schedule 2 - Bill of Fundamental Voters' Rights and Duties	Electoral Act §§ 49; Schedule 2, para. 3	Electoral Act §§ 3, 4	Electoral Act §§ 173-191
South Africa	Electoral Act, No. 73 of 1998 (last amended 2019); Electoral Commission Act, No. 51 of 1996	Election Regulations GN R12 in GG 25894 of 7 January 2004 (last amended 2014)	Electoral Act Schedule 2, § 8	Constitution of South Africa, Art. 190; Electoral Commission Act, § 5; Electoral Act Schedule 2, § 7	Electoral Act §§ 87-94; Schedule 2, § 9
Tanzania	National Elections Act, cap. 343 (last amended 2015)	The National Elections Regulations 2015 GN No. 307 of 2015; The National Elections Rules 2010 GN No. 447 of 2010 (last amended 2012)	National Elections Act § 53	Constitution of Tanzania, Art. 74; National Elections Act § 4	National Elections Act §§ 87-106
Zambia	Electoral Process Act No. 35 of 2016; Electoral Commission Act No. 25 of 2016	Code of Conduct, SI No. 60 of 2016	Code of Conduct §§ 7(1) & 9(1)	Electoral Commission Act, § 4; Electoral Process Act § 4	Code of Conduct § 15(1)
Zimbabwe	Electoral Act, Cap. 2:13 (last amended 2018)	Electoral Code of Conduct for Political Parties and Candidates (Fourth Schedule)	Electoral Act §§ 40A-40F, 160E-160K; Code of Conduct §§ 2 & 4	Constitution of Zimbabwe, Art. 239; Electoral Act §§ 4A, 5, Schedule 6	Electoral Act §§ 37, 66A, 80, 133-160; Code of Conduct §§ 5 & 6

## 7.1 Offences during Election Time

In 2016, Zambia overhauled its elections laws with the passage of the Electoral Process Act.<sup>105</sup> Under both the Act, and a new Electoral Code of Conduct passed that same year,<sup>106</sup> Zambia established a list of election period offences. The offences include the following two prohibitions:

**"A person shall not –**

**...**

**(e) prevent the reasonable access to voters of any candidate or political party in any manner for the purposes of conducting voter education, fund raising, canvassing membership or soliciting support;**

**...**

**(g) deface, remove or destroy any political campaign materials of any person or political party or publications of the Commission"**<sup>107</sup>

In modern elections, the internet is becoming a primary way to access information about voting, elections, and political parties. A complete internet shutdown removes reasonable access to the essential information protected within the ambit of these offences. This can be raised when litigating on an internet shutdown during the election period.

A similar provision can be found within the South African Electoral Act, which makes it an offence to prevent candidates and political parties "from gaining reasonable access to voters, whether in a public or private space".<sup>108</sup>

## 7.2 Reporting Obligations of the Media

In some electoral laws and regulatory schemes, the media is tasked with specific reporting requirements to ensure unbiased access to accurate information over the course of an election. For example, in the Zambia Electoral Code of Conduct, it states:

**"(1) Print and electronic media shall—**

**(a) provide fair and balanced reporting of the campaigns, policies, meetings, rallies and press conferences of all registered political parties and candidates during the campaign period;**

**(b) provide news of the electoral process up to the declaration of results"**<sup>109</sup>

**"Media shall disclose accurate election results and provide updates on the progress of the vote counting process and shall not speculate election results but shall broadcast confirmed election results as they are announced and published by presiding officers."**<sup>110</sup>

<sup>105</sup> Zambia Electoral Process Act, Act No. 35 of 2016.

<sup>106</sup> Zambia Electoral Code of Conduct, Statutory Instrument No. 60 of 2016.

<sup>107</sup> Zambia Electoral Code of Conduct, Statutory Instrument No. 60 of 2016, Section 15(1).

<sup>108</sup> South Africa Electoral Act, No. 73 of 1998, Section 87(1)(e).

<sup>109</sup> Zambia Electoral Code of Conduct, Statutory Instrument No. 60 of 2016, Section 7(1).

<sup>110</sup> Zambia Electoral Code of Conduct, Statutory Instrument No. 60 of 2016, Section 9(1).

A similar provision is found in the Lesotho National Assembly Electoral Act,<sup>111</sup> which states:

**“A political party registered with Commission shall have the right to have the substance of its campaign propaganda reported on news broadcasts of the Government-owned media and in any newspaper in circulation in Lesotho.”<sup>112</sup>**

These provisions mandate additional requirements for access to information that could be hindered or prevented by an internet shutdown.

### 7.3 Legislative Protections of Freedom of Expression

Some electoral laws specifically require safeguards that protect freedom of expression and access to information during elections. For example, within the Lesotho National Assembly Electoral Act,<sup>113</sup> section 63 states, “a political party registered with the Commission is entitled to complete and unhindered freedom of expression and information in the exercise of the right to campaign.” These types of provisions can be used to strengthen the standing of political parties that want to bring challenges to internet shutdowns during elections.

<sup>111</sup> Lesotho National Assembly Electoral Act, No. 1 of 2011.

<sup>112</sup> Lesotho National Assembly Electoral Act, No. 1 of 2011, Section 67(1).

<sup>113</sup> Lesotho National Assembly Electoral Act, No. 1 of 2011.

## 8. Constitutional Considerations

Every Constitution in the region includes provisions which protect freedom of expression. These typically also include specific language protecting access to information, sometimes in another section. Even if courts decide that an internet shutdown order is properly authorised under a statute or regulation, challenges to shutdowns should also raise questions of constitutionality. Limitations on freedom of expression and access to information generally follow the limitations as outlined in the section on international human rights. Limitations must be written in law, they must pursue a legitimate purpose, and they must be necessary and proportional to achieving that purpose.

Greater restrictions can be placed on freedom of expression during a national emergency, as declared in terms of the Constitution. National emergencies must be officially declared in order for derogations from rights like freedom of expression and access to information to be lawful. In addition to articles protecting freedom of expression, each Constitution in the region also outlines procedures for the declaration of a national emergency. Should a state defend an internet shutdown by saying that there was a national emergency, litigation should examine whether the procedures for declaring a national emergency were followed.

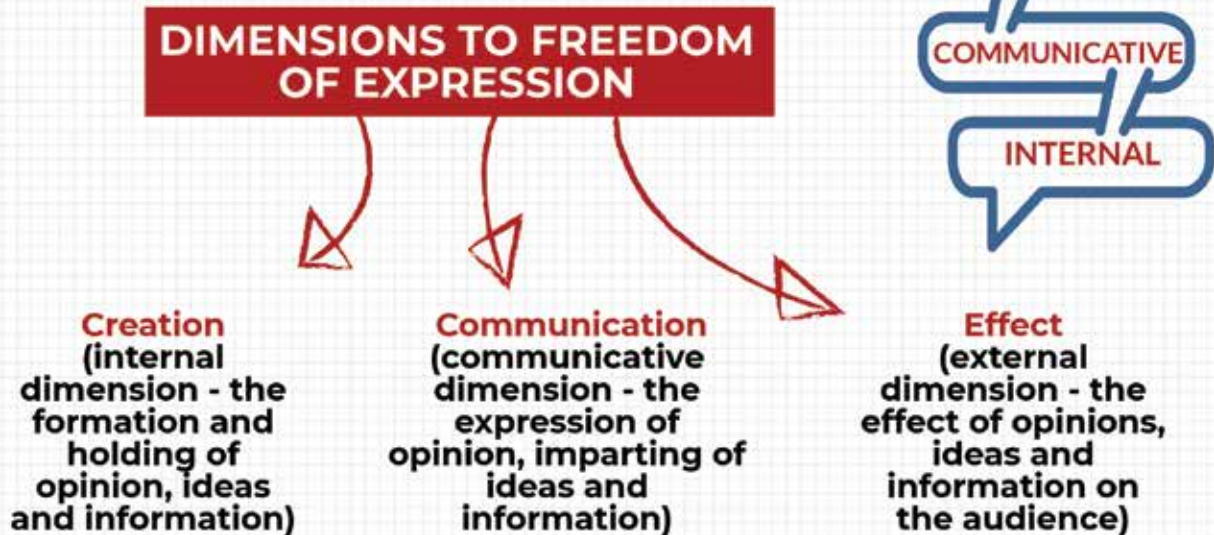
Below is a chart outlining the location of these various provisions within the Constitution of each country in the region. When litigating, reference to the specific language within the Constitution, as well as any country specific case law, should be included.

