State of Internet Freedom in Africa 2017

Intermediaries' Role In Advancing Internet Freedom: Challenges And Prospects

September 2017

CIPESA

CONTENTS

1.0 Introduction

Growing use of the internet and related technologies has provided new spaces for advancing the right to freedom of expression (FOE), promoted access to information, and spurred innovation and socio-economic growth in various African countries. Within Africa, internet penetration stands at 31.2% from the estimated 388 million internet users, which represents 10% of the total world internet users.[1]

However, the expanding civic space facilitated by the internet has not been welcome in all states, with some governments seeking to variously control this space. The actions by governments include, among others, the arrest, intimidation, prosecution and detention of critics; imposition of liability on internet intermediaries for not complying with information or surveillance requests; and censorship of content that they do not approve. As shown later in this report, such actions have often been at the expense of users' rights to privacy, expression and access to information.

On the other hand, states and intermediaries face challenges in tackling unlawful conduct online, such as violence against women, fake news, hate speech, child rights violations, and terrorism. While the internet should be free, open and secure for all to enjoy its benefits, where states and internet intermediaries have attempted to respond to these challenges, they have often undermined citizens' rights to free expression, privacy and the right of access to information. Moreover, many African countries lack adequate policies and laws to protect user's rights. Caught in the middle of these challenges are intermediaries, meaning the entities that enable the communication of information from one party to another.[2]

Internet intermediaries include internet search engines and portals (e.g. Google, Yahoo, Bing), internet service providers or ISPs (including network operators and mobile telecommunication providers), web hosting providers, social media platforms, and media houses that provide platforms where users can comment and blog. Such intermediaries bring together or facilitate transactions between third parties and the internet by giving access, hosting, transmitting, and indexing content, products and services originated by third parties on the internet or providing internet-based services to third parties.[3] It is important to note that the definition of internet intermediaries (hereinafter referred to as intermediaries) explicitly excludes content producers i.e. the people who create, generate, edit or maintain content such as text, videos and photos online, whether in websites, blogs or on social media platforms.

Intermediaries play a mediating role between producers of content and audiences. However, there have been concerns when intermediaries are held liable for the content of others. These include instances where intermediaries are encouraged to censor content they host or transmit in order to avoid liability, or intermediaries closing down the option of 'user generated content' out of fear of facing penalties or lawsuits. Such actions significantly reduce the space for free expression and access to information online.

1 *Internet Users in Africa, June 2017, Internet World Stats. http://www.internetworldstats.com/stats1.htm*

2 *Thomas F. Cotter. 2005. Some Observations on the Law and Economics of Intermediaries. Michigan State Law Review, Vol. 1, p. 2. (Washington & Lee Legal Studies Paper No. 2005-14). http://ssrn.com/abstract=822987*

3 *Karine Perset/OECD. March 2010. The Economic and Social Role of Internet Intermediaries. Paris, Organisation for Economic and Co-operation and Development, p. 9. (DSTI/ICCP(2009)9/FINAL.) www.oecd.org/internet/ieconomy/44949023.pdf*

'Intermediary liability' therefore arises when intermediaries are held legally responsible for content posted on their platform or transmitted using their infrastructure, instead of the individual producing, accessing, or sharing the content being held liable.

Different countries and intermediaries around the world continue to develop measures to regulate the use of the internet and associated technologies. It is important to understand the evolving approaches and practices in different African countries and draw lessons towards developing best practice for intermediaries to play a more positive role in advancing internet freedom. This report thus examines the legal, policy, institutional and practice landscape in 10 African countries, identifies in-country approaches to intermediary liability, and develops recommendations to reinforce internet freedom on the continent. The report pays special attention to internet shutdowns, surveillance, filtering and censorship, with regards to challenges such as hate speech, fake news, child and women rights, and terrorism.

The countries covered in the study are **Botswana, Burundi, Democratic Republic of Congo (DR Congo), Ghana, Kenya, Malawi, Tanzania, Uganda, Zambia** and **Zimbabwe**. These countries recognise the concept of intermediaries and define them in various ways with the common definition based on the role they play in giving access to, hosting, transmitting and indexing content originated by third parties or providing internet-based services to third parties. These activities include provision of internet access as service providers (ISPs), data processing and web hosting providers, internet search engines and portals, e-commerce platforms, internet payment systems, and social networking platforms.

Many of the countries studied have outdated legal and policy frameworks that regulate internet use. Some are experiencing a shrinking democratic space, commonly characterised by increasing interest by governments to control social media platforms.[4]

All countries under review are parties to a number of international, continental and regional instruments such as the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR) and African Charter on Human and Peoples' Rights (ACHPR) that guarantee freedom of expression, right to privacy, and the right to information. Further, national constitutions also provide for these rights. However, the implementation of these rights and guarantees especially on the internet, are at variance with best practice. The intermediaries on the other hand, have developed policies and practices that in some cases violate users' rights as opposed to safeguarding them. In this regard, specific gaps include transparency and accountability with respect to the retention and disclosure of user information and activity to authorities and third parties.

The report calls for greater protection of free expression, as well as the rights of access to information and privacy online. Intermediaries are particularly encouraged to be more proactive in safeguarding the rights of users, including by making user terms and conditions simpler and widely accessible; implementing measures to improve complaints handling; and ensuring transparency and accountability in how government requests for disclosure of users' information or content removal are handled. For civil society, it is recommended that interventions for monitoring human rights pay greater attention to violations on the internet. The academia are encouraged to conduct more research to inform advocacy, policy and legislative development, while the media is encouraged to profile and raise awareness on violation of human rights online.

4 *State of Internet Freedom in Africa 2016, Case Studies from Select Countries on Strategies African Governments Use to Stifle Citizens' Digital Rights, https://cipesa.org/?wpfb_dl=225*

2.0 Methodology

This study adopted a qualitative research methodology which involved the description of the country and sector contexts, followed by analysis of the legal and regulatory regimes in which the intermediaries operate, focusing on the period 2014 to 2017.

Researchers working in each of the focus countries conducted field work, including conducting interviews with key informants. Respondents included representatives of various intermediaries working in those countries, government, civil society organisations, technical community, academia, the legal fraternity, media and select individuals drawn from the general public conversant with the issues at hand. Desk research was also conducted to review media reports, academic works, legal and policy documents, and other literature.

The information obtained was thereafter analysed and compiled into the various country reports. The overall findings were further analysed and distilled into this regional report.

3.0 Country Contexts

3.1 Political Economy

By population, DR Congo is the largest of the countries studied with 81 million people, followed by Tanzania with 56.9 million. The smallest countries by population are Botswana and Burundi with populations of 2.3 million and 11.5 million respectively. On the economic front, the countries are at different levels of economic empowerment. According to the World Bank, as of 2016, Botswana had the highest GDP per capita at USD 16,734, followed by Ghana, Zambia and Kenya with USD 4,294, USD 3,922, and USD 3,155 respectively.[5] The countries with the lowest GDP per capita are Malawi, DR Congo and Burundi with USD 1,169, USD 800 and USD 778 respectively. According to the GSMA, the mobile industry in Sub-Saharan Africa is expected to contribute USD 142 billion to GDP by 2020, up from USD 110 billion in 2016.[6]

3.2 Political Environment

The political environment in any country has a bearing on the state of internet freedom and the operations of intermediaries. Elections on the continent remain highly contested, with several violations occurring during this during this period, including social media disruptions in some countries. In the last four years, elections in Malawi (May 2014), Burundi (July 2015), Tanzania (October 2015), Uganda (February 2016), Zambia (August 2016), and Kenya (August 2017), were conducted in politically tense environments, with the results disputed in most cases.

In DR Congo, elections earlier scheduled for November 2016 were postponed and no new date has been set. Earlier in January 2015, security forces launched a brutal crackdown to suppress public protests demanding timely elections, during which at least 40 people including a police officer were killed.[7] Meanwhile, Zimbabwe expects to hold its next election in July–August 2018, and it is likely to be contested given the current political circumstances, where the incumbent president Mugabe, 94, who has been in power for 30 years, may contest again amidst political wrangles over his succession.

Ghana continues to be a politically stable state and held its seventh successive peaceful general election in December 2016. Botswana, another multiparty democracy, in February 2017 saw the formation of a coalition to challenge the ruling party that has been in power since 1966, in the 2019 elections.[8]

5 *Comparison of GDP per capita, PPP (Current Int'l $), Bank, International Comparison Program database, https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD*

6 *The Mobile Economy, Sub-Saharan Africa 2017, GSMA, https://www.gsmaintelligence.com/research/?file=7bf3592e6d750144e58d9dcfac6adfab&download*

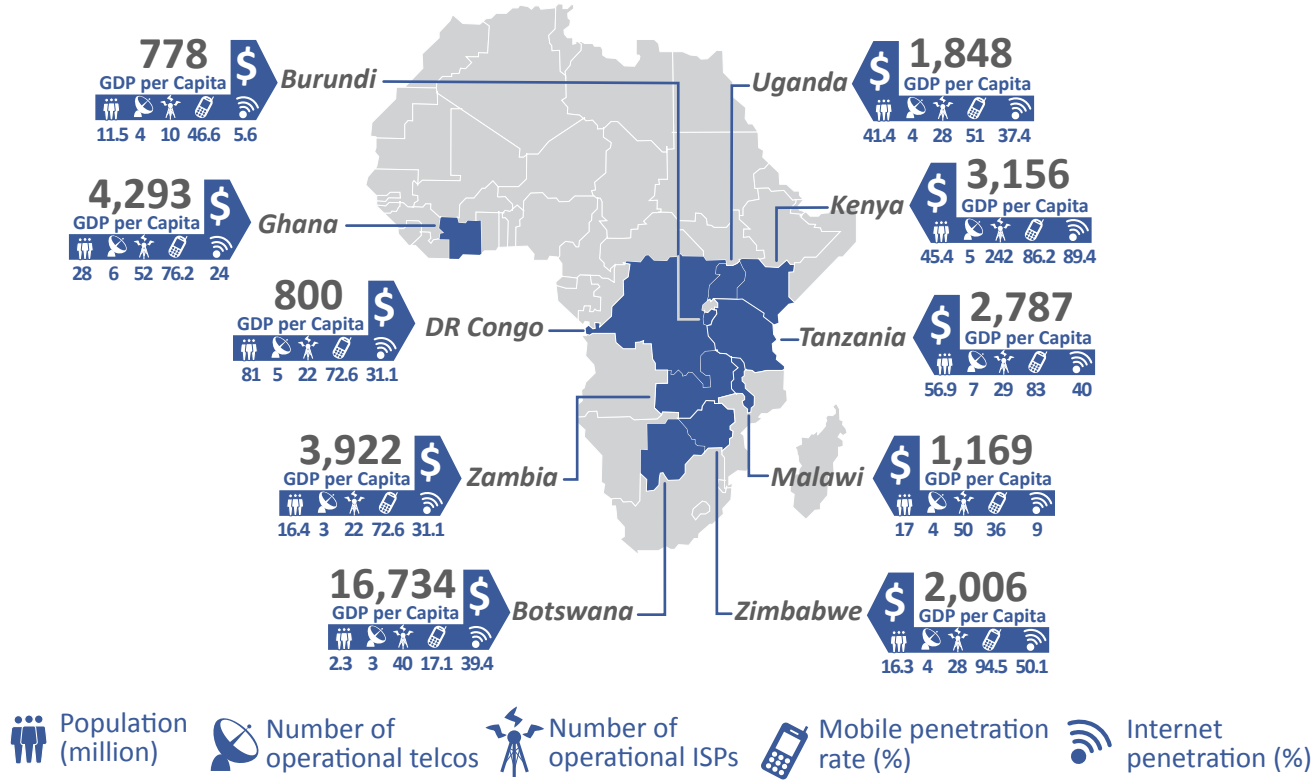
7 *"DR Congo: Deadly Crackdown on Protests," Human Rights Watch, 24 January 2015. https://www.hrw.org/news/2015/01/24/dr-congo-deadly-crackdown-protests*

8 *Botswana opposition groups unite to challenge ruling BDP, Reuters. http://www.reuters.com/article/us-botswana-politics/botswana-opposition-groups-unite-to-challenge-ruling-bdp-idUSKBN15I2JN*

3.3 ICT Status

Most of the countries had between three and seven operational telecommunication service providers. Tanzania had the most with seven, while Botswana and Zambia had three each. Kenya had the highest number of ISPs at 242.[9] Burundi had the least number of ISPs at 10. As with GDP, Botswana had the highest mobile penetration rate (171%),[10] followed by Zimbabwe (94%).[11] Malawi and Burundi had the lowest penetration rates at 36%[12] and 47%[13] respectively.

