# State of Internet Freedom in Africa 2016

## Case Studies from Select Countries on Strategies African Governments Use to Stifle Citizens' Digital Rights

September 2016

CIPESA

# State of Internet Freedom in Africa 2016

## Case Studies from Select Countries on Strategies African Governments Use to Stifle Citizens' Digital Rights

**September 2016**

CIPESA

# Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support from Facebook and Google.

The report presents the findings of a study on what governments are doing to inhibit citizens' access to ICT, for example content blocks, censorship, filtering, infrastructure control, law-making, court cases; how governments are using ICT activity and data to monitor citizens; and how government bodies and functionaries are using propaganda, impersonation, threats, cloning, and other tactics to shape online content in their favour. Full country reports are available for ten countries: Burundi, Democratic Republic of Congo, Ethiopia, Kenya, Rwanda, Somalia, Tanzania, Uganda, Zambia and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

## Research steering committee
Ashnah Kalemera, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Marilyn Vernon, Wairagala Wakabi

## Country researchers
**Burundi -** Jean Paul Nkurunziza - Internet Society Burundi Chapter and Alain Ndikumana - Institut des Statistiques et Etudes Economiques du Burundi (ISTEEBU)

**Democratic Republic of Congo -** Arsene Baguma Tungali and Gauis Kawone, Rudi International

**Ethiopia** - Melaku Girma

**Kenya -** Kenya ICT Action Network (KICTANet)

**Rwanda -** Robert Mugabe, Great Lakes Voices

**Somalia -** Mohamed Ibrahim, Union of Somalia Journalists

**Tanzania -** Jamii Media

**Uganda -** Peter Magellah, Chapter Four

**Zambia -** Hellen Mwale, Media Institute of Southern Africa Zambia Chapter

**Zimbabwe -** Natasha (Stash) Msonza, Digital Society of Zimbabwe

## Design
Ish Designs
muwonge_issa@yahoo.com

***State of Internet Freedom in Africa 2016***
Published by CIPESA, www.cipesa.org
September 2016

# CONTENTS

# 1.0 Introduction

The proliferation of Information and Communication Technologies (ICT) holds much promise for enhancing democracy and citizen participation in governance in Africa. Digital technologies expand the breadth of possibilities for people to enjoy freedoms of expression and association, and can be an enabler for enjoying the right of access to information. However, many state and non-state actors are steadily moving to curtail what individuals may do online, thereby inhibiting freedom of expression and the right to privacy, and undermining the potential of ICT to contribute to democratic governance and the enjoyment of citizens' rights.

Proponents of placing controls on information flows and freedom of expression in the online sphere have their rationalisations – namely, to deter crimes such as cyber fraud, child pornography, hate speech, and terrorism. The reality in many African countries is that several governments are throttling legitimate expression and citizen organising in the name of protecting national security or the public good.

Tanzania's new law on cybercrime[1], which came into force in September 2015, has already been used to charge up to 10 social media users with offenses such as "insulting the president". In the first two months of 2016, up to 10 social media users in Kenya were arrested or summoned by security authorities over their online communications.[2] In Uganda, the communications regulator ordered a blockage of access to all social media and mobile money as the country went to elections on February 18, 2016 and then again in May while the re-elected president was being sworn in, and there were arrests of social media users over content deemed critical of the president.[3] Ethiopia has had two shut downs of the internet this year, hundreds of websites remain blocked in the country, bloggers are regularly prosecuted, and the state continues to up its surveillance capabilities. Rwanda maintains a blockage of websites and continues active surveillance of citizens' communications. In Zimbabwe, the past year has seen several individuals charged over their social media posts, while the Zambian government has maintained its hunt for critical citizen journalists.

The right to receive, seek and impart information or ideas regardless of the medium used is enshrined in the Universal Declaration of Human Rights (UDHR). It is also guaranteed by the African Charter on Human and Peoples' Rights and indeed in the constitutions of various African countries. But as the above cases illustrate, rights holders including civil society and media practitioners have come under growing threat by governments seeking to restrict citizen voices critical of state operations. Through recent laws and regulations, as well as proposed laws, governments in the region have showed strong readiness to rein in critical civic voices. In the countries studied, there are numerous challenges to free expression online and these are affecting the way citizens and organisations communicate over digital technologies. Repressive and archaic laws, some dating back to the colonial era, are being used in some African countries to infringe on digital rights, interception of communications happens sometimes without judicial oversight, user data is not adequately protected, surveillance is conducted without transparency by intermediaries or state organs, and there have been numerous threats against social media users, and arraignments over individuals' online communications. The sum total of this is that many citizens operate anonymously online for fear of reprisals, many citizens heavily self-censor and have several taboo topics, while others have totally withdrawn from the online public sphere.

*1. The Cyber Crimes Act, 2015, No. 14 of 2015*
*2. New Year, Old Habits: Threats to Freedom of Expression Online in Kenya, http://www.cipesa.org/2016/01/new-year-old-habits-threats-to-freedom-of-expression-online-in-kenya/*
*3. See Ugandans Turn to Proxies, VPN in Face of Social Media Shutdown, http://www.cipesa.org/2016/02/ugandans-turn-to-proxies-vpn-in-face-of-social-media-shutdown/; Two arrested over 'dead' Museveni picture, http://www.monitor.co.ug/News/National/Two-arrested-over--dead--Museveni-picture/688334-3106714-11plidxz/index.html*

In order to promote internet freedom in Africa, there is a need to understand what the state of internet freedom is, what the obstacles are, which stakeholders are most at risk, and what tactics governments have used to curtail internet freedom over the years. This report investigates these issues, looking at cases studies from ten countries: Burundi, Democratic Republic of Congo, Ethiopia, Kenya, Rwanda, Somalia, Tanzania, Uganda, Zambia and Zimbabwe. We explore what governments are doing to inhibit citizens' access to ICT, for example content blocks, censorship, filtering, infrastructure control, law-making, court cases; how governments are using ICT activity and data to monitor citizens; and how government bodies and functionaries are using propaganda, impersonation, threats, cloning, and other tactics to shape online content in their favour.

Many African countries face a democracy deficit with those in the Sub-Sahara region characterised by one reputable index as either authoritarian, mixed democratic and autocratic or flawed democracies.


**Economic Intelligence Unit's Democracy Index 2015**[4]

Such a scenario means that, on the one hand ICT has the potential to aid the democratisation of such countries by enhancing citizen-to-citizen and citizen-to-government interactions, offering citizens alternative sources of Information, enabling citizen organising and the enjoyment of a gamut of rights and freedoms. On the other hand, however, governments that do not respect offline rights are most likely not to respect online rights. And yet it is not only state actors that are a threat to internet freedom; non-state actors present a threat too. In Somalia, for instance, the federal government, regional governments and the militant group Al Shabaab are competing against each other in controlling what citizens can do with ICT. And in many countries, citizens are the drivers of online violence against women, hate speech, and attacks against members of the Lesbian, Gay, Bisexual, Transgender, Queer and Intersex (LGBTQI) community.

In July 2016, the United Nations Human Rights Council condemned internet shut downs and declared that the same rights people have offline must also be protected online. This message needs to be pressed home with African governments and citizens alike. The incidents which are chronicled in this research report demonstrate that many African governments are predators of internet freedom. The level of access to ICT, while growing steadily, is still low, and the threats to internet freedom could result into further alienating huge numbers of African citizens from the information society, from participation in governance processes, and from enjoying their rights to free expression, association and access to information.

The research results presented in this report focus on recent legal and policy developments, as well as on abuses and violations of internet freedom over the 12 months period to September 2016. However, in order to establish trends on strategies used by respective African governments, the study takes an interest in practices over the last five years.

*4. EIU. (2014). The Democracy Index 2014.http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0115*

# 2.0 Method

Researchers based in each of the focus countries interviewed key informants who were purposively selected. The informants were chosen on the basis of their known or presumed knowledge about issues related to or affecting internet freedom in the countries studied. They included activists and human rights defenders that are advancing free expression and association in these countries, as well as some of those who had been victims of abuses and violations. Others were internet and telecom service providers, regulators, law enforcement officials, and journalists. Some of these individuals were interviewed face-to-face; in other instances, such as with exiled actors from countries such as Burundi, Ethiopia, Somalia and Rwanda, some interviewees were interviewed by phone or via the internet or interviewed physically in the countries where they are staying. In total, 400 key informants were interviewed for this report, with numbers for each country varying.

Policy analysis was conducted so as to generate an understanding of the laws that affect digital rights. The analysis took an interest both in policies and laws that have been used to curtail internet freedom and those that could potentially be employed in curtailing freedom of expression and access to digital technologies. Besides the existing laws, an analysis was done of relevant Bills currently under consideration in the focus countries. Moreover, document review was done, including of open access sources such as media articles and secondary research reports, as well as analysis of records such as court orders and regulatory decisions, some of which are not readily available in the public domain. Finally, in some countries we conducted tests on certain websites to establish whether they were blocked or not, or relied on third party test results – such as by the Open Observatory of Network Interference (OONI).

# 3.0 Laws and Policies Affecting Internet Freedom in Africa

Over the years, various African governments have gone to great lengths to devise mechanisms of controlling the enjoyments of peoples' right to freedom of expression. The dawn of the internet has, however, complicated matters for such states given the difficulty of controlling the spread of information, the availability of encryption, the world wide nature of the Internet, and the difficulty of determining the originator of information which is anonymous or pseudonymous.[5]

Accordingly, several African governments have resorted to using provisions from within the existing draconian communications laws and policies to censor and control online communications. The first official act of Internet censorship in Africa is believed to have occurred in February 1996 when the Zambian government succeeded in removing a banned edition of The Post from the newspaper's website by threatening to prosecute the country's main Internet Service Provider (ISP), Zamnet.[6] The offending edition of The Post was banned under the Preservation of Public Security Act because it allegedly contained a report based on leaked documents which revealed secret government plans for a referendum on the adoption of a new constitution. A presidential decree warned the public that anyone caught with the banned edition, including the electronic version, would be liable to prosecution.[7]

In the recent past, however, there has been a wave of activity on legislation that primarily target online communications in other Africa countries. Since 2010, the government in Tanzania has brought to parliament various bills that have a direct effect on online freedom of expression - the Cybercrimes Act, 2015, the Statistics Act, 2015, the Electronic and Postal Communication Act, 2010, the Access to Information Bill, 2015, and the Media Services Bill, 2015.