SOUTHERN AFRICA CONSTITUTIONAL PROVISIONS IMPACTING ORDERS TO SHUT DOWN THE INTERNET				
	FREEDOM OF EXPRESSION	FREEDOM TO ACCESS INFORMATION	RESTRICTIONS ON FUNDAMENTAL RIGHTS	DECLARATION OF NATIONAL EMERGENCIES
Angola	Article 40	Article 40 & 44	Articles 40(3) & 57	Article 58
Botswana	Article 12	Article 12	Article 12(2)	Article 17
DRC	Article 23	Article 24		Articles 61, 85, 119, 144, 145, 148 & 155
Eswatini	Article 24	Article 24	Article 24(3)	Articles 36 & 37
Lesotho	Article 14	Article 14	Article 14(2)	Article 23
Madagascar	Article 10	Article 11	Article 10	Article 61
Malawi	Article 35	Article 37	Article 44	Article 45
Mauritius	Article 12	Article 12	Article 12(2)	Article 18
Mozambique	Article 48	Article 48	Article 56	Articles 72, 161, 166, 179(2)(g), 195(d), 269, & 282-290
Namibia	Article 21(1)(a)		Articles 21(2) & 22	Article 26
South Africa	Article 16	Article 16	Articles 16(2) & 36	Article 37
Tanzania	Article 18	Article 18	Article 30	Articles 31 & 32
Zambia	Article 20	Article 20	Articles 20(3), 11	Articles 30 & 31
Zimbabwe	Article 61	Article 62	Articles 61(5), 62(4), & 86	Article 87

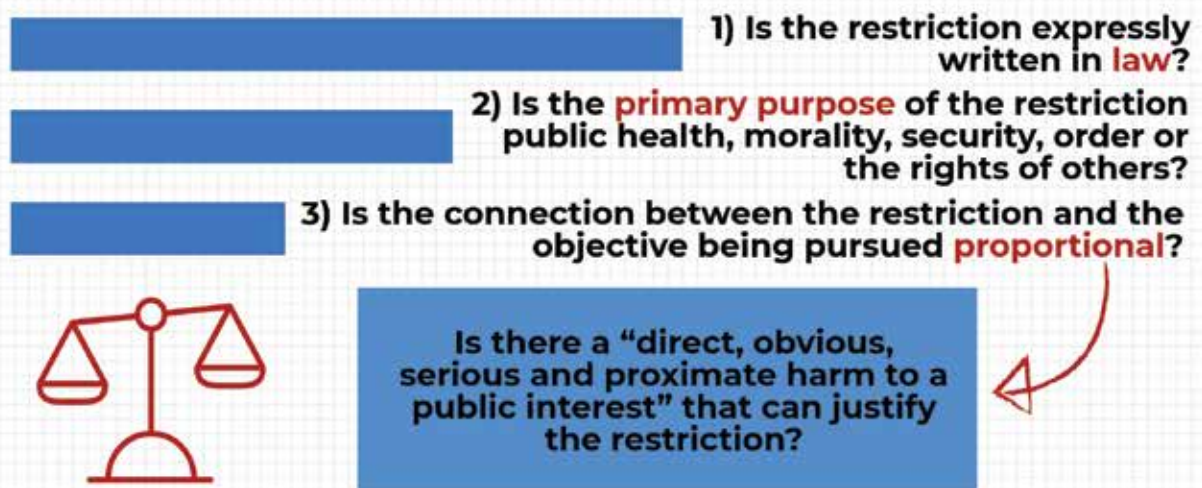


## 8.1 Freedom of Expression Case Studies

**Chavunduka & Another v Minister of Home Affairs & Another, 2000 (1) ZLR 552 (SC)**



## IS THE LIMITATION OF FREEDOM OF EXPRESSION JUSTIFIED?



In 2000, the Constitutional Court of Zimbabwe passed a landmark decision on the right to freedom of expression. In the case, *Chavunduka & Anor v Minister of Home Affairs & Anor (Chavunduka)*,<sup>114</sup> the Court struck down a provision which criminalised lying about the security forces. The Court focused its decision on interpreting section 20(1) of the former Constitution of Zimbabwe, which protected the right to freedom of expression. The text of that section read in part:

<sup>114</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor* 2000(1) ZLR 552(S). Writing for the unanimous court Gubbay CJ at 558C-G.

**“Except with his own consent or by way of parental discipline, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence.”<sup>115</sup>**

While a new Constitution was passed in 2013, it still has protections of freedom of expression. The text in the new Constitution is:

**“Every person has the right to freedom of expression, which includes-- freedom to seek, receive and communicate ideas and other information; freedom of artistic expression and scientific research and creativity; and academic freedom”.<sup>116</sup>**

In the 2013 Constitution, there are also specific protections for freedom of thought, conscience and opinion.<sup>117</sup> Importantly, the new Constitution reaffirms Zimbabwe's, “commitment to upholding and defending fundamental human rights and freedoms.”<sup>118</sup> Therefore, the interpretation of freedom of expression in Zimbabwe is still strongly informed by *Chavunduka*.

In *Chavunduka*, the Court noted that freedom of expression, “is to be given a benevolent and purposive interpretation.”<sup>119</sup> The Court goes on to state that freedom of expression has four broad special objectives to serve:

**“(i) it helps an individual to obtain self-fulfillment;  
(ii) it assists in the discovery of truth, and in promoting political and social participation;  
(iii) it strengthens the capacity of an individual to participate in decision-making; and,  
(iv) it provides a mechanism by which it would be possible to establish a reasonable balance between stability and social change.”<sup>120</sup>**

The Court goes on to say that limitations on the right are only enforceable “when the activity or expression poses danger of direct, obvious and serious harm to the rights of others or the public interests listed in... the Constitution.”<sup>121</sup> The prior Constitution delineated the permissible limitations to the freedom of expression in section 20(2),<sup>122</sup> under the current Constitution permissible limitation are outlined in section 86:

<sup>115</sup> Constitution of Zimbabwe, last amended 2005, Article 20(1) repealed.

<sup>116</sup> Constitution of Zimbabwe, Section 61.

<sup>117</sup> Constitution of Zimbabwe, Section 60.

<sup>118</sup> Constitution of Zimbabwe, Preamble.

<sup>119</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor* 2000(1) ZLR 552(S). Writing for the unanimous court Gubbay CJ at 558C-G.

<sup>120</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*.

<sup>121</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*.

<sup>122</sup> Constitution of Zimbabwe, last amended 2005, Article 20(2) *repealed*: “Nothing contained in or done under the authority of any law shall be held to be in contravention of subsection (1) to the extent that the law in question makes provision—

(a) in the interests of defence, public safety, public order, the economic interests of the State, public morality or public health;  
(b) for the purpose of—  
(i) protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings;  
(ii) preventing the disclosure of information received in confidence;  
(iii) maintaining the authority and independence of the courts or tribunals or the Senate or the House of Assembly;  
(iv) regulating the technical administration, technical operation or general efficiency of telephony, telegraphy, posts, wireless broadcasting or television or creating or regulating any monopoly in these fields;  
(v) in the case of correspondence, preventing the unlawful dispatch therewith of other matter; or  
(c) that imposes restrictions upon public officers; except so far as that provision or, as the case may be, the thing done under the authority thereof is shown not to be reasonably justifiable in a democratic society.