ICT Sector Statistics



In sharp contrast to mobile penetration, internet penetration in most of these countries remains low. Kenya recorded the highest level of internet penetration at 89%. DR Congo, Burundi and Malawi had the lowest levels of internet penetration at 4.2%, 5.6% and 9% respectively.[14] In Botswana, the high level of mobile penetration has not translated to greater internet access, which stands at 39.4%.

Cost is a key factor in access to the internet. Despite the low levels of internet penetration in Ghana and Tanzania, the price of a monthly 1GB prepaid data basket was lowest in these countries at USD2, according to Research ICT Africa.[15] On the other hand, Zimbabwe had the most expensive data bundles at USD30 per 1GB monthly basket yet the country recorded the second highest internet penetration rate at 50.1% (as per Table 1 above). This is unlike Kenya, where a 1GB basket costs a fraction of the price in Zimbabwe but internet penetration is nearly 90%.

9 *Sector Statistics, 2016/2017 (JANUARY-MARCH 2017), Communications Authority of Kenya. http://www.ca.go.ke/images/downloads/STATISTICS/SECTOR%20STATISTICS%20REPORT%20Q3%20FY%202016-2017.pdf*

10 *BOCRA (2016). BOCRA Annual Report. https://www.bocra.org.bw/sites/default/files/documents/BOCRA%20Annual%20Report%202016%20%28web%29.pdf*

11 *2017 first quarter Sector Performance Report, POTRAZ. http://www.techzim.co.zw/wp-content/uploads/2017/07/Mar-2017-Zimbabwe-telecoms-report-POTRAZ.pdf*

12 *National Survey on Access to and Usage of ICT Services in Malawi: http://www.macra.org.mw/wp-content/uploads/2016/01/MACRA-Survey-Report-National-Household-and-Individual-access-to-and-usage-of-ICT.pdf*

13 *Observatoire du Marche Internet/1 er Trimestre 2017, ARCT.http://arct.gov.bi/images/observatoiremarche/omi2017.pdf*

14 *Observatoire Du Marche Internet/1 Trimestre 2017, ARCT. See: http://arct.gov.bi/images/observatoiremarche/omi2017.pdf; BuddeComm, "Democratic Republic of Congo – Telecomms, Mobile and Broadband – Statistics and Analyses," https://www.budde.com.au/Research/Democratic-Republic-of-Congo-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses; and Internet World Stats, Malawi. See: http://www.internetworldstats.com/africa.htm#mw*

15 *Research ICT Africa, 2017, Cheapest price for 1GB basket in Africa by country, https://www.researchictafrica.net/pricing/ramp_1gb.php*

Nonetheless, telecommunication service providers such as Airtel, Orange and Safaricom have subsidised or zero-rated access to websites such as Wikipedia, and social media platforms such as Facebook, Twitter and WhatsApp.

Google.com and its country domains remain the most visited websites across the ten countries. Other popular sites include social networking sites YouTube, Facebook, Yahoo and Wikipedia. It is worth noting that these sites are global and not domiciled in the countries studied. However, consumers use them to access local and global content. It is therefore important to look into the manner in which companies that own these domains handle local users' data and respond to African governments' requests.

The most popular local sites mostly belong to media enterprises or e-commerce services. These include actualite.cd in DR Congo, jumia.com.gh in Ghana, nation.co.ke in Kenya, nyasatimes.com in Malawi, jamiiforusms.com in Tanzania, monitor.co.ug in Uganda, lusakatimes.com in Zambia, and the herald.co.zw in Zimbabwe.[16] On social media, accounts with the largest following included those run by media stations, telecommunication companies, politicians, religious leaders, business personalities and persons in the entertainment industry.

3.4 State Co-ownership of Network Operators and Infrastructure

Some governments in the countries studied have invested significantly in the telecoms sector, such as in national fibre optic cables, satellite stations, mobile networks and fixed telephone lines.[17] States also own and control the radio frequencies for mobile telephony, radio and TV broadcasting, and license the frequencies to operators.

Further, in some countries, governments own significant interests in the mobile network operators. Vodacom is one of Africa's leading communications companies with operations in South Africa, Tanzania, the DRC, Mozambique, Lesotho and Kenya. Vodafone owns 64.5% of the company, while the South African government, through the Public Investment Corporation (PIC), controls around 13.5% of the company.[18] In Botswana, the government owns a 51% stake in Botswana Telecommunications Company Limited (BTCL).[19] Onatel in Burundi, Zambia Telecommunications Company Limited (Zamtel), TTCL in Tanzania and Net*One Zimbabwe[20] are fully owned by government. The Ghanaian government owns a 30% stake in Vodafone Ghana following its sale of its shareholding in Ghana Telecom at a cost of US$900 million in 2008.[21] The Ghana National Petroleum Corporation, a state agency, owns 25% of Airtel Ghana. The Tanzanian government owns a 40% stake in Bharti Airtel Tanzania Ltd,[22] while the government of Zanzibar owns 15% of Zantel. The Kenyan government owns a 30% stake in Telkom Kenya[23] and a 35% stake in Safaricom Limited, the country's largest mobile operator.[24]

16 *Alexa.com, https://www.alexa.com/topsites/category/Regional/Africa*

17 *See for instance, Fiber Optic Social Network, "Tanzania to Expand Fiber Optic Networks", June 26, 2015, available at http://www.fomsn.com/fiber-optic-news/fiber/tanzania-to-expand-fiber-optic-networks/; TECHNOMAG, "Liquid Telecom Injects $32m To Zim Fibre Contractors", available at http://www.technomag.co.zw/2014/03/25/liquid-telecom-injects-32m-to-zim-fibre-contractors/ ; Kurt Wagner, "Facebook plans to lay almost 500 miles of fiber cable in Africa for better wireless internet", available at https://www.recode.net/2017/2/27/14741128/facebook-fiber-mark-zuckerberg-cable-africa-uganda*

18 *Vodacom Group Report, 2017. See: http://www.vodacom-reports.co.za/integrated-reports/ir-2017/pdf/full-integrated.pdf*

19 *What Impact Will Government Shareholding Have On The Future Success Of Btcl? Sunday Standard, 18 Feb 2016. http://www.sundaystandard.info/what-impact-will-government-shareholding-have-future-success-btcl*

20 *About Net One, Net One. See: http://www.netone.co.zw/?page_id=5*

21 *Acquisition of a 70% Stake in Ghana Telecom, Vodafone. See: http://www.vodafone.com/content/index/media/vodafone-group-releases/2008/acquisition_of_a_70.html*

22 *Tanzania agrees to buy back Bharti Airtel's stake in State telecom, the East African. See: http://www.theeastafrican.co.ke/news/Tanzania-to-buy-back-Bharti-Airtel-stake-in-State-telco/2558-2731244-1ukvh6z/index.html*

23 *Orange Sells its 70% Stake in Telkom Kenya, Cellular News. See: http://www.cellular-news.com/story/Business/68258.php*

24 *Vodafone transfers stake in Kenya operator Safaricom to Vodacom, Financial Times, see: https://www.ft.com/content/bbbb386e-3956-11e7-ac89-b01cc67cfeec*

Meanwhile, state control in the regulation of the telecommunication sector remains quite strong in certain countries. In Botswana, the Department of Telecommunications and Postal Services (DTPS) which is responsible for developing ICT policies and laws also 'supervises' government-owned independent entities like the Botswana Communications and Regulatory Authority (BOCRA), the Botswana Fibre Network (BoFiNet) and Botswana Telecommunications Company Limited (BTCL). The same position is true in other countries such as in Ghana, Kenya, Tanzania, and Zimbabwe, where the Ministries of ICT oversee the national regulators and other state-owned enterprises, including interests in public traded companies.

Consequently, whereas there are legal procedures and standards to be complied with in the performance of their functions, these can sometimes be implemented in a manner that satisfies the interests of the incumbent government.[25] Further, the control of infrastructure, regulation and licensing makes the government-controlled operators quite influential, which position is likely to disadvantage private operators or make them vulnerable, where the government- controlled firm is a dominant player in the market.

3.5 Legal Protection of Human Rights

There are a number of instruments that protect and promote human rights on the internet at the international, regional, and national levels. Some of the rights protected include the right to freedom of expression, freedom of the media, political participation, privacy, information, dignity, security of the person, freedom from discrimination against race, sex, ethnicity, and freedom from torture, cruel and inhuman treatment. The instruments also recognise the specific rights of women and children as special categories of persons requiring additional protection.

The international instruments include the international Bill of Rights comprising the Universal Declaration of Human Rights (UDHR); International Covenant on Civil and Political Rights (ICCPR) and its Optional Protocols; and the International Covenant on Economic, Social and Cultural Rights (ICESCR) and its Optional Protocols. Others are the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and its Optional Protocol; Convention on the Rights of the Child (CRC); Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (UNCAT) and its Optional Protocol; and the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD).