Tanzania's Cybercrime Act, 2015 gives a police officer in charge of a police station or a law enforcement officer the power to issue an order for the collection of data relating to information subject to a criminal investigation. This provision has a high potential for abuse.[8] Under the Statistics Act, 2015 it is an offence for a "radio station, television station, newspaper or magazine, website or any other media" to publish "false statistical information" or for an "agency or person" to publish "official statistical information which may result in the distortion of facts." This is provided under the provisions of sections 37 (4) and (5) of the Act. Additionally, the Statistics Act imposes harsh penalties on those found guilty of publishing misleading and inaccurate statistics or statistics not approved by the National Statistics Bureau. The punishment is a one-year jail term and a fine of 10 million Tanzania Shillings (about US$ 4,586).

In Zimbabwe, there is no specific law or policy dealing with internet rights and access, although the constitution provides for these rights without mentioning the online domain. There are, however, several Bills under consideration by parliament that include the Data Protection Bill; the Electronic Transaction and Electronic Commerce Bill; and the Computer Crime and Cybercrime Bill.[9] Nonetheless, the government continues to invoke various provisions within the existing but deficient legislation in order to quell criticism and dissent, infringing onto online spaces and social media platforms to punish individuals perceived to be troublemakers.[10]

*5. Can the Internet be Regulated?, http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/RP9596/96rp35*
*6. The right to Communicate: Internet in Africa available at https://www.article19.org/data/files/pdfs/publications/africa-internet.pdf*
*7. Ibid*
*8. S. 35, Cyber Crimes Act, 2015*
*9. Authorities move to control cyberspace,*
*http://www.theindependent.co.zw/2015/07/24/authorities-move-to-control-cyberspace*
*10. For example the Criminal Law and Codification Act (CODE) which was used to arrest the alleged Facebook pseudonymous character, Baba Jukwa believed to be former Sunday Mail Editor Edmund Kudzayi. Charges were later dropped due to failure by the state to gather sufficient evidence.*

In the absence of a cyber law in Zimbabwe, the Criminal Law and Codification Act 2004 (CODE), popularly known as the 'insult law' [11] has been the government's weapon of choice against critics both online and offline. In the face of rising protests in 2016, given the number of arrests made on the basis of CODE, this has been the easiest law for the government to invoke in harassing and arresting real and perceived 'trouble-makers'[12] opponents and critics of President Robert Mugabe.

Because of this law, ordinary people have increasingly been at risk of arrest for any statements or criticisms made in respect of exercising their freedom of speech. Indeed, in justifying the need to regulate social media, the government invokes the arguments of national security and the endeavour to protect women and children online from cyber-bullying in various forms, paedophiles and 'revenge porn.'[13] While these are valid and welcome grounds for social media regulation, there are also reasonable grounds for anticipating that dissenting activists will be targeted with a clampdown on internet freedoms. The country is already invoking existing laws such as the Public Order and Security Act (POSA); Criminal Law (Codification and Reform) Act; the Access to Information and Protection of Privacy Act (AIPPA) and the Interception of Communications Act (ICA).

Like Zimbabwe, Kenya does not have any specific laws or polices dedicated to internet freedoms, but also relies on a variety of legislation to exert control. Section 29 of the Kenya Information and Communications Act (KICA) 2013, penalises the use of ICT to disseminate messages deemed to be "grossly offensive" or that cause "annoyance, inconvenience or needless anxiety to another person" with a fine of up to Kenya Shillings 50,000 (about US$ 495), three years in prison, or both.[14] The KICA does not clearly define what constitutes content that causes "annoyance, inconvenience or needless anxiety to others," while the Penal Code has no clear definition of a "rumour" or "report which is likely to cause fear and alarm to the public or to disturb the public peace.[15] "

On the other hand, the Security Laws (Amendment) Act 2014, allows admissibility in court of electronic messages and digital material regardless of whether it is not in its original form. Part V of that law regarding "special operations" raises particular concerns, as it expands the surveillance capabilities of the Kenyan intelligence and law enforcement agencies without sufficient procedural safeguards.[16] This law, passed amidst government's frantic efforts to fight terrorist attacks inside the country by the Somali militant group Al Shabaab, gives broad powers to the Director General of the National Intelligence Service to authorise any officer of the Service to monitor communications, "obtain any information, material, record, document or thing" and "to take all necessary action, within the law, to preserve national security."

Kenya's National Intelligence Service Act, 2012 gives security agencies the powers to monitor communications as well as to "search for or remove or return, examine, take extracts from, make copies of or record in any other manner the information, material, record, document or thing." Additionally, the Media Council Act, 2013 contains "broad" speech offences, which could be further reinforced by the Cybercrime and Computer Related Crimes Bill, 2014 when it comes into force.[17] Early this year the Kenya government indicated that it was preparing a bill to regulate social media use ahead of the 2017 elections.[18] The debate around this was to tame hate-speech and prevent violence during the elections. During the period of January to April 2015, 27 bloggers were arrested and charged under the now repealed section 29 of the KICA Act. In the first two months of 2016, up to 10 social media users in Kenya were arrested summoned by security authorities over their online communications.[19]

Kenya, which has seen a rise in anti-gay rhetoric led by various political leaders, with attempts to introduce an anti-homosexuality law, in February 2016 had the Kenya Film Classification Board (KFCB) order Google to pull down a video the agency deemed inappropriate for promoting gay relationships. The KFCB also expressed its interest to rate and therefore censor content from Netflix[20] and potentially ban it for national security reasons.[21]

*11. Section 33 of CODE, which makes it a criminal offence to intentionally make public statements that undermine or insult the President in person or in his official capacity.*
*12. Interview with TZ, Political Analysts conducted 22 June 2016.*

*14. The Kenya Information and Communications Act, chapter 411A, 2009*
*15 . New Year, Old Habits: Threats to Freedom of Freedom of Expression Online in Kenya, http://cipesa.org/2016/01/new-year-old-habits-threats-to-freedom-of-expression-online-in-kenya/*
*16. Kenya High Court Ruling on Security Amendment Act a Victory for Free Speech, https://www.article19.org/resources.php/resource/37866/en/kenya:-high-court-ruling-on-security-amendment-act-a-victory-for-free-speech*
*17. Ibid*
*18. Kaka Mwalimu, Government prepares bill to regulate social media usage, http://www.hivisasa.com/national/news/145899*
*19. CIPESA, New Year, Old Habits: Threats to Freedom of Expression Online in Kenya, http://www.cipesa.org/2016/01/new-year-old-habits-threats-to-freedom-of-expression-online-in-kenya/*
*20. Margaret Wahito, Netflix content must be classified afresh, says KFCB, http://www.capitalfm.co.ke/business/2016/01/netflix-content-must-be-classified-afresh-says-kfcb/*
*21..http://www.standardmedia.co.ke/business/article/2000188791/kenya-film-board-protests-decision-not-to-regulate-netflix?articleID=2000188791&story_title=kenya-film-board-protests-decision-not-to-regulate-netflix&pageNo=1*

In Burundi, the main law governing the media is the Press law No 1/15 of May 9, 2015, which covers all types of communication, radio, television, cinematography, written, on the internet and all media public or private.[22] In March 2016, another law, the Ministerial Law No 540/356 whose main object is to fight fraud in electronic communications was adopted.[23] In its first Article, the new law prohibits the possession of two SIM cards from one telecom operator. Any user requiring two SIM cards from one telecom operator has to be authorised by the national telecommunication regulatory authority. Moreover, Article 3 obliges mobile operators to "take all the necessary measures" to verify if SIM card users are the "real subscribers" and incase of detection of an anomaly, block the SIM card. The country has recently promulgated a law that imposes a single gateway for all incoming and outgoing international calls from Burundi.

In Rwanda, the 2008 Interception of Communications law (amended in 2013)[24] allows the national security services to apply for issue of an interception warrant to monitor citizens' voice and data communications on grounds of national security. Warrants are issued by a national prosecutor who is appointed by the justice minister. In urgent security matters, however, a warrant may be issued verbally, "but the written warrant shall be completed in a period not exceeding twenty four hours". A warrant shall be valid for three months. Article 7 of the 2013 law requires service providers to ensure that their systems "are technically capable of supporting interceptions at all times, security organs have powers to intercept communications using equipment that is not facilitated by communication service providers."

The 2001 Law Governing Telecommunications[25] states that court can authorise the interception or recording of communications in the interests of national security and the prevention, investigation, detection and prosecution of criminal offences. According to article 52(1), "The Minister may, whilst observing national legislation and international agreements ratified by the Rwandan Republic interrupt or cause to be interrupted, any private communication which appears dangerous to the National integrity, contrary to law, public order or public morals".

Article 7 of a 2015 ministerial order in Congo[26] entrusts telecommunication companies to protect their subscribers' privacy, but wording is very vague and too permissive of abuse for state actors. For example, if national security or a judicial case is cited, this article allows "authorities," namely ministries and other agencies, to violate subscribers' privacy without any documentation or consent from the Attorney General. Article 11 of the same order requires telecommunication companies to send data collected about subscribers' identities to government services before deleting them from their database. This provides for easy state surveillance and the vagueness of the law can be exploited to abuse rights.