**“The fundamental rights and freedoms set out in this Chapter may be limited only in terms of a law of general application and to the extent that the limitation is fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom, taking into account all relevant factors, including—**

- a. The nature of the right or freedom concerned;**
- b. The purpose of the limitation, in particular whether it is necessary in the interests of defence, public safety, public order, public morality, public health, regional or town planning or the general public interest;**
- c. The nature and extent of the limitation;**
- d. The need to ensure that the enjoyment of rights and freedoms by any person does not prejudice the rights and freedoms of others;**
- e. The relationship between the limitation and its purpose, in particular whether it imposes greater restrictions on the right or freedom concerned than are necessary to achieve its purpose; and**
- f. Whether there are any less restrictive means of achieving the purpose of the limitation.”<sup>123</sup>**

The Court explained this as:

**“The only limitation on the ‘freedom’ or ‘liberty’ is the duty not to injure the rights of others or the collective interests listed in...the Constitution. In other words the State through the exercise of legislative power may limit the individual’s exercise of the right to freedom of expression if that were necessary for the protection of one or more of the public interests listed in...the Constitution.”<sup>124</sup>**

The Court helpfully outlines the test for whether or not the restriction on freedom of expression is constitutionally justified as:

**“(1) Is the restriction on the exercise of the right to freedom of expression imposed under s 31(a) (iii) of the Criminal Code contained in law.**

**(2) If the restriction is contained in law does the provision have as its primary objective the protection of a public interest in one or more of the matters listed in... the Constitution.**

**(3) If the protection of a public interest listed in...the Constitution is the primary purpose of the legislation, is there a rational connection between the restriction on the exercise of the right to freedom of expression and the objective pursued.”<sup>125</sup>**

The Court goes on to say that these limitations involve a “strict requirement”, and “[t]he exercise of the power to limit the exercise of the right to freedom of expression is not only required to be constitutionally justified. It is itself restricted by the principle of proportionality.” Or in other words, to what degree does the state action

<sup>123</sup> Constitution of Zimbabwe, Section 86(2).

<sup>124</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*.

<sup>125</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*.

interfere with the right to freedom of expression?<sup>126</sup> To answer this question, the Court looks to the purpose and effect of a legislation.<sup>127</sup> The purpose of the proportionality test is “to strike a balance between the interests of the public and the rights of the individual in the exercise of freedom of expression”.<sup>128</sup> The proportionality tests asks whether there is a, “direct, obvious, serious and proximate harm to a public interest...Not every case of actual or potential harm on the public interests listed in...the Constitution justifies the imposition of restrictions on the exercise of freedom of expression”. Furthermore, “[t]he exercise of the right to freedom of expression is not protected because it is harmless. It is protected despite the harm it may cause.”<sup>129</sup>

The Court points specifically to the interplay between freedom of expression and the maintenance of public order, explaining that freedom of expression must work in tangent with maintenance of public order.<sup>130</sup> However, the Court explicitly warns:

**“A law cannot be used to restrict the exercise of freedom of expression under the guise of protecting public order when what is protected is not public order. This is because the maintenance of public order or preservation of public safety is synonymous with the protection of fundamental human rights and freedoms. The State cannot therefore violate fundamental human rights and freedoms under the cover of maintaining public order or preserving public safety. It is always important to understand and appreciate the meaning of the concepts of public order and public safety. They describe the definitional balancing line between the exercise of the right to freedom of expression and the public interests for the protection of which the State may restrict the exercise of that right.”<sup>131</sup>**

<sup>126</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*, “The first thing the Constitution controls in the exercise by the Government of the power to hinder the enjoyment of freedom of expression under the strict justificatory requirements of s 20(2) is the degree of interference. The interference imposed in terms of the impugned law must be limited to being a restriction or hindrance of the enjoyment of the exercise of the right to freedom of expression. There must be a limitation of acts by which the right to freedom of expression is exercised.”

<sup>127</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*, “In deciding whether a measure imposes restrictions to the exercise of freedom of expression the court examines its purpose or effect.”

<sup>128</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*. The court goes on to outline three helpful questions that the court can apply when determining the question of proportionality: “The applicants must establish the following facts arising from the application of the three criteria of the proportionality test:

- (a) That there is no rational connection between the restriction on the exercise of the right to freedom of expression and the objective sought to be achieved by the provisions of the statute.
- (b) That even if there is a rational connection between the restriction on the exercise of freedom of expression and the objective pursued the means used to effect the connection do not impair the right to freedom of expression as little as possible. That would mean that there are other less intrusive means available which the legislature could have used to restrict the exercise of the right to freedom of expression to achieve the same objective.
- (c) That the effects of the restrictive measure so severely trench on the right to freedom of expression that the legislative objective sought to be achieved is outweighed by the restriction on freedom of expression.

The criterion of the proportionality test applicable will vary depending on the circumstances of each case.”

<sup>129</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*.

<sup>130</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*, “A valid legislative restriction of the exercise of the right to freedom of expression should be as limited as the scope of the meaning of the public interest for the protection of which it is imposed. While it is intended that there should be freedom of expression it is also intended that in the exercise of the right, conditions should not be deliberately created for the undermining of the maintenance of the public order or preservation of public safety. There is a direct and vital relationship between the exercise of freedom of expression and the preservation of public peace and tranquility.”

<sup>131</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*.

The Court also stresses the importance of a free media, and the press' ability to exercise freedom of expression, especially highlighting their role to play when government and security forces act illegally.<sup>132</sup> A shutdown of the internet prohibits the press and media from exercising this essential task.

The justification for the restriction to a law must be contained within the law that restricts the right.<sup>133</sup> On this requirement alone, an internet shutdown cannot be justified using the Interception of Communications Act. While the Act sets out justifications for restricting privacy,<sup>134</sup> there are no justifications for interrupting freedom of expression. It is impermissibly broad.<sup>135</sup> As the Court stated:

**"It is easy for Government to place a restriction of the exercise of a fundamental right within the requirement for adoption of a legitimate objective. It is for the court to ensure that the law was conceived and expressed solely to achieve that objective. The law should not in its design have the effect of overreaching and restricting expression which is not necessary for the achievement of the objective concerned. The court applies the principle of proportionality to test the relationship between the restriction to the exercise of the right to freedom of expression and the objective pursued. The question is whether the restriction is necessary and proportionate to the objective pursued. Any restriction to the exercise of the right to freedom of expression claiming to be for the protection of any of the public interests listed in s 20(2)(a) of the Constitution must meet strict requirements indicating its necessity and proportionality."**<sup>136</sup>

Furthermore, to legally shutdown the internet, the government of Zimbabwe would need to rely on some sort of legal restriction to freedom of expression. This restriction would need to pass all of the tests laid out in *Chavunduka*. Namely, is the restriction set out in law, in a way that clearly references and actually relies on one of the permissible justifications for restrictions laid out in Section 86 of the Constitution? If there is such legislation, is the harm of restricting freedom of expression proportional to the threat to public order or security.