At the regional level, this study reviewed the status of commitments under instruments adopted at the African Union level, such as the African Charter on Human and Peoples' Rights (ACHPR), Charter on the Rights and Welfare of the Child (CRWC); Charter on Democracy and Elections; and the Protocol to the Charter on the Rights of Women in Africa (Maputo Protocol). The table below shows the status of ratification, signature or accession to the various instruments, classified per country.[26]

25 *Freedom on the Net: https://freedomhouse.org/report/freedom-net/2016/malawi*

26 *Status of Ratifications, OHCHR. See: http://indicators.ohchr.org; Legal Instruments, ACHPR. See: www.achpr.org/instruments/*

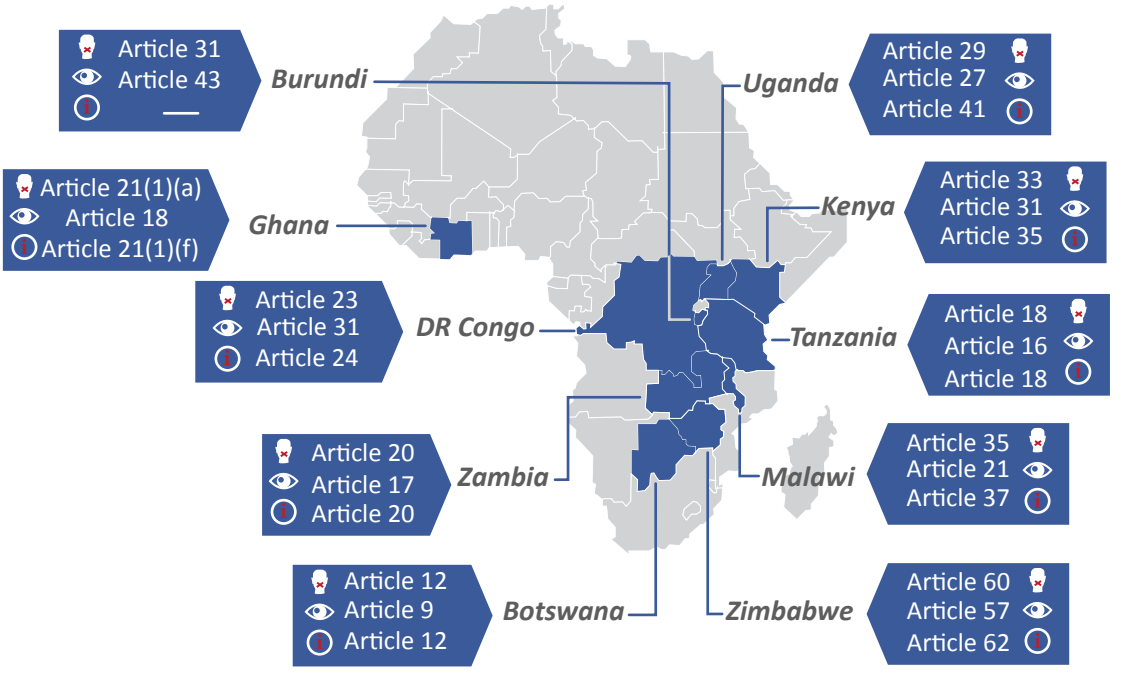
Status of Ratification of Key International and Regional Instruments

	Int'l Bill of Rights	ACHPR & Maputo	CEDAW	CRC	UNCAT	ICERD	CRWC	CDE
Botswana	R +(N-ICESCR)	R	R+P	R	R+P	R	R	R
Burundi	R	R+P	R+P	R	R	R	R	R
DR Congo	R+2P	R+P	R	R	R+P	R	N	R
Ghana	R+P	R+P	R+P	R	R+P	R	R	R
Kenya	R	R+P	R	R	R	R	R	R
Malawi	R+P	R+P	R+P	R	R	R	R	R
Uganda	R+P	R+P	R	R	R	R	R	R
Tanzania	R	R+P	R+P	R	N	R	R	N
Zambia	R+P	R+P	R+P	R	R+P	R	R	R
Zimbabwe	R	R+P	R	R	N	R	N	N

R Ratified, acceded or signed instrument only, P No Action taken N No of Protocols signed or ratified

At the national level, the constitutions of the respective countries also contain, as shown in Table 3 below, provisions that uphold the protection of the rights to freedom of expression, privacy including of communications, and access to information.

Provisions of Country Constitutions Protecting Freedom of Expression (FOE), Right to Privacy (RTP) and Freedom of Information (FOI)



As shown above, freedom of expression and the right to privacy are protected under all the constitutions in all countries under review. However, other national laws either promote the rights as enshrined in the constitutions, or limit them. It is important to note that where limitations are provided for under national law, the Special Rapporteur on Freedom of Expression has indicated that any limitation to freedom of expression must pass the following three-part, cumulative test:[27]

a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
b) It purpose must be (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and,
c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

Moreover, the Special Rapporteur indicated that any legislation restricting FOE must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory, and with adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application. Further, that the responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of states' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. And it exists over and above compliance with national laws and regulations protecting human rights.[28]

Consequently, where provisions in legislation are not progressive or have been abused, courts should declare such legislation unconstitutional. This was the case in Kenya where section 29 of the Kenya Information and Communication Act on misuse of telecommunication system and section 194 of the Penal Code on criminal defamation were declared unconstitutional in February 2017.[29] Similarly, in June 2016, the government of Ghana withdrew, the Interception of Postal Packets and Telecommunication Messages Bill, 2015 which, would have interfered with the privacy of users' correspondence under the constitution.[30]

3.6 Status of ICT Legislation

States have put in place legal measures to regulate telecommunications and key functions of internet intermediaries. As access to and use of the internet and related technologies has evolved, governments have taken reactive steps towards reviewing and updating laws to regulate online platforms. This is evident in the content and number of bills currently under development in the countries under review.

As shown in Table 4 below, Ghana, Kenya, and Zimbabwe have the highest number of laws already in force, while Malawi has the least legislation regulating the work of intermediaries, largely because of consolidation of ICT legislation under one law. In Tanzania, a number of the legislations are still new as the country adopted several bills in 2016. Kenya and Malawi also adopted access to information laws in 2016 and 2017 respectively. Notably, Ghana is the only country with a data protection law.

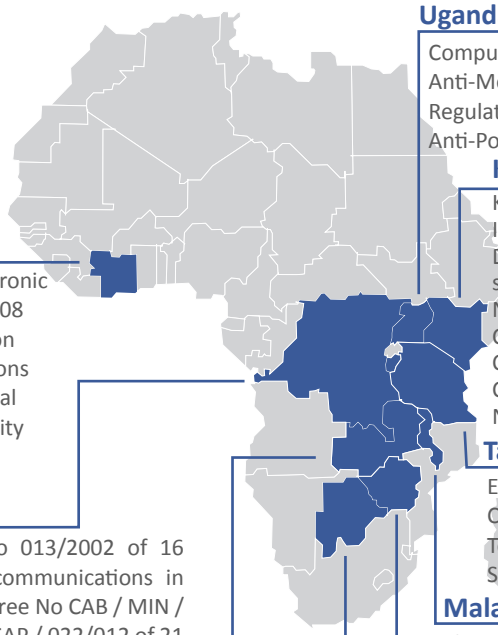
27 *See para 24 (a), (b) and (c) of the Human Rights Council "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27". http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*

28 *Ian Brown & Douwe Korff, GNI, Digital Freedoms in International Law ; Practical steps to protect human rights online, page 14. https://globalnetworkinitiative.org/sites/default/files/Digital Freedoms in International Law.pdf*

29 *Kenya: Court strikes down criminal defamation laws, Article 19 https://www.article19.org/resources.php/resource/38626/en/kenya:-court-strikes-down-criminal-defamation-laws*

30 *Mark Anthony Vinokor, "Govt withdraws "Spy Bill" from Parliament", graphic.com, June 30, 2016, available at https://www.graphic.com.gh/news/general-news/govt-withdraws-spy-bill-from-parliament.html (accessed September 14, 2017).*

Relevant Sector Statutes Regulating Intermediaries



Uganda

Computer Misuse Act 2011; Communications Act, 2013; Anti-Money Laundering Act; Anti-Terrorism Act; and the Regulation of Interception of Communications Act, 2010; Anti-Pornography Act, 2014.

Kenya

Kenya Information and Communications Act; Access to Information Act; Guidelines for the Prevention of Dissemination of Undesirable Bulk Political SMS and social media content via Electronic Communications Networks (Guidelines for Political Messaging); National Cohesion and Integration Act; Defamation Act; Copyright Act; Penal Code; Sexual Offences Act; Children Act; Prevention of Terrorism Act; and the National Intelligence Service Act

Ghana

Anti-Terrorism Act; Electronic Communications Act, 2008 (Act 775); Data Protection Act; Electronic Transactions Act, 772; and the National Communications Authority Act 769

Tanzania

Electronic and Postal Communication Act (EPOCA); Cyber Crime Act; Media Service Act; Prevention of Terrorism Act; Law of Marriage Act (2002); and the Sexual Offenses Special Provisions Act (1998)

DR Congo

The Framework law No 013/2002 of 16 October 2002 on Telecommunications in DRC; The ministerial decree No CAB / MIN / PTNTIC / TKKM / PKM / SAP / 022/012 of 21 December 2012; and decree law 1-61 of 25 February 1961

Malawi

Electronic and Transactions and Cyber Security Act, 2016

Zimbabwe

Criminal Law Code; Postal and Telecommunications Act; Interception of Communications Act; Criminal Law and Codification Act; and the Censorship and Entertainments Control Act

Zambia

Electronic Communications and Transactions Act; Information and Communications Technology Act; State Security Act; Penal Code and the Defamation Act

Botswana

Penal Code; Botswana Communications and Regulatory Authority Act; Electronic Communications and Transactions Act; Cybercrime and Computer Related Crimes Act; and Electronic Records and Evidence Act

Burundi

Decree Law No 100/97 of 18 April 2014; Ministerial Law No 540/356 of 17 March 2016; Law No 1/15 of 9 May 2015; and Law No 1/11 of 4 June 2013

Many countries are in the process of updating their laws. In DR Congo, at least three bills covering ICT and electronic commerce are yet to be enacted as the process was halted in April 2017, following the resignation of the ICT minister.[31] Equally, Botswana is yet to enact the Data Protection and Privacy Bill 2017 and introduce a freedom of information bill, following a failed attempt to do so in 2012.[32] For Kenya, the Computer and Cybercrime Bill 2017 and the Privacy and Data Protection Bill 2012, are yet to be enacted. Zambia is also yet to enact its Cyber Security Bill 2017, Cyber Crime Bill 2017, Electronic Commerce Bill 2017, and Data Protection Bill 2017. Uganda proposed a Data Protection and Privacy Bill back in 2015 which has to-date not been passed into law.

31 *They include the draft law on trade and electronic commerce; the draft law amending and supplementing Law No. 14/2002 of 16 October 2002 establishing the Regulator; and the draft Law on Telecommunications and Information Technology Communication in the Democratic Republic of Congo, amending and supplementing, Law No. 13/2002 on Telecommunications. See: Marcel Tshishiku, "Assemblée Nationale: Les députés refusent au ministre Ambatobe le droit de défendre trois projets de loi," La tempête des tropiques, 20 April 2017. http://www.latempete.info/21319-2/*

32 *The death of the right to information bill in botswana, IFLA Journal http://journals.sagepub.com/doi/abs/10.1177/0340035213497673*