In Uganda, although the country's constitution provides for citizens' right to freedom of expression and privacy, under Articles 29, 27 and 41, there are numerous laws passed between 2010 and 2015 that constrain freedom of expression on the internet as well as offline.[27] The 2010 Regulation of Interception of Communications Act gives the ICT minister the powers to set up a monitoring centre, which maintains connections with telecommunication systems. Section 8 of the Act requires service providers to assist in intercepting communication by ensuring that their telecommunication systems are technically capable of supporting lawful interception at all times. The operators are required to install software and hardware, ensure their services are capable of rendering real time and full time monitoring facilities, provide all call-related information in real time or as soon as possible upon call termination; and provide for more than one interface from which the intercepted communication shall be transmitted to the monitoring centre.

The Anti-Terrorism Act (2002) gives security officers powers to intercept the communications of a person suspected of terrorist activities and to keep such persons under surveillance. The scope of the interception and surveillance includes letters and postal packages, telephone calls, faxes, emails and other communications, access to bank accounts, as well as monitoring meetings of any group of persons. Under the anti-terrorism law, journalists who "promote terrorism" can be liable to capital punishment. On January 19, 2016 the President signed into law the Anti-Terrorism (Amendment) Act, 2016 .[28] The Act purportedly aligns Uganda law with international requirements on money laundering and terror financing. However, there are concerns on provisions that make it a crime to interfere with communication systems of any kind.

*24. Law No. 1/15, http://assemblee.bi/IMG/pdf/15%20du9%20mai%202015.pdf*
*24. Law No. 540/356, http://www.arct.gov.bi/images/image0008.pdf*
*25. Law on Interception of Communications,*
*http://www.vertic.org/media/National%20Legislation/Rwanda/RW_Law_48_2008_Interception_Communications.pdf*
*24. Telecommunications Law, http://www.rura.rw/fileadmin/laws/TelecomLaw.pdf*
*26. http://www.leganet.cd/Legislation/Droit%20economique/telecommunication/AIM.19.05.2015.html.*
*27. http://www.cipesa.org/?wpfb_dl=76*
*28. The Anti-Terrorism (Amendment) Act, 2016, http://www.parliament.go.ug/images/Anti-Terrorism_amendment_Act_201621.pdf*

On February 26, 2016 Uganda gazzetted a Bill to amend the Communications Act 2013. The Communications (amendment) Bill 2016 seeks to amend section 93(1) of the Communications Act, 2013 to enable the minister to make regulations for the sector without seeking parliamentary approval. There are fears that, if this amendment is passed, the ICT minister could single-handedly issue tough rules against social media use, but the government denies this.

Uganda's Computer Misuse Act[29] seeks to provide for safety and security of electronic transactions and information systems and to prevent unlawful access, abuse or misuse of information systems.[30] The Act makes it an offence for a person to make a communication that will "disturb the peace and quiet or right to privacy of a person". However, it does not define the circumstances under which such can be applied hence making any form of cyber communication potentially capable of being an ingredient of such a crime.[31] The Act has a broad definition of a computer, which covers all types of electronic or electromagnetic systems capable of storing or transmitting data. The broad definition of a computer means any person using an electronic or electromagnetic system has a duty to act within the confines of the Act, failure of which that person commits one of the several offences under the Act.

The broad nature of this Act was tested in Nyakahuma vs. Uganda[32] where in a High Court reference to determine whether posting materials on the internet amounted to publication within the meaning of the Penal Code Act[33], the judge ruled that the broad nature of the Computer Misuse Act captured all forms of posts made on cyberspace irrespective of the tool used to post.

Uganda also passed the Anti-Pornography Act, 2014, which requires ISPs to monitor online content to identify and remove content considered pornographic. It also gives powers to the police to direct media houses not to publish content the police considers violates the Act. In April 2016, cabinet announced the appointment of members of the Anti-Pornography Committee.[34] The same month saw the Ethics Minister seeking parliament's approval of approximately US$ 770,380 to procure "pornography detecting software".[35]

Section 3 of the Anti-Pornography Act 2014 provides for the establishment of a pornography control committee whose functions include early detection and prohibition of pornography, ensuring that perpetrators of pornography are apprehended and prosecuted, collecting and destroying pornography materials and educating the public against pornography. In August 2016, the minister for Ethics told the press that the country was purchasing a machine to detect and remove pornographic content from the Internet, social media sites, blogs and phones. He promised that the machine had already been purchased and would be in the country by September 2016.[36] It should be noted that at the time of writing this report it was not clear if the machine was already in the country. It was unclear also how the machine would operate.

In Ethiopia, government uses a variety of laws and policies to curtail online freedoms and communication. According to Freedom House's Freedom on the Net 2015 report, the government in 2012, introduced specific restrictions on an array of ICT activities under amendments to the 1996 Telecom Fraud Offences Law, which had already placed bans on certain communication applications, such as Voice over Internet Protocol (VoIP) like Skype and Google Voice, call back services, and internet-based fax services.[38] According to Section 15 of the law, digital or electronic evidence; evidence gathered through interception or surveillance; and information obtained through interception conducted by foreign law enforcement bodies, are admissible as evidence in court. The law also added the requirement for all individuals to register their telecommunications equipment—including smartphones—with the government, which security officials typically enforce by confiscating ICT equipment when a registration permit cannot be furnished at security checkpoints, according to sources in the country.[39]

*29. Act No. 2 of 2011*
*30. See long title to Computer Misuse Act, 2011*
*31. S. 25 ibid*
*32. High Court criminal reference No 1/2013 available at http://www.ulii.org/ug/judgment/high-court-criminal-division/2013/30-0*
*33. Cap 120, laws of Uganda*
*34. Pornography control committee named, The Sunday Vision, April 14, 2016,*
*http://www.newvision.co.ug/new_vision/news/1422110/anti-pornographic-committee-named*
*35. Anti Pornography Committee Redundant,*
*http://www.monitor.co.ug/News/National/Anti-pornography-committee-redundant/688334-3304124-l07jex/index.html*
*36. Pornography detection machine arrives September – Lokodo,*
*http://www.newvision.co.ug/new_vision/news/1431545/pornography-detection-machine-arrives-august-lokodo#sthash.512ufsil.dpuf,*
*37. A Proclamation on Telecom Fraud Offence," Federal Negarit Gazeta No. 61, September 4, 2012, http://www.abyssinialaw.com/uploads/761.pdf.*
*38. Freedom House (2015), Freedom on the Net - Ethiopia Report, https://freedomhouse.org/report/freedom-net/2015/ethiopia*
*39. Ibid*

The Anti-Terrorism Proclamation of 2009 authorises interception of communication and a number of journalists, bloggers, and democracy activists have been charged and sentenced under this law.[40] In 2013, through Proclamation No- 808-2013[41] , the Ethiopian government revamped the Information Network Security Agency (INSA), which is said to be at the forefront of the government's internet control and censorship strategy. According to the law, social media outlets, blogs and other internet related media had great capabilities to instigate dispute and war, to damage the country's image and create havoc in the economic atmosphere of the country.

Ethiopia's National Intelligence and Security Service (NISS), under Article 8 (7) of its proclamation law, is mandated to conduct surveillance, using a court warrant, "in order to protect national security and prevent threats to national security" and can do this "by entering into any place and by employing various mechanisms." Under Article 27, all persons have a duty to cooperate, if requested, in furnishing intelligence or evidence necessary for the work of the NISS. Those requested to provide assistance to the service are required to keep the request confidential.[42]

However, in countries with no legal provisions, the situation can be worse, as authorities can issue orders curtailing internet freedom without having the bother of citing any law. In Somalia, a draft Somali Communications Act was presented to Parliament after consultation in May 2014 in attempt to get legislation to the ICT sector for the first time in more than two decades. However, the Bill was not debated until 2015 when it had two readings. Again, the parliament has not yet undertaken the third and final reading of the Bill. This has left the issues of ICT and internet regulation to semi-autonomous regions and local authorities make the rules regarding what citizens may or may not do with ICT. These authorities include local administrators and militant groups such as Al Shabaab.

*40. State of Internet Freedom in East Africa, 2014, http://www.cipesa.org/?wpfb_dl=76*
*41. A Proclamation to Reestablish the Information Network Security Agency, https://chilot.files.wordpress.com/2014/04/proclamation-no-808-2013-information-network-security-agency.pdf*
*42. State of Internet Freedom in East Africa 2014, http://www.cipesa.org/?wpfb_dl=76*

# 4.0 Results

## 4.1 Internet Shutdowns Becoming the New Control Tools

For many African countries, Internet shutdowns are becoming the most preferred control mechanisms governments are using to curtail the right to freedom of expression and access to information online. This is a marked shift from SMS filtering or websites blocking that were hitherto more prevalent. The shutdowns are effected through orders to service providers to block access to either selected services (such as Facebook, Whatsapp, Twitter and mobile money services), or a total obstruction of access to the entire internet.