## 8.2 Constitutional Limitations on Telecommunications Regulations

In *Alick Kimu v Access Malawi Limited and Others*,<sup>137</sup> the plaintiff sued four telecommunication providers in Malawi for violating the terms of the service contract and constitutional rights. The providers were issued a directive by the Malawi Communications Regulatory Authority (MACRA) to provide call detail records (CDR), which "includes information about who called which number; details of calls received; time and duration of calls; location where call was made or received; SMS sent and received; type of handset used and other detailed subscriber

<sup>132</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*, "It is the duty of a free media of communication to give accurate information to the public on unlawful activities of members of a security service institution. It is in the public interest that the media should be free to provide criticism of such conduct. Indeed a democracy cannot exist without that freedom to put forward opinions about the functioning of public institutions...The concept of free and uninhibited expression and dissemination of opinion about the functioning of public institutions permeates all free and democratic societies. Not only does the media have the duty to impart such ideas and information concerning the activities of security service institutions relating to securing of the maintenance of public order or the preservation of public safety, the public have a right to receive the ideas and information."

<sup>133</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*, "It is a fundamental principle of constitutional law that any restriction which hinders the enjoyment of a fundamental right must be introduced by a legal provision. The grounds for the justification of the restriction must be found in the law by which it is imposed."

<sup>134</sup> See Interception of Communication Act, Cap. 11:20, Sections 6(1)(b) and (6)(1)(c).

<sup>135</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*, "...if arbitrary and discriminatory enforcement is to be preventable laws must provide explicit standards for those who apply them. The discretion of those entrusted with law enforcement should be limited by clear and explicit legislative standards."

<sup>136</sup> *Chavunduka & Anor v Minister of Home Affairs & Anor*.

<sup>137</sup> *Kimu v Access Malawi Limited & Others* (Commercial Case No. 54 of 2011) MWWCommC 1 (02 May 2012).



information.”<sup>138</sup> The service providers thought that this directive violated the right to privacy as protected under the Malawi Constitution, but in the end acquiesced with the request. They sent a letter to their subscribers stating that they would:

**“no longer be in a position to safeguard the privacy and confidentiality of customers’ communication activities, as we understand it to be our obligation under our respective operating licenses, subscriber contracts, the Communications Act[1998] and the Constitution of the Republic of Malawi”.**<sup>139</sup>

Following receipt of the communication, the plaintiff sued.

The Court found that providing the information violated the right to privacy as protected in the Constitution. In reaching this conclusion, they agreed that the constitutional right to privacy can only be limited:

**“if the limitation is prescribed by law, is reasonable, is recognized by international human rights standard and is necessary in [an] open and democratic society.”**<sup>140</sup>

In applying the standard, the Court focused on the broad nature of the order. The Court states:

**“If as seems to be suggested by the confidentiality clauses the issue is about national security, the need to repair or maintain the network or law enforcement we do not think that the way forward is a blanket directive that lays bare every subscriber’s call records. It is to deal with each instance on a case by case basis...Allowing blanket access appears to us to therefore not only to be unnecessary in the circumstances but to be in breach of the proportionality test as well. It would allow access to even those persons that are clearly not in conflict with the law.”**

The Court rightly recognised that limitations to fundamental rights, such as privacy, need to be narrowly tailored to the government interest trying to be protected. While the right at question in this case was the right to privacy, the same standard applies to freedom of expression. Just like a blanket request for information violates the right to privacy of citizens who have broken no law, a total shutdown of the internet also violates the right to freedom of expression, especially of those citizens who have not broken the law.

In applying this test, the Court also made it clear that “a limitation does not become legal merely because it came from MACRA indeed any regulator”.<sup>141</sup> That is to say that an unlawful order from the government cannot be a defence for private corporations who implement the order and end up violating the rights of their consumers.

This point was emphasised by the Court when determining costs. The Court ordered costs against the four defendants. In doing so it stated, “If [the defendants] were put in this situation by MACRA and wanted a way out what stopped them from approaching the courts and seeking directions on the way forward. It would then be understood if they asked that MACRA pays the costs or that each party pays its own way. In the instant case they let the defendant literally drag them to court. They should pay the plaintiff having succeeded.”<sup>142</sup>

Private corporations who hold telecommunication licenses have an obligation to provide the services that are authorised by the license in conformity with the law and constitution. If the corporation feels that they have

<sup>138</sup> *Kimu v Access Malawi Limited & Others* (Commercial Case No. 54 of 2011) MWCommC 1 (02 May 2012).

<sup>139</sup> *Kimu v Access Malawi Limited & Others* (Commercial Case No. 54 of 2011) MWCommC 1 (02 May 2012).

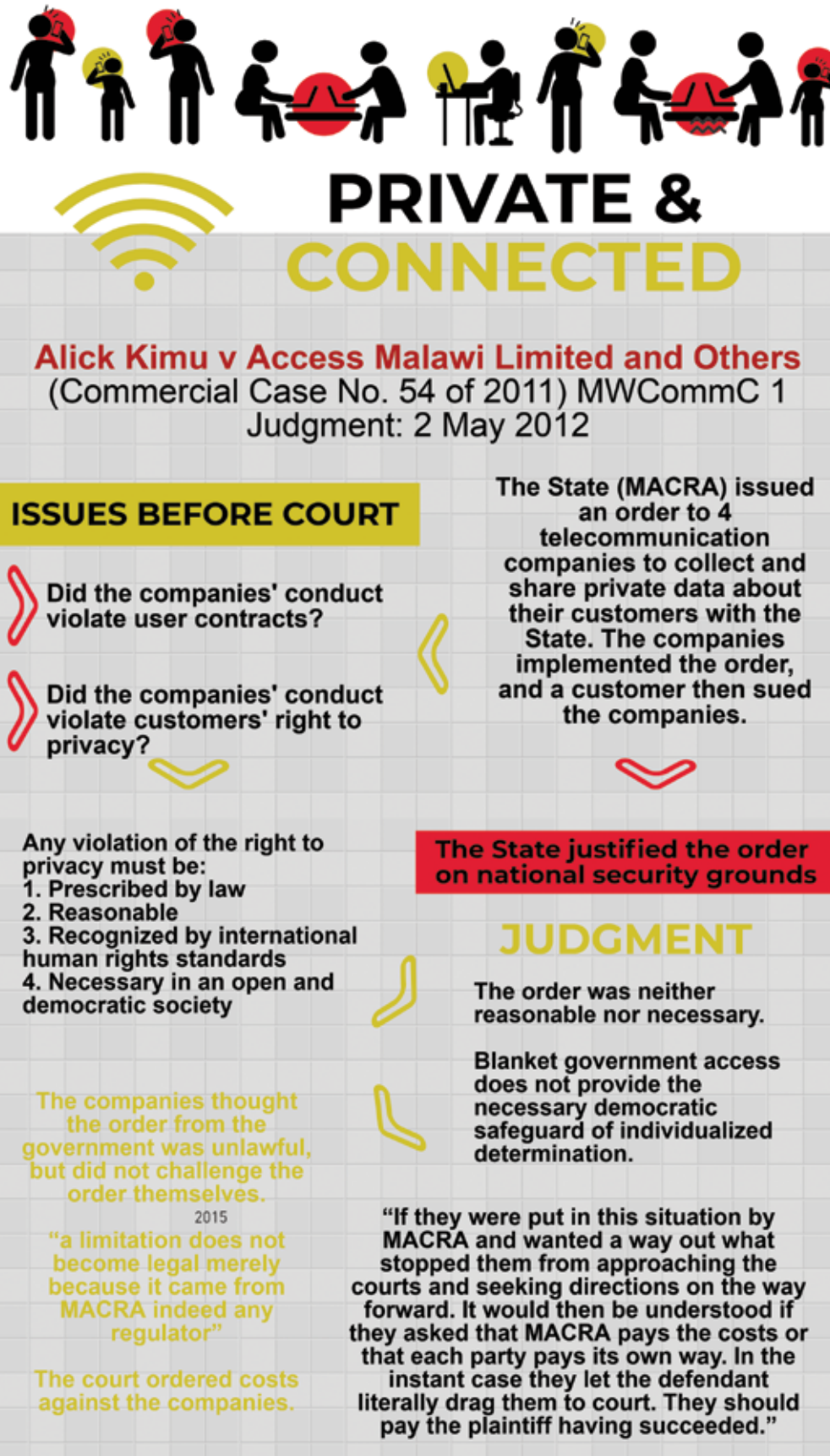
<sup>140</sup> *Kimu v Access Malawi Limited & Others* (Commercial Case No. 54 of 2011) MWCommC 1 (02 May 2012).