4.0 Overview of Information Controls in Place

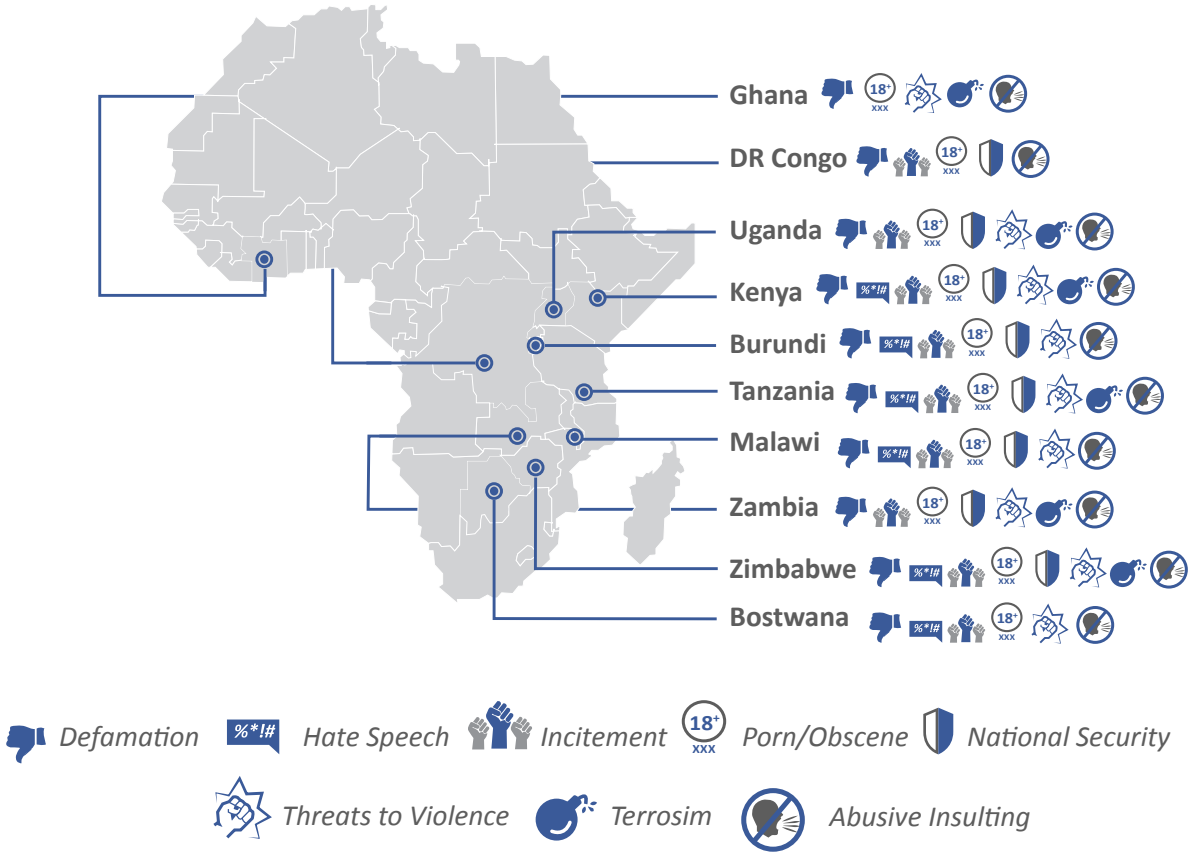
Governments sensitive to criticism have been heavy-handed in their responses towards perceived critics. The measures taken include arrests, intimidation, prosecution and detention of perceived critics, censorship, use of new and old draconian legislation, technical attacks, and repeated threats of regulating social media and intermediaries. Some of the perceived dangers and justifications for their responses include hate speech, false information or "fake news", offensive communication including insults, pornography, obscenity, defamation, incitement (threats to violence), national security, among others. In this section, we provide an overview of existing limits, measures and tactics deployed by governments, which violate internet freedom.

4.1 Content Controls in Legislation

Most of the countries under review have laws prohibiting defamation, hate speech, incitement, pornography or obscene content, threats to violence, terrorism, abusive or insulting speech (to individual, religion, place or public official), leaking official secrets, or speech that threatens national security. Terminology in legislation varies: for example, insults are in some cases treated as offensive communication in others, as hate speech or defamation. On the other hand, what some countries term pornography others refer to as obscene or offensive communication.

As shown in the Figure below, Kenya, Tanzania and Zimbabwe, lead with the highest number of prohibitions under local statutes, followed closely by Malawi, Uganda and Zambia.

Types of Content Limited by Law



4.1.1 Offensive Communication

In some of the reviewed countries, "making offensive communication" is an offence used to punish and silence voices of dissent. Its definition is broad and may refer to the use of abusive, obscene or insulting language. In Botswana, for example, Section 93 of the Penal Code restricts abusive, obscene or insulting language in a public gathering directed towards the President, MPs and any public officer. Section 95 outlaws threatening breach of the peace or violence; section 96 addresses incitement to violence and disobedience of the law; section 140 addresses writing or uttering words with intent to wound religious feelings. While the offences do not specifically mention the online context, the provisions can still be used to charge persons who commit the offences online. In September 2016, Botswana security services arrested an individual for allegedly producing and disseminating a satirical digitally manipulated image of President Ian Khama. The INK Centre for Investigative Journalism condemned the arrest as a violation of freedom of expression.[33]

Section 33 of the Zimbabwe's Criminal Law and Codification Act also prohibits speech that insults the President. It is an offence to publicly make statements that cause hatred, contempt or ridicule of the person or office of the President or Acting President of Zimbabwe. The offence is punishable by a fine of up to two million Zimbabwe dollars (USD 5,500), or a years' imprisonment, or both. The provision has since been condemned as unconstitutional, but it is yet to be repealed.[34] Similar provisions exist in Tanzania, and have been used to quash government critics.

Incidences of warnings, arrests, and detentions of opposition political party leaders, artists, political activists, and whistleblowers are common in Tanzania. In 2016, at least ten people[35] were arrested and charged for online offences. This included six charged under section 16 of the Cybercrime Act, 2015 for insulting or criticising the leadership style of president Magufuli through posts on Facebook and WhatsApp.[36] More recently, outspoken opposition MPs Tundu Lissu[37] and Halima Mdee[38] were in February and July 2017 also arrested and detained for abusing President Magufuli and, for sedition and incitement, respectively. The videos of their purported offences were circulated online.[39] Another Chadema MP, Godbless Lema, was detained for four months and was charged with sedition in December 2016, for insulting President Magufuli in video and audio clips widely shared on social media.[40] In March 2017, Tanzanian rapper Nay wa Mitego was arrested and detained for a day in relation to the lyrics of the song, "WAPO", which were deemed insulting to the government and President Magufuli.[41]

In September 2017, the Tanzanian government introduced the Electronic and Postal Communications (Online Content) Regulations 2017.[42] The new regulations impose a TShs. 5 million (USD2,300) fine for social media users and online content producers found with materials deemed "indecent, obscene, hate speech, extreme violence or material that will offend or incite others, cause annoyance, threaten harm or evil, encourage or incite crime, or lead to public disorder." The regulations also require the registration of online radio, TV and other digital platforms, including bloggers and website managers, with the Tanzania Communications Regulatory Authority (TCRA), which shall have unfettered powers under the regulations, including the deregistration of registrants. While authorities have defended the measures, arguing that they prevent moral decadence and promote national security and cohesion, rights activists say the government's intentions are to curtail people's right to free speech.[43]

33 *United States Department of State. (2016). Botswana Human Rights Report. Bureau of Democracy, Human Rights and Labour.*

34 *Zimbabwe court says Robert Mugabe 'insult law' invalid - http://www.bbc.com/news/world-africa-24757351*

35 *State of Internet Freedom in Tanzania, 2016, CIPESA https://cipesa.org/?wpfb_dl=229*

36 *LHRC, Tanzania Human Rights Report 2016, Cases of Cybercrime by the Media, Page 39-40, http://www.humanrights.or.tz/*

37 *Athuman Mtulya, Tundu Lisu arrested, 6th February 2017,the citizen, see: http://www.thecitizen.co.tz/News/Tundu-Lissu-arrested/1840340-3802454-format-xhtml-fnaqq2/index.html; Tanzania's Tundu Lissu charged with abusing the president, The East African. See: http://www.theeastafrican.co.ke/news/Tanzania-Tundu-Lissu-charged-with-abusing-president/2558-4032472-qdl5y1/index.html*

38 *The Citizen, Kinondoni DC orders arrest of Kawe MP Mdee for insulting the President July 4, 2017, see : http://www.thecitizen.co.tz/News/1840340-3999268-gst1r8z/index.html; Tanzania: Chadema's Lema Out on Bail, All Africa. http://allafrica.com/stories/201608300114.html*

39 *Tundu Lissu still in critical, stable condition after shooting, Daily Nation. See: http://www.nation.co.ke/news/Tundu-Lissu-in-critical-but-stable-condition-Nairobi/1056-4096058-10pwvqgz/index.html*

40 *Lema Finally Bailed out, March 03, 2017, http://www.azaniapost.com/politics/lema-finally-bailed-out-h1469.html*

41 *Tanzania rapper Nay wa Mitego arrested for criticizing the president, March 2017, Afro London, See more: http://afrolondonnews.com/2017/03/27/tanzania-rapper-nay-wa-mitego-arrested-for-criticising-president/; Nay Wa Mitego - WAPO (Official Music Video), YouTube. https://www.youtube.com/watch?v=RDqbv7Voxp0*

42 *Tanzania to license blogs, websites as part of new online media regulation, Africa News. http://www.africanews.com/2017/09/27/tanzania-to-license-blogs-websites-as-part-of-new-online-media-regulation/*

43 *New communication law must protect free speech, The Citizen, 26 September 2017. http://www.thecitizen.co.tz/oped/New-communication-law-must-protect-free-speech/1840568-4112832-xqc346/index.html*

In December 2016, Swaibu Nsamba Gwogyolonga, an opposition leader in Uganda, was accused of vilifying President Museveni by posting on Facebook the president's image in a casket. He was arrested and charged with "offensive communication and libel contrary to Sections 25 of the Computer Misuse Act 2011 and 181(1) of the Penal Code respectively, and he is currently out on bail.[44] Further in April 2017, Dr. Stella Nyanzi, a Makerere University academic and activist, was abducted by law enforcement, detained and later charged with two counts of cyber harassment and offensive communication under section 24 (1)(2)(a) and 25 of the Computer Misuse Act 2011 for "repeatedly insulting the person of the President" on her Facebook page, referring to him as "a pair of buttocks" and his wife, Janet, as "empty-brained".[45] Dr. Nyanzi, who is well known for using social media to criticise the government, was remanded in prison for 33 days before being freed on bail in May 2017.[46]

The Uganda Communications Commission (UCC), the industry regulator, issued a statement early September 2017, warning the general public against "irresponsible use of the social and electronic communications."[47] The UCC cited complaints received and the increasing use of social and electronic media to "perpetrate illegalities" like sectarianism, hate speech, inciting public violence and prejudice, and pornographic content, which it said were exposing "the unsuspecting public" to financial, social and emotional distress, and posing serious national security concerns.

Zimbabwe's POTRAZ also issued a statement in July 2016 warning against "the abuse of social media" over a campaign to stay away from work in protest against government and the deteriorating economic crisis in July 2016.[48] The statement in part warned against the "possession of, generating, sharing or passing on abusive, threatening, subversive or offensive communication messages, including WhatsApp or any other social media messages that may deemed to cause despondency, incite violence, threaten citizens and cause unrest". It warned that those who abused social media would be arrested and dealt with in the national interest."

4.1.2 Pornographic or Obscene Content

Various legislation in the countries under review aim to safeguard the rights of children and protect them from sexual exploitation. Section 12 of Kenya's Sexual Offences Act of 2006 prohibits child pornography, including its promotion and distribution (Section 12). Section 16 of Botswana's Cybercrime and Computer Related Act prohibits the production, possession and distribution of pornographic or obscene materials, including child pornography through a computer system. Section 13 of Tanzania's Cybercrime Act also prohibits child pornography through a computer system. Ghana's Criminal Code, 1960 (Act 29) prohibits the publishing of nude photos and videos which constitute indecent exposure.

Child pornography is also prohibited under section 23 of Uganda's Computer Misuse Act, 2011.[49] Further, Uganda's Anti-Pornography Act, 2014 prohibits the production, trafficking in, broadcast, procuring, importation and exportation and selling of pornography.[50] It establishes a Pornography Control Committee to detect pornography and support the development, acquisition and installation of pornography detection software in communication devices.