In Ethiopia, whereas website blocking remains prevalent – with tests by OpenNet researchers showing several websites were inaccessible in the country as of September 2016 – the authorities seem to be developing an appetite for shutdowns. In July 2016, government ordered that access to Facebook, Twitter, Instagram, Viber, WhatsApp and other sites be blocked. The government claimed the country-wide ban was necessary after university entrance exams were posted online and that the blockage was intended to prevent students from being distracted from studying during the exam period and to prevent the spread of false rumours.[43] Again in August 2016, Ethiopia shut down the internet during protests by the Oromos and Amhara ethnic groups against alleged marginalisation by the government.[44] Protesters are believed to have relied on the internet to plan, mobilise and coordinate with each other and this may have prompted the state to shut down the internet.[45]

In Uganda, government ordered the shutdown of internet access on the eve of the presidential elections voting day, citing "national security", as well as during the inauguration in May 2016, affecting social media platforms including Facebook, Whatsapp, Twitter and mobile money transfer services.[46] The shutdowns and threats of shutdowns are not new in Uganda as the Uganda Communications Commission previously ordered a shutdown of access to social media platforms such as Twitter and Facebook in April 2011 during the "walk to work" protests led by the opposition. In 2015, the government also threatened to shut-down the internet over what it termed at "misuse" by the public.[47]

The Zimbabwean government, never one to miss out on fresh ways to stifle citizens' rights, has generally been suspected of interfering with mobile telephone networks in periods of significant political activity such as the elections of 2013 and the August 2016 'Million Man March'[48] , where mobile networks seemed to be jammed and mobile money transfers were noticeably slower than usual.'[49] Some critics claimed the Zimbabwe government had always throttled the internet, but because there was no deliberate observation at the time, this happened without ordinary people noticing.[50]

In April 2016, upon his return from a visit to Japan, President Mugabe made a public pronouncement that he would introduce "Chinese-style" internet restrictions on social media, ostensibly "to control 'abuse'[51] of the digital platforms and cyberspace." The communications regulator also issued public threats that those who 'misused' social media would be nabbed. Many Zimbabweans on Twitter took this to mean a possible ban of social media. The government is generally not trusted to fairly regulate the platforms it considers offensive or threatening, hence any regulation would be perceived as tantamount to a ban. This is why it was easy for the citizenry to believe that there was a shutdown of some parts of the internet, especially of Whatsapp, on the day of the first #ShutDownZimbabwe2016 protests.

*43. Ethiopia blocks Facebook and other social media for exams, http://www.bbc.com/news/world-africa-36763572*
*44. What is behind Ethiopia's wave of protests?, http://www.bbc.com/news/world-africa-36940906*
*45. How the Ethiopia Protests Were Stifled by a Coordinated Internet Shutdown, http://qz.com/757824/how-the-ethiopia-protests-were-stifled-by-a-coordinated-internet-shutdown/*
*46. Social media, Mobile Money switched off over national security concerns, http://mobile.monitor.co.ug/News/Social-media-Mobile-Money-switched-off-over/2466686-3082556-format-xhtml-kuye9l/index.html ; Government shuts down social media again, http://mobile.monitor.co.ug/News/Government-shuts-down-social-media-again/2466686-3201024-format-xhtml-u0c08e/index.html*
*47. UCC Social Media Platforms Abuse, http://www.monitor.co.ug/News/National/UCC-social-media-platforms-abuse/-/688334/2619032/-/151o4ktz/-/index.html*
*48. An initiative organized by the ruling party Zanu PF's youth league early this year on 25th May 2016, as a way to 'celebrate the visionary and iconic leadership of President Mugabe': http://www.herald.co.zw/live-one-million-man-march-25-may-2016-in-solidarity-with-the-iconic-leadership-of-president-mugabe*
*49. Interview with political analyst, TZ held 22 June 2016.*
*50. Interview with Chris Musodza conducted on 1 August 2016*
*51. The President alluded to the role that the mobile application WhatsApp was playing in spreading mis-information, and that this needed to be curbed. See article: http://www.techzim.co.zw/2016/04/china-style-internet-censorship-coming-to-zimbabwe-president-mugabe/#.V6p3c46zDaY*

In April 2015, the Burundi government shut down social media networks including Viber, Twitter, Whatsapp, and Facebook during public protests to block President Pierre Nkurunziza from seeking another term in office.[52] This was despite the fact that only 8% of Burundians access the internet. However, the protesters had been able to use social media to quickly communicate and mobilise.[53] Just like happened in Uganda, many users were able to by-pass the blockage by installing VPNs on their communication devices.

Meanwhile in DRC, the internet and Short Message Services (SMS) were completely shut down starting from January 19, 2015, for about 20 days, denying people their right to access various sources of information and their right to freedom of expression. During this period government allowed limited access to internet mainly for banks and government agencies. Sources within the telecommunication sector informed the UN's Radio Okapi that the order came from the country's authorities who did not give any official reason. Lambert Mende, DRC's Information Minister and spokesman of the government, communicated to other media outlets that internet and Radio France International (RFI) were blocked for "good reasons."[54] Anonymously, telecommunications operators complained of the negative impact blockages would have on their income. Some reportedly feared that clients would seek legal recourse by taking them to court as the agreement for mobile internet services provision was made with subscribers not government.[55]

Prior to this, from December 3-28, 2011, the government had ordered all SMS to be blocked as the country was awaiting the results of the presidential election that had taken place in November 2011. The Réseau national des ONG des droits de l'homme de la République Démocratique du Congo (Renadhoc), a network of national human rights non-governmental organisations, condemned these actions on local and national media outlets, calling on the government to reconsider its decision.[56]

For many human rights defenders this presents a worrying trend as many of the shutdowns are being ordered at critical moments in democratic processes.[57] In June 2016, the United Nations Security Council passed a landmark resolution condemning internet shutdowns. It condemned "unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and called on all States to refrain from and cease such measures."[58]

*52.- Burundi Shuts down Internet Access, http://www.itwebafrica.com/ict-and-governance/363-burundi/234560-burundi-shuts-down-internet-access*
*53. Despite low Internet Use, Burundi Blocks Viber and Whatsapp, https://www.eff.org/deeplinks/2015/04/despite-low-internet-use-burundi-blocks-viber-and-whatsapp*
*54. Radio Okapi, http://www.radiookapi.net/actualite/2015/01/21/rdc-linternetinternet-sera-bientot-retabli-assure-lambert-mende/*
*55. 7Sur7, http://7sur7.cd/new/coupure-de-linternet-en-rdc-les-operateurs-de-la-telephonie-mobile-aux-abois/*
*56. National Network of Congolese Human Rights NGO: Declaration of Suspension https://rsf.org/sites/default/files/_declaration_du_renadhoc_sur_la_suspension_prolongee_de_s_sms_en_rdc_22.12.2011-2.pdf*
*57. Stop Internet Shutdowns Becoming New Normal Africa, https://webwewant.org/news/stop-internet-shutdowns-becoming-new-normal-africa/*
*58. Internet Statement Adopted, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf*

## 4.2 Using and Abusing Courts of Law to Stifle Internet Freedom

Another emerging trend has been the use and abuse of law courts to stifle online freedoms. There is a marked increase in arrests, and in charging of journalists, media houses and human rights activists for online related offences. Majority of the legal provisions used are less than 10 years old – with most falling in laws passed in the last six years - although there are also instances of laws dating back more than four decades being used. Increasingly, governments have learnt that using courts of law provides some legitimacy to their actions as steeped in the rule of law. Moreover, it 'sets an example for others' not to annoy the government and in effect has a chilling effect as it results into self-censorship – a desired effect by undemocratic governments.

In Tanzania, the Cyber Crimes Act passed in September 2015 has already been used against 10 social media users.[59] For example, in October 2015, Benedict Angelo Ngonyani was charged for "spreading misleading information"[60] after he posted on Facebook that Tanzania's Chief of Defence Forces, General Davis Mwamunyange, had been hospitalised following food poisoning. In the same month, Sospiter Jonas was charged with "misuse of the internet" after posting on Facebook content stating that Tanzanian Prime Minister Mizengo Pinda "will only become a gospel preacher".[61] In October 2015, four communication volunteers of opposition party, Chama Cha ma Demokratia na Maendeleo (CHADEMA) were charged for publishing "inaccurate" election results on Facebook and Twitter.[62] Many social media users have been charged for "publication of false information" in accordance with Section 16 of the Act, which states: "Any person who publishes information, data or facts presented in a picture, text, symbol or any other form in a computer system where such information, data or fact is false, deceptive, misleading or inaccurate commits an offence, and shall on conviction be liable to a fine not less than three million shillings or to imprisonment for a term not less than six months or to both." In one of the latest incidents, a lecturer at Mkwawa University College of Education was arrested in September 2016 for allegedly insulting President Pombe Magufuli in a Whatsapp message. While confirming the detention of the lecturer, police declined to reveal the content of the message he was accused of sending.[63]

In Kenya, there has been an increase in the number of documented cases of social media users charged in court during 2016. On January 25, 10 bloggers were summoned by the Directorate of Criminal Investigations (DCI) for questioning over alleged misuse of a licensed telecommunications system under Section 29 of the Information and Communication Act.[64] The 10 included Robert Alai, Cyprian Nyakundi, Patrick Msafari, Seth Odongo, Charles Dienya, Anthony Mburu, Eddy Illah, Phelix G-Cord, George Nyongesa and Yassin Juma. The arrests were condemned by the Bloggers Association of Kenya (BAKE) as attempts by the government to intimidate Kenyans online and were tantamount to "criminalisation of civil matters" with users being arrested on charges that ultimately infringe upon freedom of expression.[65]

However, Zimbabwe seems to have by far the largest number of suits brought against individuals over their online communications. In April 2016, an agriculture ministry staffer from Nyanga, Ernest Matsapa, was charged with the crime of "criminal nuisance" after the authorities accused him of "unlawfully and intentionally" sending an audio and visual message on a Whatapp group of which he is a member.[66] The clip is said to have depicted an incapacitated Mugabe as having become a burden on citizens, including his family.[67] Zimbabwe Lawyers for Human Rights (ZLHR) officials told OpenNet Africa that since August 2015, they have assisted over 120 people arrested for posts they made