<sup>141</sup> *Kimu v Access Malawi Limited & Others* (Commercial Case No. 54 of 2011) MWCommC 1 (02 May 2012).

<sup>142</sup> *Kimu v Access Malawi Limited & Others* (Commercial Case No. 54 of 2011) MWCommC 1 (02 May 2012).



been given an unlawful order by the government, they have a responsibility to challenge that order in court. They cannot be allowed to unlawfully restrict the rights of their customers. If they do this, they are liable in court for the costs to the consumers.



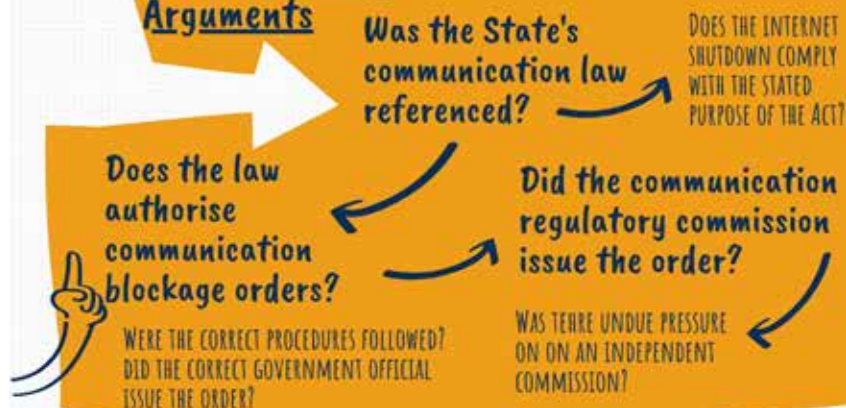
## 9. Thinking Through Litigation Strategy





## Possible Arguments in Litigation on Internet Shutdown?

### Main Statutory Arguments



### Constitutional Arguments

#### Rights violated?

FREEDOM OF EXPRESSION  
ACCESS TO INFORMATION  
OTHERS?

Valid limitation of rights?

Was it written law?  
Was stated justification permissible?  
Was restriction necessary  
proportionality?

Declared State of Emergency?

Does election law have heightened protection for expression in elections?

DID BLOCKAGE RESTRICT REPORTING?  
CRIMINAL PENALTIES FOR INTERFERING IN REPORTING?

Did shutdown occur during elections?

Does the election law have reporting requirements during elections?

### More Statutory Arguments

Does communication law forbid unlawful interruption of communications?

DID ISP LICENCE HOLDER OR GOVERNMENT CONTRAVENE THIS PROVISION?

Was there a warrant or interception order issued?

Does the interception act authorise order for communication blockage?  
Procedures followed?  
Legal threshold for warrant or order?

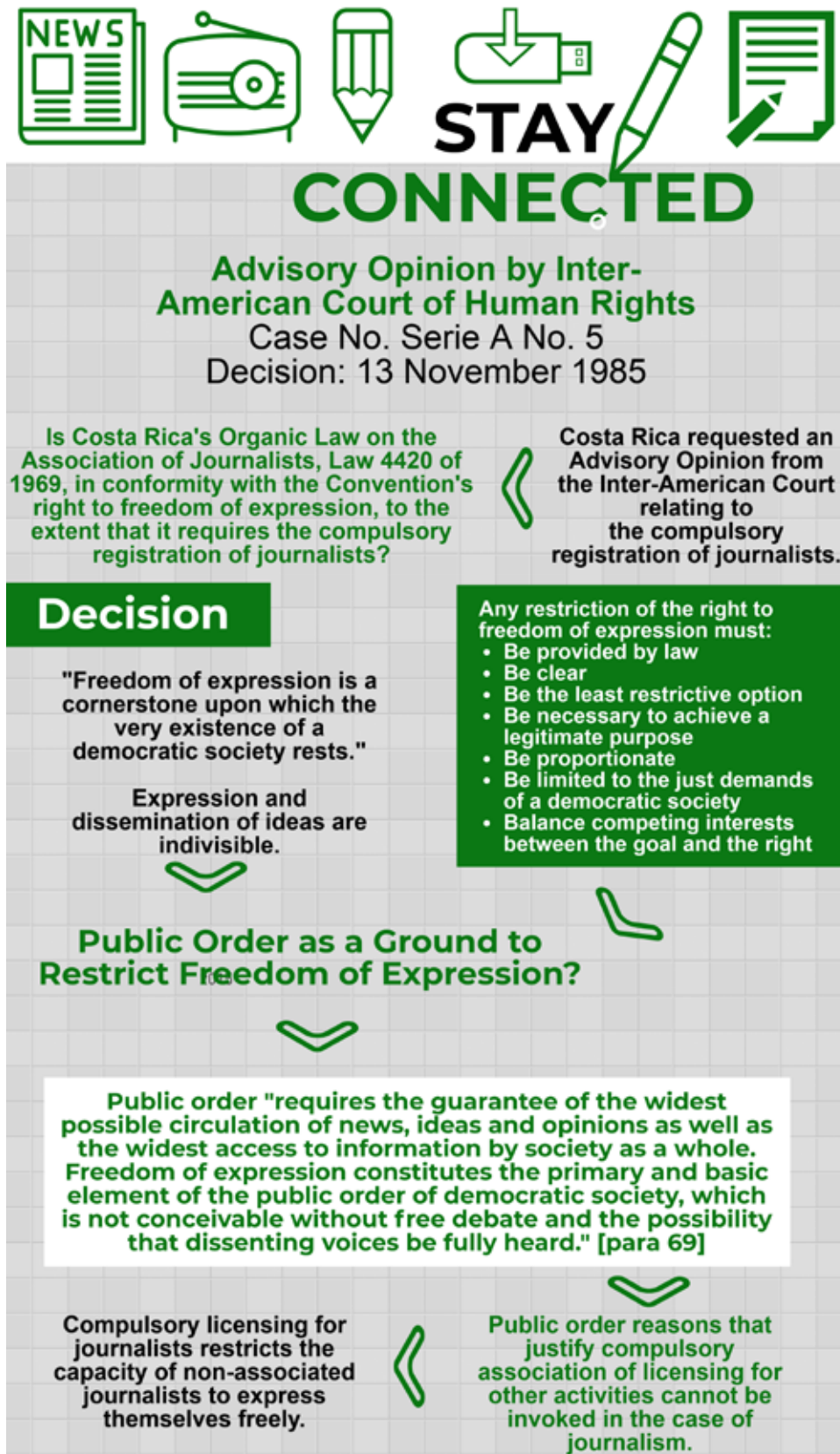
## 10. Conclusion

With the rise of internet shutdowns, litigation should be viewed as a strategy to combat the shutdowns, protect peoples' rights and restore the rule of law. The regulatory frameworks for the majority of Southern African countries do not provide any authority for government orders for internet shutdowns. Despite the lack of express authorisation, governments have been giving these orders. This is both disruptive to industry and society, as well as the principle of rule of law.