44 *Ibrahim Manzil & Betty Ndagire, Museveni social media critic granted bail, The Daily Monitor, http://mobile.monitor.co.ug/News/Museveni-social-media-critic-granted-bail/2466686-3506668-format-xhtml-muf015/index.html*

45 *Dr Nyanzi charged in court for insulting Museveni http://www.monitor.co.ug/News/National/Dr-Stella-Nyanzi-court-amid-heavy-police-deployment/688334-3884426-pb9rfmz/index.html*

46 *Uganda: Academic and activist Stella Nyanzi released on bail for free speech charges, Article 19 https://www.article19.org/resources.php/resource/38744/en/uganda:-academic-and-activist-stella-nyanzi-released-on-bail-for-free-speech-charges*

47 *Uganda Communications Commission, Warning Against Irresponsible Use of Social and ELectronic Communication Platforms, http://ucc.co.ug/files/downloads/UCC_PUBLIC_NOTICE_AGAINST_IRRESPONSIBLE_USE_OF_SOCIAL_MEDIA%2014-09-2017.pdf*

48 *Zimbabwe: Potraz Threatens Subscribers Over Social Media, Financial Gazette (Harare), 6 July 2016. http://allafrica.com/stories/201607070652.html*

49 *Computer Misuse Act https://www.nita.go.ug/sites/default/files/publications/Computer-Misuse-Act.pdf*

50 *The Anti-Pornography Act, 2014 is available at http://www.ulii.org/ug/legislation/act/2015/1-7; www.ug-cert.ug/files/downloads/The-Anti-pornography-act-2014*

Content relating to sexual minorities has also come under the attention of regulators. For instance, in March 2017, BOCRA banned live broadcasting by Gabz FM following an interview with anti-gay pastor, Steven Anderson. According to BOCRA, the broadcast was "unsuitable for children and … a warning should have been issued in accordance with section 37 of the Communications Regulatory Authority (CRA) Act."[51] It added that Pastor Anderson's "implausible and indecent" comments were not censored and the pastor "incited hatred against the homosexual community."

Similarly, the Kenya Films and Classification Board (KFCB) banned the screening of films such as the Wolf of Wall Street and 50 Shades of Grey which it labelled pornographic;[52] attempted to take down a YouTube music video for promoting homosexuality and immorality;[53] and threatened to ban Netflix over claims that its content was immoral and too explicit by Kenyan standards.[54] Zimbabwe's Censorship and Entertainments Control Act establishes a Board of Censors whose main function is to prohibit the importation, production and dissemination of "undesirable" publications, pictures, statues and records. The POTRAZ also regulates the online space and has the authority to censor online content deemed to be against national interests.

4.1.3 Hate Speech

Tackling online hate speech is a growing concern globally. Regulators and intermediaries are struggling with how to combat its spread given its impact. The DR Congo, Ghana, Uganda and Zambia do not have specific legislation prohibiting hate speech, while Botswana and Ghana lack specific legislation prohibiting speech that threatens national security. In such countries, hate speech may be dealt with as offensive communication or incitement. Even as various countries struggle to stem hate speech online and offline, the prosecution of hate speech cases is still haphazard, politicised and reactionary.[55] Also, hate speech is often not distinguished from abuse or insults, and may also amount to fake news or incitement.

The constitutions of Kenya and Zimbabwe outline "advocacy of hatred or hate speech" as part of the limitations on freedom of expression. Further, sections 13 and 62 of Kenya's National Cohesion and Integration Act, 2008 define and prohibit hate speech and this extends to hate speech online.[56] In July 2017, the government through the Communications Authority (CA) and National Cohesion and Integration Commission (NCIC) published the Guidelines on Prevention of Dissemination of Undesirable Bulk and Premium Rate Political Messages and Political Social Media Content via Electronic Networks.[57] The guidelines prohibit speech that is "offensive, abusive, insulting, misleading, confusing, obscene or profane language." They also prohibit publishing information that "might spread rumours, mislead or cannot be supported by facts."

In the run-up to the August 2017 general election in Kenya, the NCIC monitored social media sites, identified 21 WhatsApp groups for spreading hate speech[58] and arrested an administrator of another group for spreading false information.[59] Further, a court in August 2017 upheld the continued detention of a WhatsApp group administrator for an additional five days over sharing hate messages.[60]

51 *Khonani Ontebetse, GOVERNMENT BANS GABZ FM LIVE BROADCASTS, Sunday Standard, March 5 2017. http://www.sundaystandard.info/government-bans-gabz-fm-live-broadcasts*

52 *"Fifty Shades of Grey" movie banned in Kenya, Daily Nation. http://www.nation.co.ke/lifestyle/showbiz/Fifty-Shades-of-Grey-movie-banned-in-Kenya/1950810-2620314-uvq9rnz/index.html*

53 *KFCB Fails in Having Kenyan Gay Music Video 'Same Love' Banned on YouTube, Nairobi Wire. http://nairobiwire.com/2016/05/kfcb-fails-in-having-kenyan-gay-music-video-same-love-banned-on-youtube.html*

54 *Kenya threatens to ban Netflix over 'inappropriate content', Financial Times. https://www.ft.com/content/9e97edf0-bf71-11e5-846f-79b0e3d20eaf*

55 *Haki Africa calls for disbandment of NCIC, Hivi Sasa. http://www.hivisasa.com/posts/haki-africa-calls-for-disbandment-of-ncic*

56 *as "words published intended to incite feelings of contempt, hatred, hostility, violence or discrimination against any person, group or community on the basis of ethnicity or race".*

57 *Communications Authority, Guidelines for Prevention Of Dissemination Of Undesirable Bulk Political Sms And Social Media Content Via Electronic Communications Networks, June 2017.*
http://www.knchr.org/Portals/0/DOC-20170630-WA0061.pdf?ver=2017-06-30-225539-533

58 *Kenya NTV, YouTube, 'NCIC, police hunting down admins of 21 WhatsApp groups spreading hate messages', 17 July 2017. https://www.youtube.com/watch?v=c_IXMspYcaY*

59 *Nairobi News, 'Police arrest WhatsApp group admin over fake news', 13 August 2017.*
http://nairobinews.nation.co.ke/news/whatsapp-group-admin-arrested-fake-news/

60 *Daily Nation, WhatsApp group admin detained for sharing hate posts, 16 August, 2017. http://www.nation.co.ke/counties/Kilifi/WhatsApp-admin-malindi-hate-messages/1183282-4059660-bc381oz/index.html*

In Malawi in January 2016, Ken Msonda, a politician, in media interviews and on comments on his Facebook page said homosexuals had no rights in Malawi and deserved to be killed. Conservative religious groups protested against homosexuality as calls for his investigation by human rights groups mounted. Msonda was subsequently charged under section 124(1)(b) of the Penal Code, which makes it a criminal offence to incite others to break the law. However, the charges were dropped, a move that was also criticised.[61] A new law, the Prevention and Combating of Hate Crimes and Hate speech Bill approved by cabinet for public consultation in October 2016, is yet to be enacted into law.

Burundi, on the other hand, is grappling with hate speech, amidst widespread violence, torture and disappearances and restrictions of liberties.[62] Facebook posts and comments, some using pseudonyms others by people apparently using their real names, have been reported to routinely contain blatant incitement to violence.[63] In the run-up to the June 2015 election, hate speech was used as a key tool to whip up support in a campaign marred by harassment, intimidation and violence.[64] During the period, the use of words such as "zirye" meaning "to eat"; "kumesa" meaning "kill him" or "to wash"; "inyezi zirye" meaning "eat the insects"; "savoner" meaning "cleaned up"; and "gukorerako" meanings include to beat, punish and even kill, in statements online and offline, continued to provoke, incite and stir tension in the country.

4.1.4 Defamation

There has been increased use of criminal defamation provisions in some countries to silence critics. Section 32 of Tanzania's Media Service Act, 2015 provides that any matter which, if published, is likely to injure the reputation of any person by exposing them to hatred, contempt or ridicule, or is likely to damage their reputation, is defamatory.[65] Sections 192-199 of the Botswana Penal Code make similar provisions for defamation. Civil remedies for defamation are also available in most countries.

At the same time, individuals can also be held responsible for their actions online. In the DRC, it was reported that a journalist who shared a modified image of an influential politician in a WhatsApp group was arrested and detained.[66] The defamation complaint was filed against him personally and not his mobile operator. He was later released after apologising to the politician.

In Zambia, in 2016 some individuals were targeted for their critical views online.[67] In May 2017, Kwalela Kafunya, a Zambian medical doctor, was arrested and charged for defamation, issuing written threats to murder and giving false information to a public officer."[68] He is alleged to have disparaged President Edgar Lungu on a Facebook account created under a pseudonym.[69] Earlier, in April 2017, Chilufya Tayali, the Economic and Equity Party (EEP) leader, was arrested and charged with criminal libel under section 191 of the Penal Code, over a post on his Facebook page.[70]

61 *UN slams dropping of case against Malawi "kill gays" politician, Mamba Online. http://www.mambaonline.com/2016/01/25/un-slams-dropping-case-malawi-kill-gays-politician/*

62 *Oral Briefing by Fatsah Ouguergouz, Chair of the Commission of Inquiry on Burundi, UNHRC http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21760&LangID=E*

63 *Hate speech stirs trouble in Burundi, IRIN News, 21 August 2017 https://www.irinnews.org/analysis/2017/08/21/hate-speech-stirs-trouble-burundi*

64 *Words are weapons as Burundi heads to the polls http://www.irinnews.org/analysis/2015/06/25/words-are-weapons-burundi-heads-polls*

65 *The United Republic Of Tanzania, The Media Service Act, 2015, Part V, Section 32, Page 14. http://parliament.go.tz/polis/uploads/bills/1474021216-a bill - the media services act, 2016.pdf*

66 *Interview with Jeremie Kihambu, supervisor at the community Radio and Television Taina, (RTCT/Goma), July 2017*

67 *"Freedom on the Net 2016; Zambia Country Profile," Freedom House, 2016, 24 July 2017, https://freedomhouse.org/report/freedom-net/2016/zambia*

68 *"Doctor in court for defaming President Lungu," Daily News, 21 June 2017.https://www.dailynews.co.zw/articles/2017/06/21/doctor-in-court-for-defaming-president-lungu*

69 *"A Medical Doctor arrested for ' defaming ' President Lungu," Lusaka Times, 5 May 2017.https://www.lusakatimes.com/2017/05/05/medical-doctor-arrested-defaming-president-lungu/*

70 *"Chilufya Tayali Arrested and charged with criminal libel," Lusaka Times, 14 April 2017. https://www.lusakatimes.com/2017/04/14/chilufya-tayali-arrested-charged-criminal-libel/*

In addition, some individuals have also pursued intermediaries for content posted on their platforms. In August 2016, Fred Muwema, a prominent Ugandan lawyer, sought orders to reveal the identity of a blogger who goes under the name Tom Voltaire Okwalinga (TVO), and further prohibiting the alleged defamatory publications on his Facebook page, pursuant to section 33 of the Defamation Act 2009.[71] A court in Ireland declined to grant orders to reveal the identity of the blogger, but accepted that the post was defamatory, and it was subsequently removed. In the first half of 2015, a court order was issued to Google on behalf of a Kenyan internet solutions firm to delist an allegedly defamatory article written by a notable social media activist and subsequently posted on his website.[72] Google complied with the request – delisting the content from www.google.ke.

There have been a number of progressive court decisions in Kenya and Zimbabwe that have reinforced the constitutional protection for freedom of expression. In the Geoffrey Andare case, the court found Section 29 of the Kenya Information and Communications Act on improper use of licensed telecommunication system vague and beyond the scope of limitations in the constitution.[73] In the Jacqueline Okuta case, the court found the criminal defamation provisions under Section 36 and 194 of the Penal Code laws unconstitutional as they were not within the scope of Articles 33(2) and 24 of the Constitution.[74] In the case of Robert Alai, a critic of the President Kenyatta, the court found the offence of 'undermining the authority of a public officer' under Section 132 of the Penal Code unconstitutional.[75]

Meanwhile, in Zimbabwe, the Constitutional Court in Madanhire, Matshazi v Attorney-General[76] in June 2014 held that section 96 of the Criminal Law Code on criminal defamation was unconstitutional, but since the alleged offence took place before the introduction of the 2013 constitution, the court restricted its findings to section 20(1) of Zimbabwe's previous constitution[77] and not the current one.