*59. Tanzanian lecturer charged with insulting president on WhatsApp, http://www.reuters.com/article/us-tanzania-president-idUSKCN11T14C?il=0*
*60. Cyber crime case involving student adjourned, http://dailynews.co.tz/index.php/home-news/45785-cyber-crime-case-involving-student-adjourned*
*61. Man charged over Pinda internet jibe, http://www.thecitizen.co.tz/News/Man-charged-over-Pinda-internet-jibe/-/1840340/2913954/-/1jf9kn/-/index.html*
*62. Chadema volunteers charged with publishing wrong results,*
*http://www.thecitizen.co.tz/tanzaniadecides/Chadema-volunteers-charged-with-publishing-wrong-results/-/2926962/2933186/-/6kxx4e/-/index.html*
*63. Hakimu Mwafongo, Varsity lecturer arrested for insulting Magufuli online,*
*http://www.thecitizen.co.tz/News/Varsity-lecturer-arrested-for-insulting-Magufuli-online/1840340-3391526-i3itquz/index.html*
*64. 10 Bloggers to be grilled over Internet posts, http://www.standardmedia.co.ke/article/2000189434/10-bloggers-to-be-grilled-over-internet-posts*
*65. James Wamathai, BAKE condemns the arrest and intimidation of Kenyans online,*
*http://www.blog.bake.co.ke/2016/01/24/bake-condemns-the-arrest-and-intimidation-of-kenyans-online/*
*66. Zimbabwe Arrests Soar Mugabe Regime Cracks Down Social Media,*
*http://www.ibtimes.co.uk/zimbabwe-arrests-soar-mugabe-regime-cracks-down-social-media-1553230*
*67. Ibid*
.

on social media sites like Facebook and Twitter.[68] The magnitude of arrests made of ordinary citizens under spurious charges, especially under Zimbabwe's insult laws, have been worryingly on the increase. In the majority of cases, courts have ruled in favour of protecting privacy rights, but have also cited some cases as being in breach of freedom of expression online.[69]

In Uganda, police in June 2015 arrested a prominent social media critic Robert Shaka, on allegations of being behind the pseudonym Tom Voltaire Okwalinga (TVO), responsible for reportedly leaking government secrets on Facebook. Shaka was arrested on charges under Section 25 of the Computer Misuse Act 2011, namely using computers and other electronic devices to issue "offensive communication".[70] The charges of making "offensive communications" brought against Shaka relate to Facebook posts by TVO on President Museveni's health status. Authorities alleged that between 2011 and 2015, Shaka had "willfully and repeatedly using a computer with no purpose of legitimate communication disturbed the right of privacy" of President Museveni "by posting statements as regards his health condition on social media."[71] Whereas this individual was released after a week in detention, his trial is still ongoing.

Section 25 of the Computer Misuse Act states, "Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor." A conviction attracts a fine not exceeding Uganda Shillings 480,000 (US$140), imprisonment not exceeding one year, or both.

In January 2016 Uganda Police arrested Charles Rwomushana, a former intelligence officer, on allegations of publishing false information. He had reportedly published photos of a dead person claiming it was the aide of former presidential candidate Amama Mbabazi. Rwomushana's arrest was followed by the arrest of two editors of the Red Pepper who picked photos from Rwomushana's Facebook account and published them.

In March 2016, the Military High Court in Rwanda sentenced two soldiers - Col Tom Byabagamba to 21 years in jail and Brig Gen (rtd) Frank Rusagara to 20-years in jail, after they were both found guilty of tarnishing the image of the country, among others. For Rusagara, it was stated that on several occasions he circulated material, mainly through his email, most of which propaganda based on mere rumors, with an aim of tarnishing the image of the state.[72] During the hearings, the military prosecution displayed messages that the former general shared using his emails.

In July 2012 the popular Ethiopian blogger Eskinder Nega, was jailed for 18 years on charges of attempting to incite violence through his blog posts. Similarly, six bloggers of the prominent Zone 9 blogging collective were arrested in April 2014 and charged with terrorism in July 2014; two of the bloggers were released and acquitted in July 2015, joined by the four others in October 2015[73] but they are back on trial after the state appealed the acquittal.[74]

In Zambia in 2013 two freelance journalists Wilson Pondamali and Thomas Zgambo and media trainer Clayson Hamasaka were arrested for alleged links to the independent website Zambian Watchdog though they were later slapped with different charges. All three separate arrest incidents were characterised with early morning raids of their homes, computers and data storage devices being confiscated while the trio were in detention.[75] Zgambo and Hamasaka were charged for forgery and possession of obscene content. Hamsaka was acquitted of the charges after two years at trial.[76]

*68. Interview with ZLHR lawyer TM, conducted on 11 June 2016*
*69. Interview with legal practitioner, Otto Saki conducted on 12 June 2016.*
*70. CIPESA, Hunting Down Social Media 'Abusers' in Uganda as Elections Near, http://www.cipesa.org/?wpfb_dl=190*
*71. Ibid*
*72. Rodrigue Rwirahira, Byabagamba, Rusagara get lengthy jail terms, The New Times, http://www.newtimes.co.rw/section/article/2016-04-01/198556/*
*73. Electronic Frontier Foundation (2015). Update: Zone 9 bloggers acquitted!, October 19, 2015, https://www.eff.org/offline/zone-9-bloggers*
*74. Ethiopia's Zone9 Bloggers go Back to Court, https://advox.globalvoices.org/2016/03/30/netizen-report-ethiopias-zone9-bloggers-go-back-to-court/*
*75. Zambian Journalist Charged with Sedition, https://advox.globalvoices.org/2013/07/11/zambianjournalist-charged-with-sedition/*
*76. Journalist Clayson Hamasaka acquitted, evidence was planted, August 11, 2015,*

Despite the fact that Intermediaries are not tasked with the role of policing content, they still play a crucial role in access and content distribution as they have to abide by the laws of the countries in which they are registered for their operation. According to Google's Transparency Report,[77] there has been only one content takedown request from Kenya in the period of June 2014 and June 2015. The request was in form of a court order on behalf of Kenya Internet Solution to delist an item from its search engine alleged to be defamatory. The company responded with 100% compliance. Further, during the same period Kenya has been one of the two African countries that have sent removal requests[78] to Twitter; both of which got 0% compliance. Kenya did not request for user information in the second half of 2015.[79] However, it made five requests in the first half of 2015 and the intermediary released data from one account, indicating 20% compliance.

The two transparency reports released by Vodafone[80] (whose Kenyan operator is Safaricom) have failed to disclose data requests or content control by the government, stating that the laws on whether to release such data are unclear. Vodafone owns 40% of Safaricom shares,[81] and currently holds the largest market share in mobile telephone and data services. Airtel Kenya, has never released any data on government requests.

*77. Google transparency report: https://www.google.com/transparencyreport/removals/government/KE/?hl=en*
*78. Twitter transparency report, https://transparency.twitter.com/removal-requests/2015/jul-dec*
*79. Facebook transparency report, https://govtrequests.facebook.com/country/Kenya/2015-H1/#*
*80. Vodafone transparency report 2015,*
*http://www.vodafone.com/content/dam/vodafone-images/sustainability/downloads/vodafone_law_enforcement_disclosure_report_2015-4.pdf*
*81. Safaricom Sustainability Report https://www.safaricom.co.ke/sustainabilityreport_2015/stakeholder-engagement/shareholder/*

## 4.3 The Extent of Online Surveillance is Unknown

Online surveillance is one of the threats to universal access to the internet, and yet many African governments are outdoing themselves in acquiring state of the art software that will enable them eavesdrop on their citizens. While databases and CCTV still exist and are in use, the most recent discussions around mass surveillance focus around the monitoring of communications, including what we do on our phones and our computers.[82] When it comes to spying on citizens' phones, government authorities can now get access to data on virtually everyone within a specific geographic area around a cell tower through bulk access to data held by mobile phone companies. There is also an increase in the use of mobile surveillance tools that allow authorities to monitor all communications and identify all devices within a localised area[83], for instance at a public protest by setting up fake mobile base stations.[84]

In Africa, Ethiopia maintains a tight control over internet access, with the state-owned Ethio Telecom maintaining a monopoly on telecommunications and a keeping costs of access high, as the country is ranked among the most expensive for internet users.[85] The government has also been accused of deploying spyware and other hacking and surveillance tools to snoop on bloggers, journalists, members of the opposition and other critical individuals.[86] Journalists, bloggers and other human rights activists are regularly arrested and imprisoned over their online communications.

In October 2015, it was reported that the Ugandan government had acquired surveillance technology, which the government was to use to "crush and blackmail opponents of the president".[87] The report by Privacy International details how the government allegedly purchased the intrusion malware FinFisher by Gamma International GmbH ('Gamma'), and how this technology was the backbone of a secret operation to spy on leading opposition members, activists, elected officials, intelligence insiders and journalists following the 2011 election.[88] The government vehemently denied those allegations and there has been no independent verification by OpenNet Africa of their veracity. Nonetheless, Wikileaks files last year also showed there were negotiations between Uganda government officials and Hacking Team for purchase of its surveillance software.