Furthermore, even countries like the Democratic Republic of Congo which have authorisations for service disruption written into their law should recognise that a consensus of the international and regional community have recognised that government ordered shutdowns infringe on the rights to freedom expression, freedom to access information, and a multitude of other rights. These provisions violate the freedom of expression as protected within the Constitution and cannot be justified in a free democratic society.

Lawyers and advocates within the region should build strategies which allow for a fast response to future internet shutdowns. These responses should highlight the rights violations of every day citizens as well as respond to the illegal basis of the internet shutdown.

# Annex I – Global Case Studies on Freedom of Expression and Technology







## STAY CONNECTED

**CM Pak v Pakistan Telecommunications Authority**  
FAO 42/2016, Islamabad High Court, Pakistan  
Judgment: 26 February 2018

Challenge by mobile cellular service providers and customers to directive by Authority to shutdown services on the instruction of government



### ISSUE BEFORE COURT

Scope of powers of government or Authority to direct licensed service providers to suspend operations

### ARGUMENTS OF PETITIONERS

- The Authority is under a statutory obligation to ensure licensees get reasonable and expected return
- If services are suspended, the government must compensate licensees
- The practice of the Authority to direct mobile cellular operators to suspend operations without notice is unlawful
- Services can only be discontinued under specific circumstances specified in Act
- There are no provisions in law empowering the Authority to suspend services

### ARGUMENTS OF GOVERNMENT

- Government can issue directives to the Authority if it has national concerns
- Only government can decide if defence or security concerns require a policy directive
- The Authority is under an obligation to then issue directive to licensees to suspend services

### JUDGMENT

**Key wording in the Act:** The Authority can only act within the limits of the Act - thus can only suspend services in terms of the Act

Interception of specific calls/ messages by government if offence committed - **this provision does not entitle government to suspend services on national security grounds**

Government to be given preference in telecommunication systems over licensees - **this provision only applies where a national emergency was declared in terms of the Constitution**

No authority is vested with the power to suspend services of service providers and deprive customers of those facilities

**Declared actions of government/Authority inconsistent with Act and thus illegal, ultra vires, without lawful authority or jurisdiction**





## STAY CONNECTED

**Valdelomar & Sibaja v Costa Rican Superintendence of Telecommunications**  
Case No. 17-191-7-CO  
Constitutional Chamber of the Supreme Court, Costa Rica  
Judgment: 14 July 2017

**ISSUE BEFORE COURT**

Constitutional challenge by 3 individuals against the fair use policy which limited mobile internet speeds and the speed of online browsing.

The constitutionality of creating fair use policies restricting internet speeds and affecting internet access.

**ARGUMENTS**

**Applicants:** Telecommunications law prohibited ISPs from imposing policies that discriminated between different users' internet access.

**State Telecommunications Authority:** All users of mobile internet services shared a single infrastructure. Heavy internet users strained this shared network, limiting internet access for others.

Fair use policy permitted companies to lower or restrict internet speeds for users who expended contracted internet allowance or data packages. The fair use policy is necessary to protect the right to internet access of everyone.

**JUDGMENT**

Internet access has become an essential element of the modern society and is a tool that enhances access to other rights.

Internet access is a fundamental right.

A restriction on internet access could affect the right to freedom of expression.

The State is obliged to promote democratisation of internet access by trying to reduce the digital divide.

The State has an obligation to protect and expand internet access.

The State must protect individuals from threats that unjustly limit internet access.

The State must adopt new technologies to improve internet access.

The State must ensure internet access is expanded and improved.

The State telecommunications authority has an obligation to ensure that individuals at a minimum had guaranteed access to the internet.

The State must regularly update the minimum speed as digital technology evolves.

The State telecommunications authority and not ISPs must determine the minimum functioning internet browsing speed.

Fair use policy must be applied in accordance with the principles of necessity, reasonableness and proportionality.

Restricting internet speeds under the existing fair use policy was not justified when internet networks were not stressed or experiencing heavy traffic.



## Media Council of Tanzania and Others v Tanzania

Ref. No. 2 of 2017, East African Court of Justice  
Judgment: 28 March 2019

The Court declared various sections of the Media Services Act No. 120 of 2016 contrary to the provisions on the Treaty for the Establishment of the East African Community. The Court ordered Tanzania to bring the provisions of the Act in line with the Treaty.

### Judgment

"Free press goes hand in hand with the principles of accountability and transparency..."

Section 7 of the Act provided for a range of instances in which a media house had an obligation to ensure that information was not issued.

The Court held that a number of these provisions were vague, unclear and imprecise and accordingly did not pass the first test of being provided in law:

- "undermine", "impede", "hate speech", "unwarranted invasion", "infringe lawful commercial interests", "hinder or cause substantial harm", "significantly undermines", "damage the information holders position".

"Principles of democracy must of necessity include adherence to press freedom"

**Criminal defamation:**  
The Court held that the definition of defamation "is not sufficiently precise to enable a journalist or other person to plan their actions within the law. The definition makes the offence continuously elusive by reason of subjectivity." [para 87]

**Minister allowed to prohibit importation of a publication if of opinion it would be contrary to public interest:**  
The Court held that the lack of clarity on the circumstances in which Minister would impose a prohibition makes the provisions objectionable relative to the rights being restricted. [para 110]

**Accreditation of journalists:**  
The Court held that the definition of journalist in the Act is too broad "to provide sufficient provision to allow an individual to foresee what activities they are forbidden from performing without accreditation." [para 79]

**Statements threatening to interest of defence, public safety, public order, economic interests:**  
The Court held that this provision is too broad and imprecise.

**Seditious intention:**  
The Court held that this provision is "hinged on the possible and potential subjective reactions of audiences to whom the publication is made. This makes it all but impossible, for a journalist or other individual, to predict and thus, plan their actions." [para 99]

**Statements known to be false:**  
The Court held that this provision is too vague.





## Esquivel v Instituto Costarricense de Electricidad Costa Rica Supreme Court, 17 January 2014

The applicant brought a case against the State company which provides electricity and telecommunications.

The applicant's residential area did not receive internet and cell phone services.

Applicant alleged that the community was denied the right to use telecommunication services.

### JUDGMENT


The principle of universality must be applied to telecommunication services and means that there must be a sufficient investment in infrastructure that provides these services in order for them to reach peripheral areas.

### ISSUE

Is there an obligation on the State to make sure that the internet and other telecommunication services are provided?

The cost for this type of investment cannot be a motive to restrain the development of this kind of public service, since any service must be planned to ensure the enrichment of quality of life of the entire population.





# STAY CONNECTED

**Summary Proceeding 1/2017**  
Mexico Supreme Court


The company Alestra filed an application against the Mexican Institute for Industrial Property, which had blocked access to a music web page on the basis that its content constituted an infraction of authors' rights.

There was no law which allowed the suspension.


## JUDGMENT

Freedom of Expression on the Internet can only be limited as provided in law, for a legitimate purpose which is necessary and proportionate.


Any restriction of the right to freedom of expression may not be too wide or generic - the Institute could not suspend the website in its entirety since that was too broad.








## STAY CONNECTED



**Singhal v Union of India**  
Writ Petition No. 167 of 2012, India  
Judgment: 24 March 2015


2 women charged under section 66 of the Information and Technology Act for publishing allegedly offensive and objectionable comments on Facebook. The women filed a petition challenging the constitutionality of section 66A.



**Section 66A of Information and Technology Act:**  
Punishes any person who sends through a computer resource or communication device any information that is grossly offensive, or with the knowledge of its falsity, the information is transmitted for the purpose of causing annoyance, injury, inconvenience, hatred or ill will.

### INTERIM ORDER

Prohibit any arrest pursuant to section 66A unless such arrest is approved by senior police officers.