4.1.5 False Information and "Fake news"

The spread of false information, also commonly referred to as "fake news", has sparked governments' interest to regulate social media. While preventing the spread of fake news may be a legitimate concern by both state and non-state actors, in repressive states the enforcement of such provisions can be used to curtail freedom expression.

As with hate speech, spreading false news may also be treated as incitement or offensive communication. In Zimbabwe, a false story about a school bus disaster went viral on Whatsapp in March 2017, causing panic among parents whose children went to that school.[78] In Kenya, during the 2017 electioneering period, fake news stories in form of manipulated videos disguised as genuine reports by CNN and BBC, were widely shared on social media platforms.[79]

In Malawi, in September and October 2016, speculation was rife about the whereabouts and the health of the country's president, Peter Mutharika, who was absent from the country with no formal communication from the government.[80] As a result, rumours gripped the nation, leading to the trending hashtag #BringBackMutharika on Twitter, as Malawians had become frustrated with the misinformation, and were seeking clarity regarding President Mutharika's unexplained and prolonged stay in the United States. The government ultimately clarified his whereabouts.

71 *Fred Muema v Facebook Ireland. http://www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/4dfdcbb6d27a627780258034005368 67?OpenDocument*

72 *Google, Transparency Report, July 2016 - December 2016. https://transparencyreport.google.com/government-removals/by-country/KE*

73 *Geoffrey Andare v Attorney General & Director of Public Prosecutions (2016)*

74 *Jacqueline Okuta & another v Attorney General & 2 others (2017)*

75 *Robert Alai v Attorney General (2017) Petition 174 of 2016*

76 *CCZ 2-15*

77 *Constitution of Zimbabwe Amendment (No. 19) Act, 2009. Constitution 20(1) of this Constitution protected the right to freedom of expression*

78 *Manama High School bus in fatal accident reports NOT true: http://bulawayo24.com/index-id-news-sc-national-byo-105652.html.*

79 *Farai Sevenzo, CNN, 'Kenya election: Fake CNN, BBC reports target voters', 1 August 2017.*
http://edition.cnn.com/2017/07/31/africa/kenya-election-fake-news/index.html

80 *#BringBackMutharika: The mystery of the AWOL president fuels rumour mill in Malawi:*
http://mgafrica.com/article/2016-10-10-bringbackmutharika-the-mystery-of-the-awol-president-fuels-rumour-mill-in-malawi

The response by governments and intermediaries alike is the development of stringent legislation and guidelines on how to address the spread of false information. Facebook, for example, developed tools and adverts to help users identify fake news.[81]

The approach by some government in dealing with fake news has been to criminalise the production of "false information". This is evident in Tanzania, where section 16 of the Cybercrimes Act 2015 makes it an offence to publish 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.

For Ghana, Section 208 of its Criminal Code provides that "any person who publishes or reproduces any statement, rumour or report which is likely to cause fear and alarm to the public or disturb the public peace, knowing or having reason to believe that the statement, rumour or report is false is guilty of a misdemeanour." The provision requires the publisher to have taken "reasonable measures to verify the accuracy of the statement, rumour or report" before publishing. In October 2011, an internet user, Amina Mohammed, was arrested and charged with causing fear and panic, over her claims that there had been mass rape during a robbery incident in a bus. She was acquitted a year later for lack of evidence.[82]

A similar approach is noted in Kenya, where clause 12 of the proposed Computer and Cyber Crimes Bill 2017, provides that a person who intentionally publishes false, misleading or fictitious data or misinforms with intent that the data shall be considered or acted upon as authentic, with or without any financial gain, commits an offence. The offence is punishable by a fine not exceeding five million shillings ($50,000) or to imprisonment for a term not exceeding two years, or to both.

Some of the cases as cited in this report involve instances where non-state actors are using fake news to raise awareness of injustices within their communities. For example, during election protests in DR Congo in January 2015, in a bid to draw international attention to the situation in the country, some anonymous bloggers created misleading content using images and videos of civil strife from Burkina Faso and Ivory Coast to depict the situation in Congo.[83]

4.1.6 National Security and Terrorism

Botswana, Burundi, DR Congo, and Malawi do not have specific legislation prohibiting terrorism related speech. Kenya's Security Laws (Amendment) Act 2014 on the other hand, introduced a new section 30A in the Prevention of Terrorism Act which criminalises publishing or uttering of statements that are likely to be understood as directly or indirectly encouraging or inducing another person to commit or prepare to commit an act of terrorism.[84]

Uganda's Anti-Terrorism Act, 2002 states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news or materials that promote terrorism is also liable be sentenced to capital punishment upon conviction. Further, under section 9, it makes any person who runs or supports any institution for publishing and disseminating news or materials that promote terrorism" guilty of an offence. This provision, can construe any content passing through an ISP or intermediary as information promoting terrorism, which is an offence under section 7 of the Act. Further, an amendment to section 7 of the Act, added the unlawful possession of materials for promoting terrorism, such as audio or video tapes or written or electronic literature, to the list of acts that amount to terrorism.[85]

81 *Abd Latif Dahir, Quartz Africa, 'Facebook has joined the battle to combat fake news in Kenya', 2 August 2017. https://qz.com/1044573/facebook-and-whatsapp-introduce-fake-news-tool-ahead-of-kenya-elections/*

82 *Amina mass rape case thrown out of Court, Ghana Web. https://www.ghanaweb.com/GhanaHomePage/economy/Amina-mass-rape-case-thrown-out-of-Court-241579*

83 *Interview with Alexandre Capron, France 24 journalist, July 2017; Top 8 fake images shared on African social media, The Observers, France 24. http://observers.france24.com/en/20160412-top-fake-images-african-social-media*

84 *Section 64, The Security Laws (Amendment) Act, 2014 http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf*

85 *Anti-Terrorism (Amendment) Act, 2015*

Governments are abusing terrorism legislation to stifle legitimate expression. In November 2016, Ugandan police arrested, detained, charged, and later released KTN Kenya news anchor and reporter Joy Doreen Biira, a Ugandan, for abetting terrorism by allegedly taking photos of mass killings in Kasese in Uganda where 55 were killed by the army, and posting them on Facebook.[86] Her laptop and phones were confiscated and she was forced to delete the posts. Her arrest was widely condemned, sparking outrage online through hashtags such as #FreeJoyDoreen and #JournalismIsNotaCrime which trended on Twitter.[87] She was released on bond and the case against her is ongoing,[88] despite calls by KTN Kenya for solidarity and her release.[89]

In Zimbabwe, the epithet 'social media terrorist' was used by government in August 2016, and popularised by state-owned media and government officials in reference to "subversive elements" and other social media activists, perceived as 'abusing' the platforms.[90] A number of little-known individuals were 'exposed' by the state-owned newspaper, The Herald, as social media terrorists in a move read as an attempt to justify the introduction of stiff social media regulations under the banner of unearthing cyber-terrorism.[91]

In Malawi, three opposition Members of Parliament were arrested and charged with treason for plotting a coup through a WhatsApp group chat in February 2016.[92] Although the charges were dropped a year later,[93] civil society groups termed the arrests "politically motivated."[94]

4.1.7 Censorship

Censorship manifests itself in many forms which include filtering or blocking of content, self-censorship, internet shutdowns, cyber attacks, and takedowns.

In January 2016, Mmegi, an independent newspaper in Botswana, experienced a cyber-attack that destroyed a significant amount of its archived material. Mmegi's editor claimed that the Directorate of Intelligence and Security Services (DISS) was behind the attack, and that it had been carried out as retaliation for an article claiming that the Directorate on Corruption and Economic Crime (DCEC) had questioned the former head of DISS about the wealth he had purportedly amassed.[95]

In Kenya, following public outcry over the public funds spent on the numerous foreign trips taken by President Kenyatta since his election in 2013,[96] a popular website www.isuhuruinkenya.co.ke, tracking and highlighting these trips was taken down by KENIC in December 7, 2015 following government order.[97] In his two years in office, the president had made more than 43 trips abroad, 10 more than those his predecessor made in ten years.

86 *Joy Doreen Biira released from police custody, The Standard. https://www.standardmedia.co.ke/article/2000225070/joy-doreen-biira-released-from-police-custody*

87 *Arrest of KTN journalist Joy Doreen Biira in Uganda's Rwenzururu kingdom sparks outrage, International Business Times. http://www.ibtimes.co.uk/arrest-ktn-journalist-joy-doreen-biira-ugandas-rwenzururu-kingdom-sparks-outrage-1593765*

88 *BEING A SOLDIER WAS MY DREAM – JOY DOREEN BIIRA, Life Magazine, January 2017. http://lifemagazine.co.ke/soldier-dream-joy-doreen-biira/*

89 *Sam Shollei: Drop case against KTN anchor Joy Doreen Biira, The Standard. https://www.standardmedia.co.ke/article/2000225422/sam-shollei-drop-case-against-ktn-anchor-joy-doreen-biira*

90 *Everson Mushava, Mushohwe threatens social media abusers, August 17, 2016. https://www.newsday.co.zw/2016/08/17/mushohwe-threatens-social-media-abusers*

91 *Social media terrorists exposed, August 09, 2016, Herald, http://www.herald.co.zw/social-media-terrorists-exposed*

92 *Kabwila Arrested: Malawi Police May Arrest More 'WhatsApp Coup Plotters' http://www.nyasatimes.com/kabwila-arrested-malawi-police-may-arrest-more-whatsapp-coup-plotters/*

93 *Treason Charges Dropped Against Kabwila, Two Others: https://malawi24.com/2017/03/29/treason-charges-dropped-kabwila-two-others/*

94 *Freedom on the Net: https://freedomhouse.org/report/freedom-net/2016/malawi*

95 *Freedom House. (2016). Botswana : Freedom in the world. Retrieved from Freedom House Website: https://freedomhouse.org/report/freedom-world/2016/botswana*

96 *Uhuru: here are the benefits of my foreign trips, Daily Nation. http://www.nation.co.ke/news/Here-are-the-benefits-from-my-foreign-trips/1056-2986584-b85kipz/index.html*

97 *Martin Gicheru, Techweez, 'KENIC Confirms Takedown of isUhuruInKenya.co.ke Domain', 7 December 2015. http://www.techweez.com/2015/12/07/isuhuruinkenya-taken-down/*

4.1.8 Internet Shutdowns

Internet shutdowns or threats to shut down the internet were noted as a common and growing trend across the countries under review especially during election periods or politically sensitive periods.

The DR Congo for example, has experienced several partial or complete internet shut downs during the years under review, ordered for "security reasons" and often without following a judicial process.[98] The most recent shutdown was on August 7, 2017, initiated by a signed letter from the Post and Telecoms chief regulator Oscar Manikunda Musata to operators stating that a shutdown was necessary "in order to prevent the exchange of abusive images via social media." The letter requested operators to "take technical measures to restrict to a minimum the capacity to transmit images [over social media platforms]."[99] The resultant four-day partial shutdown, widely condemned by civil society groups, affected social media platforms WhatsApp, Facebook, and Twitter.[100]

Earlier in December 2016, the country experienced an 11-day partial shutdown that affected multimedia sharing and video calls on social media, this time ordered by the Autorité de Régulation des Postes et Télécommunications du Congo (ARPTC), again in a letter to ISPs a day before the end of President Kabila's term.[101] Citizens denounced it as an "extortion of their freedom of expression and right to information".[102] The signals of the UN backed Radio Okapi and Radio France Internationale (RFI) were jammed in November 2016, an act denounced as a "restriction on freedom of expression and people's right to information."[103] In January 2015, the internet had been shut down for several days and some opposition leaders' phone numbers were blocked.[104] Intermediaries interviewed cited their contractual obligations as reasons for obeying shutdown orders from the government.