In the Democratic Republic of Congo, the government is using external expertise to reinforce its citizen surveillance program.[89] It has been said that intelligence agents and informants monitor a number of social media profiles of journalists, activists, and politicians. Some sources suspect the government uses mass surveillance tools such as RANDOM,[90] which records the traffic of telecommunications companies, and SWITCH[91], which is used for social media monitoring. In their 2015 transparency report on "Freedom of Expression and Respect of Privacy," telecom provider Orange state their position by pointing out that, "Our general process with regards to shut downs or blockages is clear. We require a written request (signed by a recognised authority) and based on local legislation. When any request is against the law, we reserve the right to alert the international community…"[92] In the same report, Orange reported having received 385 requests from the Congolese government for customers' data.[93]

*82. Mass Surveillance, https://www.privacyinternational.org/node/52*
*83. Ibid*
*84. Someone Sent a Mysterious Mass Text to Protestors in Kiev, http://mashable.com/2014/01/21/kiev-protesters-text-message/#kL9Wi88XkSq4*
*85. Ethiopia Ranked the Most Expensive Country for Internet Users, http://www.addisinsight.com/2016/04/12/ethiopia-ranked-expensive-country-internet-users/*
*86. The Tragedy of Ethiopia's Internet, http://motherboard.vice.com/read/the-tragedy-of-ethiopias-internet*
*87. UK's Firm Surveillance Kit Used to Crash Uganda Opposition, http://www.bbc.com/news/uk-34529237*
*88. Uganda's Grand Ambition of Secret Surveillance, https://www.privacyinternational.org/node/656*
*89. Desc Wondo, http://desc-wondo.org/fr/rdc-falcon-eye-un-dispositif-securitaire-de-videosurveillance-inefficace-jj-wondo/*
*90. Desc Wondo, http://desc-wondo.org/fr/a-linstar-de-la-nsa-kabila-deploie-ses-oreilles-electroniques-en-rdc-par-le-dispositif-random-desc/.*
*91. Desc Wondo, http://desc-wondo.org/fr/les-manifestations-du-26-mai-2016-comment-le-regime-de-kabila-se-prepare-a-contrer-lopposition-jj-wondo/.*
*92. http://www.orange.com/fr/content/download/37558/1150685/version/1/file/Rapport+de+transparence+liberté+d'expression+données+2015+V3.pdf.*
*93. Orange, transparency report on freedom of expression and privacy protection Year 2015, http://www.orange.com/en/content/download/37558/1150696/version/2/file/Transparency+report+on+freedom+of+speach+and+privacy.pdf*

On February 25, 2015, Congolese opposition leaders Franck Diongo and Jean Claude Vuemba filed a complaint against the National Intelligence Agency (ANR) for blocking their phone numbers for more than four months.[94] Diongo claimed that telecommunication companies produced a letter from the ANR directing that their phone numbers as well as the phone numbers of four other opposition leaders – Samy Badibanga, Fidèle Babala, Delly Sessanga, and José Makila – be blocked for months.[95] It was also reported that as the opposition was preparing for a mass protest in March 2016 to request an electoral calendar, security services were also gearing up for mass surveillance. According to information from President Joseph Kabila's inner circle, the ANR prepared to monitor social media posts and started intercepting mobile communications of various politicians and civil society leaders.[96]

In Zambia, two individuals sued Airtel for divulging to third parties text messages that were sent through their networks. The two claimed that the mobile company tapped their phone conversations as well as that of other opposition MPs and handed them over to government. The two cite section 64 of the Electronic and Communication Transactions Act,[97] which states that a person shall not intercept, attempt to intercept or procure another person to intercept or attempt to intercept, any communication. It also prohibits the use of electronic or mechanical device to intercept any communication. Meanwhile reports of the Zambia government purchasing surveillance technology from China emerged in 2013, and in 2015 leaked emails revealed government could have purchased Remote Control System (RCS) spyware from the Hacking Team company.[98] In August 2016, reports of internet connectivity interruptions were reported during the election period but these were not concretely verified.[99]

In Tanzania, the US State Department Human Rights Report of 2014 noted that state actors used to monitor telephones and correspondence of some citizens and foreign residents. Again, the actual nature and extent of this practice were unknown".[100] There is speculation amongst citizens that government conducts surveillance of communications over social media platforms such as WhatsApp especially of individuals spreading "false", "defamatory" or "insulting" statements against government or the president. In a recent incident, a message allegedly from the communications regulator demands that the owner of a particular phone number surrenders to the police on allegations that his/her number was used to spread false and defamatory statements against the president.[101] In another case, the Member of Parliament (MP) for Arusha (CHADEMA), Godbless Lema, was arrested and reprimanded by the police on allegations of publishing online statements which were construed as incitement.[102] Such incidents have instilled fear among citizens that the government is monitoring their activities online and consequently people are not free to express their views fearing the merciless hand of the authorities.

In September 2015, the Tanzania Human Rights Defenders Coalition (THRDC) filed a landmark case challenging the constitutionality of some of the provisions of the Cyber Crime Act. THRDC argues that some provisions of the law infringe Articles of the Constitution on freedom of expression, right to information, and privacy.[103] To date, a decision in the case remains pending.[104]

Meanwhile, the popular online forum Jamii Media, after being issued with eight letters by Tanzanian police demanding the disclosure of the IP address of users, went to court on April 2016 to challenge these acts by the law enforcement agency. The users whose identities authorities sought were linked to bringing to light corruption scandals in the oil and banking sectors. According to legal representatives of Jamii Media, the disclosure notices indicate a bias towards protecting notable figures implicated in the scandals or against whom users have used profanities.[105]

*94. Congo Independent, http://www.congoindependant.com/article.php?articleid=10367.*
*95. Radio Okapi, http://www.radiookapi.net/actualite/2015/02/19/kinshasa-les-numeros-de-telephone-de-certains-opposants-coupes-depuis-un-mois/.*
*96. Desc Wondo, http://desc-wondo.org/fr/les-manifestations-du-26-mai-2016-comment-le-regime-de-kabila-se-prepare-a-contrer-lopposition-jj-wondo/.*
*97. Electronic and Communication Transactions Act, No. 21 of 2009*
*98. Freedom House, 2015. Freedom On the Net Zambia Report, https://freedomhouse.org/report/freedom-net/2015/Zambia*
*99. Internet outage reported in parts of Zambia, Tech Trends, August 18, 2016, http://www.techtrends.co.zm/internet-outage/*
*100. US State Department, Tanzania 2014 Human Rights Report, Available athttp://www.state.gov/documents/organization/236626.pdf as accessed on 20th July 2016.*
*101. This message was shared in various social medias such as Whatsapp, Instagram and Facebook.*
*102. Read more at http://www.tanzaniatoday.co.tz/news/lema-akamatwa-na-polisi as accessed on 29th August 2016.*
*103. THRDC Progressive Report 2015*
*104. Interview with Advocate Jebra Kambole*
*105. Interview with the Jamii Media Attorney.*

In its petition, Jamii Media challenged the arbitrary letters from the police force and specifically the provisions of Section 32 and 38 of the Cybercrime Act that might infringe the right to be heard, privacy and freedom of expression as provided for under the Constitution. Initially, the Government responded by raising six preliminary points of objections against the petition filed by Jamii Media. The Government argued, among others, that the petition was frivolous and vexatious and that it ought to be struck out. The Government stated that Jamii Media should explore other remedies rather than to file for a constitutional petition. In a recent ruling regarding these preliminary objections, all six objectives were overruled and therefore the main case will continue.[106]

According to emails released by WikiLeaks, Hacking Team exchanged communications with representatives from the Tanzanian President's Office.[107] An email from the government representative expressed interest in visiting Hacking Team's office with a view of purchasing its Galileo surveillance system.[108] This surveillance technology has the ability to bypass encryption, take control of a user's device and monitor all activities conducted on the device.

*106. See more at http://www.jamiiforums.com/threads/jamiiforums-yashinda-mapingamizi-yaliyowekwa-na-ofisi-ya-mwanasheria-mkuu-wa-serikali-ag.1101852/*
*107. Wikileaks, https://wikileaks.org/hackingteam/emails/emailid/11776*
*108. Galileo is a remote control system which allows to take control of a target and to monitor them even if they are using encryption. Hacking Team sells it as a tool to "bypass encryption, collect relevant data out of any device, and keep monitoring your targets wherever they are, even outside your monitoring domain." For more information: https://www.hackingteam.it/images/stories/galileo.pdf*

## 4.4 Continuous Blockages of Online Sites

Ordering website blocking and SMS blocking have been one of the oldest control measures used in Africa. Ethiopia and Rwanda have over the years been the big boys of website blocking. They still are – with Ethiopia the 'leader' by far. While a number of websites can still not be accessed in the two countries after authorities ordered for their blocking, this system is not as popular in some of the other countries studied. That is not to say it is non-existent.

In Ethiopia, the government has for years ordered access to hundreds of websites to be blocked. Tests conducted in September 2016 by OpenNet Africa researchers confirmed that hundreds of these websites can still not be accessed from within the country. Among the websites and social media accounts blocked are those of opposition groups including Ethiopian Current Affairs Discussion Forum/ (http://ecadforum.com/), Patriotic Ginbot 7 Movement for Unity and Democracy (http://www.patriotg7.org), Ethiopian's People Congress for United Struggle (http://www.ethioshengo.org/), Ethiopian People's Revolutionary Party (http://www.eprp.com), Blue Opposition Party (https://www.facebook.com/semayawiethi) and Oromo Liberation Front (http://oromoliberationfront.org). Several news sites, blogs and advocacy organisations websites such as http://www.defendethiopians.org for Global Alliance for the Rights of Ethiopians and http://www.solidaritymovement.org for Solidarity Movement for a New Ethiopia are also blocked.

In Rwanda, the websites blocked are mostly critical online newspapers and websites of opposition groups. For some of the newspapers sites that are blocked, their editors were charged in court over publishing material considered defamatory,[109] endangering national security or genocide denial [110] and got sentenced or many fled into exile. In the cases which have been adjudicated publically, the blockage of the websites was ordered by court of the press ombudsman.[111] But not all blockages or other attacks on critical websites have been issued through transparent, legal, or known processes. For example, John Williams Ntwali, the owner of www.ireme.net, and www.ireme.org, one of the few independent and critical websites whose publisher is still living in Rwanda, has had its websites maliciously put down by what he think are state agents.[112] As recently as August 2016, the local language website of Great Lakes Voice was blocked by authorities, according to various sources that spoke to OpenNet Africa.

In DRC, websites such as www.desc-wondo.org and www.vacradio.com, critical of government activities and owned by individuals sympathetic to the opposition, were recently blocked. On March 25, 2016, Jean Jacques Wondo, owner of a website publishing political, geostrategic, and security analyses on current affairs in the DRC, received complaints from his readers in the DRC who were not able to access his content. No government department or institution claimed responsibility for blocking it.[113] Similarly, the same incident happened to the Voice of Africa in Canada (VAC) radio station, a website managed by Congolese in the diaspora, well known for its critical voice against the DRC government. On March 27, 2016, its co-founder, Coralie Kienge, announced that his website was not accessible in the DRC.[114] Currently, both websites are accessible in the DRC. However, we were unable to establish how long the blockages lasted.