### FINAL ORDER

Declared section 66A unconstitutional on substantive grounds for violating the right to freedom of expression. Also declared section 118(d) of the Kerala Police Act unconstitutional as applied to section 66A.

### JUDGMENT

"Mere discussion or even advocacy of a particular cause howsoever unpopular is at the heart" of the right to freedom of expression (para 13).


Section 66A is capable of limiting all forms of internet communications as it makes no distinction "between mere discussion or advocacy of a particular point of view, which may be annoying or inconvenient or grossly offensive to some and incitement by which such words lead to an imminent causal connection with public disorder, security of State etc" (para 20).

The offence did not provide clear guidelines on what is prohibited and was struck down for being vague, unreasonable and arbitrary.

By failing to define terms such as annoyance and inconvenience, the offence curtailed protected and innocent speech.

#### POST-JUDGMENT

In February 2019, 4 years after the judgment, the Supreme Court was presented with an application based on the fact that section 66A was still enforced by police and courts despite the judgment. The Supreme Court granted an order that copies of the judgment be issued through appropriate circulars to the Chief Secretaries of all States, the Directors General of Police, and all District Courts.



## Annex II – Major Internet Providers in Southern Africa

### ANGOLA

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Angola Telecom	Rua das Quipacas, 186, 3rd Floor, Luanda	222 700 000	info@angolatelecom.ao	<a href="http://www.angolatelecom.ao/">http://www.angolatelecom.ao/</a>	Adilson dos Santos	/	State-Owned
Unitel	Unitel Talatona Building, Sector Talatona, Via CS3 Luanda South, Samba	+244 923 199 100	support.client@unitel.co.ao	<a href="http://www.unitel.ao/servlet/web/Particulares">http://www.unitel.ao/servlet/web/Particulares</a>	Tony Dolton	/	Various
Movicel	Luanda	+244 2226 92 000	support1919@movicel.co.ao	<a href="https://www.movicel.co.ao/">https://www.movicel.co.ao/</a>	Gianvittorio Maselli	/	Various, including Angola Telecom
Internet Technologies Angola (ITA)	Rua 29 - EPAL 3o Patriota - Benfica Caixa	+244 225 286 000	info@ita.co.ao	<a href="https://ita.co.ao/en/">https://ita.co.ao/en/</a>	Rolf Mendelsohn	/	/
Multitel	Largo Ingombotas Ingombotas Building, 1º andar - Luanda	222 704 200	secretaria@multitel.co.ao	<a href="http://multitel.co.ao/PT">http://multitel.co.ao/PT</a>	Antonio Geirinhas	/	Various, including Angola Telecom



## BOTSWANA

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL / CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Botswana Telecommunications Corporation (BTC)	Khama Crescent, Plot 50350, Megaleng P O Box 700 Gaborone.	+267 395 8000	customer@btsnet.bw	<a href="http://www.btc.bw/">http://www.btc.bw/</a>	Anthony Msunga (Managing Director)	Sydney Mganga	State-owned
MASCOM	Tsholetsa House Plot 4705/6 Botswana Road Main Mall	+267 71 696 964	customerservice@mascom.bw	<a href="https://www.mascom.bw/">https://www.mascom.bw/</a>	Jose Vieira Couceiro	/	Econet Wireless Global Ltd (South Africa)
Orange Botswana	Pilane Rd, Gaborone.	+267 369 3000	customerservice@orange.com	<a href="http://www.orange.co.bw/">http://www.orange.co.bw/</a> (not working at time of recording)	Patrick Benon	/	Orange S.A. (France)
Cene Media	Acacia House Plot 74358, New CBD, Gaborone.	+267 395 6992	sales@cenemedia.com	<a href="http://www.cenemedia.com/">http://www.cenemedia.com/</a>	Mark Sprey (Managing Director)	/	ConceroTel (HQ in Australia)

## THE DEMOCRATIC REPUBLIC OF CONGO

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Airtel DRC	Immeuble 5 a Sec, Combe, Kinshasa	+24399 600 0121	info.airtelrdr@ cd.airtel.com	<a href="https://www.airtel.cd/">https://www. airtel.cd/</a>	Emmanuel Hamez (Managing Director)	/	Bharti Airtel (India)
Vodacom DRC	Vodacom House, 292 Justice Street, Combe, Kinshasa	+243813131000	vodacom@ vodacom.cd	<a href="https://www.vodacom.cd/particulier/homepage">https://www. vodacom.cd/ particulier/ homepage</a>	/	/	Vodacom Group (South Africa)
Orange RDC	Ave Colonel Mondjiba, Kinshasa	+243 892 222 202	info@orange.cd	<a href="http://www.orange.cd/">http://www. orange.cd/</a>	Gerard Lokossou	/	Orange S.A. (France)
Africell DRC	25 Avenue de la Justice, Red Cross district, Gombe commune.	(+243) 900,000,000	info@africell.cd	<a href="https://www.africell.cd/">https://www. africell.cd/</a>	Milad Khairallah	/	Africell

## ESWATINI

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Eswatini Posts and Telecommunications	Phutfumani Building, Mahlokohla Street, Mbabane	(00268) 2405 2000	info@EPTC.co.sz	<a href="http://www.sptc.co.sz/home.php">http://www.sptc.co.sz/home.php</a>	Petros Dlamini (Managing Director)	/	State-owned
MTN Swaziland	Mahlalekukhwini House Portion 14 of Farm 50 Cnr MR103 & Nshakabili Road Ezulwini	+268 2406 0000	feedback.sz@mtn.com	<a href="https://www.mtn.co.sz/Pages/Home.aspx">https://www.mtn.co.sz/Pages/Home.aspx</a>	Sibusiso Nhleko (acting CEO)	/	MTN Group (South Africa)
Eswatini Mobile	P.O. Box 2150 Mbabane 1st Floor, Plot No 15, Corner Gwamile & Mdada Street, Mbabane	340110000	info@swazimobile.com	<a href="https://www.swazimobile.com/">https://www.swazimobile.com/</a>	Jeff Pemberton	/	/

## LESOTHO

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL / CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Vodacom Lesotho	VODACOM PARK, 585 MABILE ROAD, Maseru 100, Lesotho	+266 5221 2000	customer@vodacom.co.ls	<a href="https://www.vodacom.co.ls">https://www.vodacom.co.ls</a>	Rishaab Tayob (MD)	/	Vodacom Group (South Africa)
Econet Telecom Lesotho	Kingsway Road Next to Lancers Inn	+266 2221 1000	/	<a href="https://www.eti.co.ls/">https://www.eti.co.ls/</a>	Dennis Plaatjies	Nthabiseng Motjolepane	Econet Wireless Global Ltd (South Africa)
Leo	4, Bowker Rd, Maseru. PO Box 11702, Maseru 100.	22215000	support@leo.co.ls	<a href="http://www.leo.co.ls/">http://www.leo.co.ls/</a>	/	/	/

## MALAWI

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL /CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
MTL (Malawi Telecom. Limited)	Lamya House Masauko Chipembere Highway P.O. Box 537 Blantyre	+265 1 846 977	info@mtl.mw	www.mtl.mw	Harry Gombachika	/	State-owned
Airtel Malawi	Lilongwe Corporate Suite Airtel Complex City Centre Behind Bisnowaty P.O. Box 57 Lilongwe, Malawi	+265 1 774 800	/	www.africa. airtel.com/ malawi	Charles Kamoto (Managing Director)	Hlupikire Chalamba	Bharti Airtel (India)
SDNP	The Malawi SDNP Coordinator P.O. Box 31762 Blantyre 3, Malawi	+265 1 874 979	mwsdnp@sdnp. org.mw	www.sdnp. org.mw	/	/	/
Telekom Networks Malawi (TNM)	P.O. Box 3039 Blantyre, Malawi	+265 888 800 900	customer@care@ tnm.co.mw	www.tnm. co.mw	Eric Valentine (acting)	Christina Mwansa (Managing Exec, legal)	Various, including MTL