Burundi, on the other hand, had its first partial ten-day Internet shut down during the election period of 2015 which affected mobile access to social media platforms.[105] The shutdown was ordered by the Agence de Régulation et de Contrôle des Télécommunications (ARCT) after protests opposed to what opponents considered as a third-term for President Pierre Nkurunziza, despite a two-term constitutional limit. In February 2016, the Uganda Communications Commission (UCC) instructed mobile network operators to shut down social media and mobile money services as the country went to the polls. A similar order was issued in May 2016 during the swearing-in of the president. In both incidents, the regulator cited national security and the need to limit use of social media for campaigning and inciting violence. The government also acknowledged its lack of technical capacity to isolate and only deal with specific individual users of social media. This perhaps justified its need to have the entire internet shut down. As result, people used proxies and Virtual Private Networks (VPNs) to circumvent the blockages and access the internet. Worth noting is how ISPs responded to the order. Whereas some service providers such as MTN and Airtel informed their customers of the blockage, others did not.

in July 2016, Zimbabwe experienced interruptions to access to the internet and instant messaging service WhatsApp across all mobile networks and ISPs.[106] Operators explained the interferences as a technical disruption of service and apologised without offering further explanation. The government and the telecoms regulator, POTRAZ, denied issuing such an order.[107] However, ISPs do not usually go against

98 *Arsene Tungali, The Evolution of Internet Shutdowns in DR Congo, CIPESA, 31 March 2017. https://cipesa.org/2017/03/the-evolution-of-internet-shutdowns-in-dr-congo/*

99 *Patient Ligodi, "Congo orders internet slowdown to restrict social media: telecoms source," Reuters, 7 August 2017, access: 7 August 2017, https://www.reuters.com/article/us-congo-violence-internet-idUSKBN1AN2DE*

100 *"RDC : Après 4 jours de limitation, les Congolais peuvent à nouveau utiliser pleinement les réseaux sociaux," Actualite.CD, 12 August 2017. https://actualite.cd/2017/08/12/rdc-apres-4-jours-de-limitation-congolais-peuvent-a-nouveau-utiliser-pleinement-reseaux-sociaux/*

101 *AFP, "DR Congo orders social networks shutdown as Kabila's term ends," Enca.com, 15 December 2016. http://www.enca.com/africa/dr-congo-orders-for-social-networks-shutdown-as-kabilas-term-ends*

102 *"Kinshasa: les habitants dénoncent le «blocage prolongé» des réseaux sociaux," Radio Okapi, 23 December 2016. http://www.radiookapi.net/2016/12/23/actualite/societe/kinshasa-les-habitants-denoncent-le-blocage-prolonge-des-reseaux*

103 *DRC: RFI and Radio Okapi signals still jammed, Africa News. http://www.africanews.com/2016/11/06/drc-rfi-and-radio-okapi-signals-still-jammed//*

104 *"Kinshasa : les numéros de téléphone de certains opposants coupés depuis un mois," Radio Okapi, 19 February 2015. http://www.radiookapi.net/actualite/2015/02/19/kinshasa-les-numeros-de-telephone-de-certains-opposants-coupes-depuis-un-mois*

105 *Update on the State of Internet Freedom in Burundi, 2015. See: https://www.opennetafrica.org/?wpfb_dl=28*

106 *Protests Shut Down Zimbabwe, ENCA. http://www.enca.com/africa/protests-shut-down-zimbabwe*

107 *Zimbabwe government denies jamming whatsapp. Zimmetro. http://zimmetro.net/index-id-news-zk-20342.html*

government orders owing to their licensing conditions. In Ghana[108] and Kenya,[109] government officials warned of the possible internet shutdowns as the countries approached general elections in 2016 and 2017 respectively. However, the polls came to pass without any reports of shutdowns.

4.1.8 Other Restrictions

Media as the fourth estate, has traditionally played a key role in shaping public opinion and discourse, at times shaping government policy. However, with the emergence of social media, traditional media's agenda setting role is diminishing, and is being taken up by social media, including internet users who are influencers, news producers and online publishers.[110] In response to this development, many traditional news media have integrated social media as part of their news production strategies, perhaps in a bid to regain more relevance online as they have offline.[111] However, even as mainstream media go online, governments are increasingly clamping media freedom by targeting both online and offline in a bid to control information flow in the public sphere.

Many of the governments in the focus countries restrict media freedom through intimidation, arrests and detention of journalists, physical destruction of their property, technical attacks on their online spaces, among others. One such example was in May 2016, when the offices of the Botswana Gazette were raided and three staff temporarily detained over a news report implicating the Botswana Directorate of Intelligence and Security Services (DISS) and Botswana Democratic Party in corruption. One of the journalists was charged for disclosing information related to an ongoing investigation. In addition, Outsa Mokone, an editor of Sunday Standard, was charged with sedition but later acquitted, following a story published in the newspaper alleging that the president was involved in a late-night car crash that was not reported to the police.[112] The country has been criticised for its apparent lack of media freedom. It ranks at number 48 according to the 2017 World Press freedom index,[113] and rated as being "partly free" by Freedom House.[114]

In Burundi, the physical destruction of Independent radio and television stations following the coup attempt in May 2015 forced many local journalists to flee to exile. Stations such as Radio Inzamba (www.inzamba.org) and Radio Humura (www.rpa.bi) now operate online from abroad.[115] Others are using Twitter and Facebook to broadcast news.

A new law in Ghana, the National Media Commission (Content Standards) Regulations, 2015 (Legislative Instrument (LI 2224), whose operation was halted by the Supreme Court presented a challenge for media freedom. It required a broadcaster to seek authorisation from the National Media Commission (NMC) before broadcasting content on any public electronic communications network, public electronic communications service and broadcasting service. In February 2016, Kennedy Agyapong, a Ghanaian Member of Parliament, threatened to assault Ato Kwamena Dadzie, a senior journalist working with Accra-based Joy FM, for writing unpleasant things about him on his (Ato's) Facebook page.

Zambian regulator ZICTA has pursued alleged critics both individuals and corporates.[116] In October 2016, ZICTA raided the premises of a number of ISPs and internet cafes it accused of operating illegally, in a move seen as limiting online anonymity.[117]

108 *Ghana Police Chief Criticized Over Proposed Social Media Ban, VOA News. https://www.voanews.com/a/ghana-police-chief-criticized-proposed-social-media-ban/3349810.html?platform=hootsuite*

109 *Simon Ndonga, Capital News, 'Kenya may shut off social media during August elections' 17 july, 2017. http://www.capitalfm.co.ke/news/2017/07/kenya-may-shut-off-social-media-august-elections/*

110 *Social media and agenda setting: implications on political agenda, Norman Mustaffa. https://www.researchgate.net/profile/Normah_Mustaffa/publication/305391627_Social_media_and_agenda_setting_Implications_on_political_agenda/links/578ca2e108ae254b1de8440c/Social-media-and-agenda-setting-Implications-on-political-agenda.pdf*

111 *5 ways traditional media outlets are embracing sociem media, PR Daily https://www.prdaily.com/Main/Articles/5_ways_traditional_media_outlets_are_embracing_soc_11579.aspx*

112 *AFP and staff reporter, Outrage over sedition charge against Botswana journalist, Mail & Guardian, 11 September 2014. https://mg.co.za/article/2014-09-11-outrage-over-sedition-charge-agaisnt-botswana-journalist/*

113 *Reporters Without Borders, Botswana – A tight grip on the media, (2017). https://rsf.org/en/botswana*

114 *Freedom House, Freedom in the world – Botswana (2016). https://freedomhouse.org/report/freedom-world/2016/botswana*

115 *Safeguarding Civil Society // East Africa: Assessing Internet Freedom and the Digital Resilience of Civil Society in East Africa, Small Media https://smallmedia.org.uk/media/projects/files/SCSEastAfrica_2017_pywMkUK.pdf*

116 *"ZICTA shuts down internet cafes operating without trading licences," Lusaka Times, 29 October 2016, 30 June 2017, https://www.lusakatimes.com/2016/10/29/zicta-shuts-internet-cafes-operating-without-trading-licences-2/*

117 *ZICTA to mute local online anonymity on October 31, Zambians to merge their online alter ego's to their national physical identity, Zambia Business Times. https://zambiabusinesstimes.com/2016/10/30/zicta-to-mute-local-online-anonymity-on-october-31-zambians-to-merge-their-online-alter-egos-to-their-national-physical-identity/*

5.0 Internet Intermediaries and Internet Freedom

5.1 Limitation of Liability on Intermediaries

A Joint Declaration on Freedom of Expression and the Internet developed in 2011, recommends that no one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information; Liability should only be incurred if the intermediary has specifically been involved in the production of content, which is published online.[118] According to the UN Special Rapporteur on freedom of expression, censorship measures should never be delegated to a private entity and as such, no state should use or force intermediaries to undertake censorship on its behalf.[119] This section looks at how internet intermediaries deal with issues that affect internet freedom.

In some countries, the laws provide for the limitation of liability of intermediaries. In Ghana intermediaries are not liable for information stored on their systems "at the request of recipients of their services" on condition that they do not "have actual knowledge that the information or an activity relating to the information is infringing the rights of a third party (a person or the state)," are not aware of the circumstances surrounding the infringement and takes steps to make the information inaccessible upon a take-down notification. In Uganda, section 29 of the Electronic Transactions Act, 2011[120] provides that service providers are not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which the intermediary merely provides access.[121] The provision does not affect an obligation in a contract; licensing or regulatory framework which is established by law; or that imposed by law or a court to remove, block or deny access to any material.

Further, provisions that limit the liability of intermediaries for "hosting, caching, linking, or mere conduits" can be found in Ghana's Electronic Transactions Act, 2008 (Act 772),[122] in section 26 of Malawi's Electronic Transactions and Cyber Security Act, 2016, in Part X of Zambia's Electronic Communications and Transactions Act 2009,[123] and in Zimbabwe's Computer Crime and Cybercrime Bill. This clear limitation of liability for "hosting, caching, linking, or mere conduits" is missing from the laws of the DR Congo, Zimbabwe, Kenya, and Tanzania.

As such, a common approach by intermediaries to shield themselves from liability is through the development and enforcement of terms and conditions specifying their roles and responsibilities and those of their customers. Some intermediaries, such as the Zambian Watchdog[124] and Jamii Forums, have incorporated provisions in their terms and conditions that limit their liability for the actions of their users.

118 *Internet intermediaries: Dilemma of Liability: https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf*

119 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27*

120 *Electronic Transactions Act, 2011. http://www.ug-cert.ug/files/downloads/Electronic%20Transactions%20Act%20(Act%20No.%208%20of%202011).pdf*

121 *This will be so only if the intermediary is not directly involved in the making, publication, dissemination or distribution of the material; or a statement made in the material; or the infringement of any rights subsisting in or in relation to the material.*

122 *https://nca.org.gh/assets/Uploads/NCA-Electronic-Transactions-Act-773.pdf*

123 *"Electronic Communications and Transactions Act," Blackhall Publishing, 31 August 2009. http://www.zambialaws.com/Principal-Legislation/electronic-communications-and-transactions-act.html*

124 *"User Terms & Conditions for using the Zambian Watchdog Website," Zambian Watchdog. https://www.zambiawatchdog.com/user-terms-conditions/*

One of Jamii Forums conditions[125] states that it shall not be liable for any statement, misstatement, inaccuracy or omission of any type for any content submitted by a site member or visitor on any forum. Further, it states that it bears no responsibility for accuracy of comments of any participants and will bear no legal liability for discussion results. The Zambian Watchdog limits its liability for any damage or loss that might result from using its platform, including for any damage, loss or liability that results from the use of such content by any third party.[126]

It is important to note that the limitation of liability provided under statutes above does not affect the authority of regulators or courts to perform their functions or execute orders under any written law.