In Somalia, the internet is essentially unregulated. However, in February 2016, ISPs blocked 29 websites critical of the government, following a November 2015 order from the federal government's Attorney General to the Ministry of Information and the Ministry of Communication to suspend 35 news websites accused of publishing anti-government propaganda and ignoring journalistic ethics.[115]

*109 Rwanda Journalist Found Guilty on Defamation Charges, https://www.article19.org/resources.php/resource/37871/en/rwanda:-journalist-found-guilty-on-defamation-charges*
*110. Jailed Rwandan Editors Turn to African Commission, https://cpj.org/blog/2012/12/jailed-rwandan-editors-turn-to-african-commission.php*
*111. Rwanda Independent Website Blocked Prior to Elections, http://www.fesmedia-africa.org/what-is-news/statements-developments/news/article/rwanda-independent-website-blocked-prior-to-elections/*
*112. Rwanda News Website Ireme Latest to be Blocked, http://greatlakesvoice.com/rwanda-news-website-ireme-latest-to-be-blocked/*
*113. Jean-Jacques Wondo Facebook<https://www.facebook.com/jeanjacques.wondo/posts/10209219986635589>*
*114. VAC Radio Twitter Page: <https://twitter.com/vac_radio/status/714198579901034496>*
*115. Somali Attorney General orders the suspension of 35 Somali news websites Over allegations of Ethics http://www.radiodalsan.com/2015/11/09/somali-attorney-general-orders-the-suspension-of-35-somali-news-websites-over-allegations-of-ethics/*

The ISPs reportedly declined to block access to six websites connected to Al Shabaab, as the authorities were not able to guarantee their security from possible retaliation.[116] [117] According to the UN, some ISP staff were arrested and released after 24 hours after promising to comply, and the Attorney-General warned that non-compliance would be considered an act of treason. As of September 11, 2016, the websites could not be accessed within Somalia.

On April 19, 2014, a court in the breakaway region of Somaliland ordered telecom companies to block the news websites of two prominent newspapers (Haatuf and Somaliland Times) for allegedly insulting government officials.[118] Continuing the tradition where regional authorities order website blocking, in October 2014, Golis Telecom in the semi-autonomous region of Puntland blocked five news websites.[119] The websites, including Puntlandtoday.com, Galgalanews.com, Puntlandnow.com, Jidbaale.com and Xaysimo.com had been restricted by the telecom company following an order from Puntland presidential palace's communication office without any court ruling as cited.[120]

Zambian Watchdog and Zambia Reports, popular sites that published content critical of government, were inaccessible in the country at different intervals between 2012 and 2014 with fingers pointed at government. The Zambia Watchdog domain name remains blocked, and is only accessible through proxies. But ISP officials told OpenNet Africa that they had blocked the website on instructions of the communications regulator. However, Zamtel Director Mpanga Mwanakatwe denied they had blocked the site although it is not accessible through his network. Zambian Watchdog publishers say in July 2013 the site was attacked using denial of service using Optima/Darkness DDoS botnet. The attack caused inaccessibility to the news site for close to eight hours. The international company which hosts the Watchdog and other news websites said this had been the most complex attack that they had seen in size and complexity.

In May 2013, the National Communication Council (CNC), Burundi's media regulator, ordered the Iwacu press group to prevent visitors to its website (www.iwacu-burundi.org) from posting comments for the next 30 days. In justifying its actions, the CNC's chairperson Pierre Bambasi was quoted as saying, "We cannot have individuals or groups screaming abuse on the internet, stirring up ethnic hatred, talking of taking up arms and urging the people to rise up."[121] Articles 10 of the 2003 law, under which Iwacu was sanctioned, prohibited journalists from publishing any information prejudicial to national unity, public security, morality, and national sovereignty.

Not to be left out of the party, the Al Shabab banned mobile internet in South/Central Somalia in January 2014, after the US and its allies increased targeted assassinations against the group's senior commanders. The Al Shabaab feared the US and its allies were using mobile Internet to locate their GPS in carrying out such attacks. The rebel group made the announcement during a broadcast on January 9 by a radio station affiliated with the group, and in a statement issued to local media. "Any individual or company that is found not following the order will be considered to be working with the enemy and they will be dealt with in accordance to Sharia law," the statement read.

In January 2016, Tanzania's government ordered Mawio newspaper's website to cease operation immediately following a ban on the newspaper.[122] The action was taken under the provisions of section 25(1) of the Newspaper Act, 1976 on grounds that the newspaper was publishing inciting news. The statement issued by the Minister of Information, Sports and Culture did not provide specific details on the content which led to the banning the newspaper.[123]

*116. Report on the Right to Freedom of Expression: Striving to Widen Democratic Space in Somalia's Political Transition, August 2016, http://www.ohchr.org/Documents/Countries/SO/UNSOM_FreedomExpressionReport_Aug312016.pdf*
*117. Internet Censorship in Somalia: Blocking websites is a threat to the free speech, http://waagacusub.net/articles/1166/Internet-Censorship-in-Somalia-Blocking-websites-is-a-threat-to-the-free-speech*
*118. Somalicurrent, a news portal based in Minneapolis also reported http://www.somalicurrent.com/2014/04/19/internet-providers-in-somaliland-ordered-to-block-haatuf-websites/*
*119. Garowe Online: http://www.garoweonline.com/en/news/press-releases/somalia-media-association-of-punt-land-condemns-telecom-companys-blocking-of-5-websites*
*120. Media Association for Puntland (MAP) is a journalist association that represents the media and the journalists in Puntland reported on January 20, 2015. http://mediapuntland.org/media-association-of-puntland-condemns-telecom-companys-blocking-of-5-websites/*
*121. Burundi - Media regulator suspends comments on press group's website, http://www.trust.org/item/20130531164503-qium7/?source%20=%20hppartner*
*122. Government Bans Mawio, Suspends 27 Stations, http://www.thecitizen.co.tz/News/Govt-bans--Mawio---suspends-27-stations/1840340-3037140-u46k0qz/index.html*
*123. Visit http://mwanahalisionline.com/gazeti-la-mawio-lafungiwa-maisha/*

In Kenya, research by the Tor Project on internet censorship has found no evidence that the country had recently experienced any intentional website blocking by the government or any other institutions.[124] However, it was reported that the Kenya government has in the past made requests to private companies to block access to websites by launching cyber-attacks. It is alleged that the Kenyan Government had made a request to a local communications company selling pay TV to bring down an activists website which had news content highlighting corruption and other wrong doings by the government.[125] The team turned down the requests stating that it was against the company policy and international regulations to deal directly with law enforcements.

Although the Kenya government is not seen to be active in online content censorship, one of our key respondents commented that it has never been shy making internet filtering requests to private companies. The requests allegedly come from various government departments and institutions. According to some knowledgeable sources, previously, the challenge with interception was that it was being done without following due process. However, and increasingly, service providers have begun challenging information requests, and insisting on court orders to provide information or to allow interception. What is important to note is that in their terms and conditions of service, Safaricom for example, indicates that it will retain and share information with law enforcement if so required for the prevention of fraud, or in respect of legal proceedings or in compliance with legal, regulatory or governmental requirement.[126]

*124. https://explorer.ooni.torproject.org/country/KE*
*125. www.nation.co.ke/news/politics/Italians-reject-bid-to-close-Kahawa-Tungu/1064-2786990-72vi9ez/index.html*
*126. Safaricom terms and conditions for post pay service*
*http://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/safaricom_advantage_plus_final_publication.pdf*

## 4.5 Online Content Removals

While blockages of specific content are significant, states also engage in online content removal, an issue that remains quite unclear. Between 2013 and 2014, Zimbabwean government authorities and opposition leaders frequently pressured users and content producers to delete content from social media platforms during the coverage period, reflecting a growing trend compared to previous years.

Most notably, the Facebook page of the anonymous whistleblower Baba Jukwa[127] was deleted in July 2014, though the manner in which it was removed remains mysterious. Baba Jukwa, believed to be a mole within or connected to the ruling party, Zanu PF - as a pseudonymous Facebook page was posting allegations of scandals and corruption, mainly against politicians and state officials. 'He' also made predictions of what was going to happen within the political landscape and within the ruling party, many of which turned out to be true.

It is believed that in late 2014, the government reportedly went out of its way to locate the person(s) behind Baba Jukwa, including sending some officials to the United States to try and liaise directly with Facebook and convince the company to delete the page, which at the time, had close to half a million followers.[128] In previous years, it is believed that the government had also reportedly sought Chinese technical assistance in censoring the page and identifying its owner.[129] Some believe that the authorities eventually just managed to hack into and take control of the Baba Jukwa page to delete the profile. Whatever the case, the page was ultimately taken down in July 2014,[130] after an editor at the state owned Sunday Mail newspaper, Edmund Kudzayi, was arrested in June on accusations of running the Baba Jukwa account[131] with the intention of subverting the government through waging what was termed as 'cyber-terrorism'.

Kudzayi was released on USD $5,200 bail about two weeks later, sparking speculation that he had just been used as a scapegoat in a 'serious head-scratching' situation.[132] However, he lost his job at the Sunday Mail. There is wide belief that 'Baba Jukwa' was not actually one person but rather a small network of disgruntled individuals collectively providing intel on the page.[133]

Popular Movement for Democratic Change (MDC) opposition party leader, Morgan Tsvangirai in May 2015 ordered that all Whatsapp and Facebook groups administered by any members of his party be shut down or the members would be suspended.[134] Following the ban, the MDC party reportedly suspended five of its officials based in Zimbabwe's second largest city Bulawayo on May 10, 2015 for allegedly 'abusing social media platforms to attack the party's top leadership.'[135] Interestingly, the Zimbabwe government currently does not censor any specific sites or content. However, there have been other strategies employed to limit freedom of expression online.