## MOZAMBIQUE

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Tmcel – Mozambique Telecom (Merged TDM and mCel)	Rua Belmiro Obadias Muianga, Nº 384 CP 1483 - Maputo	258 21 351100	corporate@tmcel.mz	<a href="http://www.tdm.mz/">http://www.tdm.mz/</a>	Mohamed Jusob	/	State-Owned
Movitel SA	Av. Guerra Popular, 1086 Maputo.	86 086 0860	social.media@movitel.co.mz	<a href="https://www.movitel.co.mz/">https://www.movitel.co.mz/</a>	Safura da Conceição (Chairperson of Board)	/	Viettel (Vietnam)
Vodacom Mozambique	No. 649 Rua dos Desportistas, Maputo	+258 84 111	/	<a href="http://www.vtm.co.mz">www.vtm.co.mz</a>	Jerry Mobbs	/	Vodacom International Ltd



## NAMIBIA

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
MTC Namibia	Windhoek, Namibia	+264 61 280 2000	info@mtc.com.na	http://www.mtc.com.na	Thinus Smit (Acting CEO)	Patience Kanalelo	Namibia Post and Telecommunications Holding (State is majority shareholder)
Telecom Namibia	Corner of Luderitz and Daniel Munamava Street Windhoek P. O Box 297	+264 (0) 61 201 9211	customer@telecom.na	https://www.telecom.na/	Theodorus Klein	Jinah Buys	Namibia Post and Telecommunications Holding (100% State-owned)
Africa Online Namibia	161 Nelson Mandela Ave, Windhoek, Namibia	061 291 1019	info@africaonline.com.na	http://www.africaonline.com.na/	Marc Gregan (Managing Director)	/	Gondwana International Networks (South Africa)
Paratus Namibia	102-106 Nickel Street, Prosperita	+264 83 300 1000	info.na@paratus.africa	https://www.na.paratus.africa/	Andrew Hall (Managing Director); Barney Harmse (Group CEO)		Part of Paratus Group
MTN Namibia	1st Floor Millennium Crown Building Corner Robert Mugabe and Dr A B May Streets	+26 461 20 98 000	support@mtnbusiness.co.na	http://www.mtnbusiness.com/na	Vaino Nghipondoka	/	MTN Group (South Africa)

## TANZANIA

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Vodacom Tanzania Ltd	15th Floor Vodacom Tower, Ursino Estate Plot 23, Old Bagamoyo Road, P.O. Box 2369 Dar es Salaam	+255 754 100 100	customercare@vodacom.co.tz	https://vodacom.co.tz/	Hishim Hendi (acting MD) Mohamed SHameel Aziz Joosub (CEO of Vodacom Group)	Nkateko Nyoka (Chief Legal Officer of Vodacom Group)	Vodacom Group (Pty) Ltd (South Africa)
MIC Tanzania Ltd (Tigo Tanzania)	MIC Tanzania LTD P.O. Box 2929 New Bagamoyo Rd, Dar es Salaam	0716123103	customercare@tigo.co.tz	https://www.tigo.co.tz/	Simon Karikari (MD)	/	Millicom (Sweden)
Airtel Tanzania Ltd	Airtel House Corner Of Ali Hassan Mwinyi Road Kawawa Road Dar es Salaam	+255 784 103 001	helpdesk@airtel.co.tz	https://www.airteltanzania.com/	Sunil Colaso (MD)	/	Bharti Airtel (India)
Viettel Tanzania Ltd (Halotel Tanzania)	4th Floor, Tropical Center, New Bagamoyo Road, P.O. Box 34716, Dar es Salaam	0620100100	Info@halotel.co.tz	http://halotel.co.tz/	Son Nguyen Van	/	Viettel Group (Vietnam)
Zanzibar Telecom Ltd (Zantel)	Zanzibar Telecom Limited, Mwai Kibaki Road/ Old Bagamoyo road, P.O. BOX 77052, Dar es Salaam	+255 775 000 000	/	http://www.zantel.co.tz/	Sherif El Barbary	/	Millicom (Sweden)

## ZAMBIA

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Zamtel	Zamtel House, Chilubi Road, Lusaka	+260 (211) 333 1152	customer@care@zamtel.co.zm	<a href="http://www.zamtel.zm/">http://www.zamtel.zm/</a>	Sydney Mupeta	Jonathan Bwembya Malama	State-owned
MTN	4647 Beit Rd, Addis Ababa Round About Rhodespark	+260 966 750 750	mtn@mtnzambia.co.zm	<a href="http://www.mtnzambia.com/en">http://www.mtnzambia.com/en</a>	Charles Molapisi	Mwenzi Mulenga	MTN Group (South Africa)
Airtel Zambia	Corner of Addis Ababa Drive Great East Road, Stand 2375, P.O. Box 320001 LUSAKA	+260 977 770097	customerservice@zm.airtel.com	<a href="https://www.airtel.co.zm/">https://www.airtel.co.zm/</a>	Apoorva Mehrotra (Managing Director)	/	Bharti Airtel (India)
Vodafone Zambia	Plot #257, Kaleya Road, Roma, Lusaka.	+260 211 378 555	care@vodafone.zm	<a href="https://www.vodafone.zm/">https://www.vodafone.zm/</a>	Lars Stork	/	Vodafone Group plc (UK)
Zamnet Communication Systems Ltd	Comesa Centre, Ben Bella Road, Lusaka	+260 211 220 736	support@zamnet.zm	<a href="http://www.zamnet.zm/">http://www.zamnet.zm/</a>	Nicodemus Mwazya (Managing Director)	/	University of Zambia

## ZIMBABWE

COMPANY NAME	REGISTERED OFFICE (ADDRESS)	TELEPHONE	EMAIL	WEBSITE	CEO	GENERAL COUNSEL/ CHIEF LEGAL OFFICER	PARENT COMPANY (INCLUDING COUNTRY OF REGISTRATION)
Econet Wireless Zimbabwe (ASP – Liquid Telecom)	No. 2 Old Mutare Road Msasa Harare, Zimbabwe	+263 4 486 121/6	sales@econet.co.zw	www.econet.co.zw	Hardy Pemhiwa	Chris Wadman	Econet Wireless Global Ltd. (Mauritius)
TelOne	Runhare House, 107 Kwame Nkrumah Avenue, P. O. Box CY 331, Causeway Harare, Zimbabwe	0242798111	clientservices@telone.co.zw	https://www.telone.co.zw/	Chipo Mtasa (Managing director)	/	State-owned
NetOne	NetOne Cellular Private Limited 16th Floor Kopje building Harare 1 Jason Moyo Avenue P.O BOX CY 579 Causeway	+263 716 778 912-9	customercare@netone.co.zw	http://www.netone.co.zw/home/	Lazarus Muchenje	/	State-owned
TeleCel	148 Seke Road Graniteside Harare	+263 4 748 321/7	info@telecelzim.co.zw	www.telecel.co.zw	Angeline Vere	/	State owned enterprise ZARNet owns 60% of Telecel, the other 40% is owned by Empower – ment Consortium a local investment vehicle.
ZOL	3rd Floor, Greenbridge, Eastgate, Cnr R Mugabe/Sam Nujoma, Harare	+263 8677 123123	support@zol.co.zw	https://www.zol.co.zw/	Denny Marandure	/	Liquid Telecom Group





## Contact

Runhare House, 107 Kwame Nkrumah Avenue

P. O. Box CY 331, Causeway Harare, Zimbabwe

Tel: 0242798111