*127. - Facebook Politics in Zimbabwe, http://africasacountry.com/2014/07/facebook-politics-in-zimbabwe-who-is-baba-jukwa*
*128. Tendai Rupapa, "Baba Jukwa investigators in US," Chronicle, September 2, 2014, http://bit.ly/1QBh73O. Cited in Freedom House, Zimbabwe Freedom on the Net 2015.*
*129. Jane Flanagan, "Mugabe hunts for internet mole 'Baba Jukwa' revealing his secrets," The Telegraph, July 4, 2013, http://bit.ly/1QBhb3L. Cited in Freedom House, Zimbabwe Freedom on the Net 2015.*
*130. Adam Taylor, "Has Baba Jukwa, Zimbabwe's infamous anonymous whistleblower, really been caught?" Washington Post, June 25, 2014, http://wapo.st/1KetzRG. Cited in Freedom House, Zimbabwe Freedom on the Net 2015.*
*131. Charles Laiton, "Sunday Mail Editor 'is Baba Jukwa," The Standard, June 22, 2014, http://bit.ly/1Lyv02G. Cited in Freedom House, Zimbabwe Freedom on the Net 2015.*
*132. Interview with journalist working in the private media held on 23 June 2016.*
*133 Baba Jukwa Speaks to Nehanda Radio, http://nehandaradio.com/2014/08/01/baba-jukwa-speaks-to-nehanda-radio*
*134. Gift Chirauro, "Is banning social media good for MDC," Techno Mag, February 10, 2015, http://bit.ly/1NNa6PT Cited in Freedom House, Zimbabwe Freedom on the Net 2015.*
*135. Luyanduhlobo Makwati, "MDC-T suspends officials for abusing social media," Southern Eye, May 10, 2015, http://bit.ly/1LSORfd. Cited in Freedom House, Zimbabwe Freedom on the Net 2015.*

Following the developments with the #ShutDownZimbabwe2016 protests, a number of things happened that not only showed the government's panic, but indicated possible things to come. On the day of the stay away, the government, through POTRAZ, issued a veiled threat through a public notice in the press.[136] The notice stipulated that people who were deemed to be sharing 'abusive and subversive materials' would be 'disconnected…arrested and dealt with accordingly in the national interest.' The public notice went on to warn further that '…all sim cards in Zimbabwe are registered in the name of the user. Perpetrators can easily be identified.' Following this notice, some sections of social media users now sincerely believe that the government has the capability to intercept and decrypt WhatsApp message. Also, what is worrying about this notice is the vagueness of what constitutes 'abuse' of social media.

In August 2016, the Army Commander General Constantino Chiwenga declared[137] in a press conference, that events happening on social media had 'serious potential to disturb the peace' and therefore the full wrath of the law would be applied.

The state media also turned up its propaganda machinery when on the morning of August 9, 2016 Zimbabweans woke up to a shocking top story headline in the Herald that read: "Social media terrorists exposed".[138] This marked the possible start of a more targeted clampdown on social media users perceived as troublemakers. Some critics believe that these trumped up accusations of social media abuse against few scapegoats [139] is intended to justify the stringent social media regulation laws that the government is expected to release soon. The 'social media terrorists' were three Zimbabweans fingered in the government's latest 'cyber-terrorism probe' whose preliminary findings unearthed 'subversive and inflammatory' messages allegedly originated by them.

*136. Here's the Zimbabwean government's warning against social media abuse. July 2016, http://www.techzim.co.zw/2016/07/heres-zimbabwean-governments-warning-social-media-abuse/#.V4jc5o6zDaY>*
*137 ZDF Stand by President Says General Chiwenga, http://www.herald.co.zw/zdf-stand-by-president-says-general-chiwenga*
*138. Social Media Terrorists Exposed, http://www.herald.co.zw/social-media-terrorists-exposed*
*139. One of the accused so-called social media terrorists (@rimbe_t) has not posted a Tweet in over a year. The article also does not stipulate which laws these 'terrorists' broke.*

# 5.0 Conclusions and Recommendations

It is clear that governments in Africa are employing different means and strategies to curtail peoples' rights in the digital sphere. There has been rising clampdown on the internet through retrogressive provisions in laws, which have facilitated arrests of users against whom various offences are brought in the different countries.

Internet shutdowns appear to be becoming the most preferred control mechanism that African governments are using to curtail the right to freedom of expression and access to information online. The shutdowns are effected through orders to ISPs to block access to either selected services (such as Facebook, Whatsapp, Twitter and mobile money services), or a total obstruction of access to the entire internet

There is also a marked increase in the number of arrests, and the charging of journalists, media houses and human rights activists for online related offences. Majority of the legal provisions used are less than 10 years old, although there are also instances of laws dating back more than four decades being used, especially in countries with no specific laws or policies governing online communication.

Some African governments are investing in hiring high tech and media survey personnel to drive their propaganda campaigns. They are actively pushing out information on social media and other platforms, intimidating critical social media users, swamping discussion forums with their disinformation, and using bots to dominate Twitter conversations, at the expense of honest conversations on issues of public interest.

## 5.1 Recommendations

### a) Government

- African governments must respect human rights online and ensure that all measures, whether legal, policy or administrative, comply with the constitution and generally accepted human rights standards stipulated in Africa-wide and international human rights instruments.

- African governments should train officials to appreciate that the rights to freedom of expression, access to information and privacy are fundamental human rights that are provided for in their respective constitutions and that they should only be limited by express legal provisions.

- African governments should seek to amend all retrogressive legislations, such as the Cybercrimes Act 2015 (Tanzania); the Criminal code of- ProclamationNo.414/2004, Anti-Terrorism Proclamation-Proclamation No. 652/2009, and Telecom Fraud Offence Proclamation-Proclamation No. 761/2012 (Ethiopia), among others, and pass legislations that promote and protect fundamental human rights online.

- The laws providing for interception of communication for the purpose of investigation such as the Regulations of Interception of Communications Act 2012 (Uganda); Security Laws (Amendment) Act 2014 (Kenya); the 2008 Interception of Communications law (Rwanda) should be amended to ensure that there is transparency in the procedure of applying for authorisation and implementation. Again, the circumstances under which interception is warranted should be narrowed to only those which pose justifiable threat to national security or peace.

- Governments should, through a consultative process, draft and pass Data Protection laws that will guarantee privacy of citizens' information and offer legal recourse to citizens when their data is illegally accessed or compromised.

- There is value in adopting multi-stakeholder approaches: in the design of policies and strategies regarding the internet, it is key to recognise the importance of multi-stakeholder approaches, as well as ensuring broad and diverse consultation with and participation of civil society and other actors working in the public interest. Such actors bring to the table concrete human rights and civil liberties concerns that should be considered at the inception of any Internet related policy effort.

## b) Civil Society

- Civil Society should continue to strongly advocate for internet freedoms in law and in practice in order to ensure the protection of the freedom of expression online, accessible and affordable internet, data protection and privacy.

- Civil society groups that have traditionally promoted human rights should embrace the online space and develop advocacy programs that promote human rights online.

- Civil society should engage in sustained sensitisation and awareness raising campaigns for users on the rights to privacy, freedom of expression particularly on social media, as well as on legislation that governs use of the internet and related technologies.

- Civil society should seek to build multi-stakeholder coalitions to lobby for the amendment of the draconian laws such as the Cybercrimes Act 2015 (Tanzania); the Criminal code of- ProclamationNo.414/2004, Anti-Terrorism Proclamation-Proclamation No. 652/2009, and Telecom Fraud Offence Proclamation-Proclamation No. 761/2012 (Ethiopia) among others, which threaten Internet freedom.

- Civil society actors should also endeavour to follow the progression of draft laws, make submissions and inputs to bills in order to ensure they uphold the principles of human rights prior to being tabled and passed by parliaments.

- Civil society actors should carry out campaigns against illegal surveillance and online attacks on government critics that are initiated by fake accounts.

- Civil society organisations and media should advocate for internet safety, educate and establish special legal advocacy desks.

## c) Media

- The online environment has affected the media industry as they have had to re-organise their operations and embrace the internet. The media industry should embrace and become active advocates for internet freedom by creating awareness and educating the public on policy engagement processes.
- The media being the fourth estate should focus on the undue and abusive practices of government in regard to internet governance issues. There is a capacity gap within the media that needs to be addressed through training to empower the press and to shed light on problematic legislations and processes relating to Internet use.
- Media outlets should invest in educating the masses on existing legislation and create a space for discussion about these issues.
- The media should also partner with the government and the private sector to create special educational programs on trending issues touching on internet freedom.
- Where possible, the media should also collaborate with other stakeholders and seek solutions to current issues that pose a threat to freedom of expression and restrict civil liberties.

## d) Telecom companies and ISPs

- Telecom companies and other ISPs should protect the privacy of their subscribers, and only share their private communications data on the strength of a court order.
- In case of government requests for user data, telecoms and ISPs, as well as intermediaries such as Facebook and Google, should publish details of these requests, providing details including numbers, information given for the requests and action taken by the telecom/ISP/ intermediary.
- Telecom companies and ISPs should challenge shut-down directives from governments in courts of law, including seeking redress from regional and international jurisdictions in case local courts can not be trusted.
- Private entities should integrate strong commitments to freedom of expression and the respect for users' right to privacy in internal policymaking and service agreement.


**Collaboration on International ICT Policy for East and Southern Africa (CIPESA)**
**156-158 Mutesa II Road, Ntinda, P.O Box 4365 Kampala, Uganda.**
**Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335**
**Email: programmes@cipesa.org**
**Twitter: @cipesaug**
**Facebook: facebook.com/cipesaug**
**www.cipesa.org**