5.2 Imposition of Liability on Intermediaries

Despite the limits discussed above, some countries have developed laws that impose obligations and make intermediaries liable for their actions or inactions in certain circumstances. These are largely around general regulation and law enforcement purposes such as detection and investigation of crime and consequently, interception and surveillance.

Some laws make intermediaries liable for acts not committed by them. For example, in Burundi, article 30 of Law 100/97 of April 18, 2014 on electronic telecommunications, provides that operators of electronic communications are fully responsible for fighting fraud on their domains. Separately, article 53 of the Law No 1/15 of 9 May 2015[127] regulating the media, provides that media organisations are responsible for any articles published on their portals, even where the person published anonymously.

In order to stem opposition to interception and surveillance, states have criminalised the resistance or opposition to such actions. In the DRC, intermediaries are required to abide by the terms and conditions in their licences and to cooperate with law enforcement authorities in investigations. Article 50 of the Framework Law No 013/2002 on Telecommunications[128] states that the refusal to grant the requests of the authority may lead to the temporary or definitive withdrawal of the operating license or to other penalties. This buttresses Article 4 of the Decree Law of February 25, 1961, which provides that when it's a matter of national security, refusal to cooperate with law enforcement insinuates complicity and "presumption of guilt".[129] A consequence of such an approach was noted in Tanzania where, in December 2016, Maxence Mello, Director and Co-Founder of Jamii Forums, was arrested for refusal to disclose user data to the authorities. He was detained for a week without bail and then charged under section 22 and 32 of the Cybercrime Act for obstructing police investigations, and under the Electronic and Postal Communication Act (REPOCA) for managing a website not registered in Tanzania.[130]

The online news and discussion forum IWACU, was in June 2013 suspended by Burundi's National Communication Council (CNC) claiming that readers' comments on IWACU had violated legal provisions that prohibit "endangering national unity, public order and security, incitement to ethnic hatred, justification of crimes, and insults to the head of state."[131] IWACU suspended its website, but a consequence, it has since

125 *Jamiii Media, Terms of Services and Policies, Published Sept 10, 2006. https://www.jamiiforums.com/threads/jamiiforums-rules.18042/, https://www.jamiiforums.com/policy.php,*

126 *"User Terms & Conditions for using the Zambian Watchdog Website," Zambian Watchdog. https://www.zambiawatchdog.com/user-terms-conditions/*

127 *Law No 1/15 of 9 May 2015) came after the protest campaign conducted by the Union of Burundian Journalists against the previous Law enacted in 2013 (Law No 1/11 of 4 June 2013), http://www.presidence.bi/spip.php?article3779*

128 *Loi-Cadre N°013/2002 Du 16 Octobre 2002 Sur Les Telecommunications En Republique Democratique Du Congo http://www.daldewolf.com/documents/document/20151125094235-25_loi-cadre_n%C2%B0_013_2002_du_16_octobre_2002_sur_la_t%C3%A9l%C3%A9communication.pdf*

129 *DÉCRET- LOI 1-61 du 25 février 1961 relatif aux mesures de sûreté de l'État. - Droit de perquisition, d'internement et de mise sous surveillance http://www.leganet.cd/Legislation/Droit%20Judiciaire/DL.1.61.25.02.61.htm*

130 *Frontline defenders, Maxence M. Melo arrested and detained. https://www.frontlinedefenders.org/en/case/maxence-m-melo-arrested-and-detained*

131 *Burundi newspaper forum shut down, The Guardian, 4 June 2013. https://www.theguardian.com/media/greenslade/2013/jun/04/press-freedom-burundi*

introduced user guidelines dictating that comments should not violate laws and regulations. The site also prohibits content that is racist, anti-Semitic, defamatory or abusive, calling for ethnic and regionalist divisions, violates individual privacy and copyright. IWACU, further reserves the right to remove any comments likely to contravene its guidelines.[132]

In Uganda, section 79 of the Uganda Communications Act prohibits the unlawful interception and disclosure of communications of persons by an operator or employee of an operator of a communication service or system.[133] Also, section 80 makes it an offence for an operator or an employee to intentionally intercept, disrupt, deny accessibility to or to divert government communication. Service providers who fail to provide services that render real time and full time monitoring facilities for the interception of communication are liable to punishment with a fine of UGX 2,040,000 ($583) or imprisonment for a period not exceeding five years, or both; and a possible cancellation of their license.[134]

Moreover, section 20 of the Anti-Terrorism Act, 2002, provides that any person who knowingly obstructs an authorised officer in carrying out interception and surveillance commits an offence. Also, under the Anti-Pornography Act 2014, ISPs shall be liable if they do not use or enforce the procedure recommended by the Pornography Control Committee to control pornography and thus permit its download or upload through their service. Under section 7 of the Act, the Committee is empowered to expedite the development, acquisition and installation of software to detect and suppress pornography.

In Kenya, because of the broad nature of the legislation, intermediaries can be held legally responsible for content carried on or through their networks, which amounts to libel under the Defamation Act; copyright infringement under the Copyright Act; infringement of privacy, child pornography under the Sexual Offences Act, 2006; hate speech under the National Cohesion and Integration Act; prohibited publication or inciting material under the Penal Code. Under the Kenya Information and Communications Act, they may also be liable for intercepting messages, disclosing the content of messages, statements or accounts specifying the telecommunication services provided. Under the 2017 Guidelines for the Prevention of Dissemination of Undesirable Bulk Political SMS and social media content via Electronic Communications Networks, intermediaries can be held liable for spreading falsehoods, hate speech and insults. However, no penalties are prescribed in these guidelines. Also, under the Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010 a registrant shall bear liability for the infringement of third party rights and interest arising from holding or using a domain name in the country code top-level domain (ccTLD).

Zambia's Electronic Communications and Transactions Act 2009, provides for a "notice and takedown" procedure.[135] Further, it does not place a general obligation on a service provider to monitor unlawful activities within their platform and neither does it impose liability for the use of location tools by a service provider.

The implementation of demands by law enforcement often creates tensions between themselves and intermediaries. Where the intermediary fails to comply, law enforcement agencies can look into other laws or methods such as in the case of Jamii Forums, to enforce compliance with their requests. For larger intermediaries such as mobile network operators, the threat of withdrawal of licenses is sufficient leverage for authorities to have their way. This also informs the justification for such intermediaries not to produce transparency reports, as this might conflict with government interests, and consequently affect their ability to do business, should their licenses be revoked.

132 *Opinion, IWACU. See: http://www.iwacu-burundi.org/englishnews/the-nile-a-source-of-energy-food-and-water-for-all/opinion/*

133 *Uganda Communications Act http://www.ug-cert.ug/files/downloads/UCC%20Act%202013*

134 *See sections 2 and 3 of the Regulation of Interception of Communications Act.*

135 *See section 58 (1) (e) and section 61 of the Electronic Communications and Transactions Act, 2009 available at https://www.zambialii.org/zm/legislation/act/2009/21/psa2009172.pdf*

5.3 Restrictions Imposed by Intermediaries

Other than the statutory provisions, various intermediaries have put in place measures that define the terms and conditions to be observed by service and platform users. These contractual obligations or community standards, spell out acceptable and unacceptable conduct or activity informed by the need to comply with the laws of the specific country, or global best practice. The terms and conditions also stipulate the various actions the intermediaries may take following a breach of the conditions. This may be in the form of taking down content, blocking content from view to particular categories of users, or deactivating user accounts.

Some intermediaries such as ISPs and web hosts do not have elaborate terms and conditions that clearly specify the various types of prohibited content on their services. Some of those observed seem to align to national legislation by providing a general prohibition of "unlawful activities" in Botswana,[136] "criminal purposes" in Kenya,[137] or "illegal or unlawful activity" in DRC.[138] These can be construed, depending on the provisions of national legislation, to also deal with issues like violence against women, defamation, hate speech, terrorism, online child pornography and any other prohibited activities under such laws.

Some policies are more specific. The user policy of Botswana's BTCL prohibits the circulation of pornographic material, content promoting online violence against women, and calls for the blocking of known offending websites and social platforms.[139] In Ghana, the terms and conditions of the main telecom operators in the country such as MTN Ghana, Vodafone Ghana, Airtel Ghana, and Africa Online, restrict content such as virus or worm writing; transmitting defamatory, discriminatory or obscene material; child pornography; pirated software; harassing other subscribers; impersonation; interference of third party communications; and, fraudulent activities such as financial scams. Following the murder of an army official in May 2017 though a mob lynching, pictures and videos of the incident were circulated on social media. In June 2017, the Ghanaian government notified service providers including Facebook and Google to take down the pictures and the four related Uniform Resource Locator (URLs).[140] The police cybercrime unit also monitored social media sites in order to apprehend those sharing those pictures and videos.[141] Nonetheless, the video still appears on YouTube, with an age restriction based on the Community Guidelines,[142] amidst calls by the family and warnings by the government against further sharing of the video.[143]

Airtel DR Congo's terms and conditions

You agree that all messages sent and received by you comply with all applicable laws and regulations and that you are solely responsible for the content of all messages sent and received through the Service. You should not encourage, permit, or engage in any illegal or unlawful activity, including the transmission of obscene or abusive communications, the spread of computer viruses, infringement of copyright or publication of defamatory information.[144]

The Daily News, a Zimbabwean online newspaper, also requests users to refrain from using abusive, vulgar, racist, tribalistic, sexist, discriminatory and hurtful language when posting comments. Transgressors are barred from contributing to the online discussions. In Kenya, the terms and conditions or privacy policies of several local intermediaries including Liquid Telecom, Kenya Web Experts,[145] Jamii Telecommunication Ltd,[146]

136 *Terms & Conditions and Privacy Policy, BTCL. http://bdia.btcl.com.bd/registration/terms-and-conditions.jsp*

137 *Hai Terms and Conditions https://office.hai.co.ke/terms*

138 *Conditions generales de vent – Service Internet 3G, Airtel DR Congo http://www.africa.airtel.com/wps/wcm/connect/africarevamp/rdc/3g/home/term*

139 *Botswana Telecommunications Company (BTCL), State of Internet in Botswana research questionnaire response, 21 July 2017*

140 *Police to arrest those sharing videos of the gruesome murder of Capt. Mahama*
http://ghananewsonline.com.gh/police-arrest-sharing-videos-gruesome-murder-capt-mahama/

141 *http://kasapafmonline.com/2017/06/02/cyber-unit-monitoring-sm-sites-arrest-persons-circulating-capt-mahamas-murder-videos/*

142 *The Sad video of Captain Maxwell Adam Mahama #RiP. SUBSCRIBE for more UPDATES, YouTube. https://www.youtube.com/watch?v=X5QXtHZYiAQ&bpctr=1506248362*

143 *Government has begun removing graphic pictures and videos of Capt Mahama, Ghana news Online.*
http://ghananewsonline.com.gh/government-begun-removing-graphic-pictures-videos-capt-mahama/

144 *Conditions generales de vent – Service Internet 3G, Airtel DR Congo http://www.africa.airtel.com/wps/wcm/connect/africarevamp/rdc/3g/home/term*

145 *Terms of Service, Kenya Website Experts. https://kenyawebexperts.com/terms-of-service.php*

146 *Terms of User, Faiba. http://www.faiba.co.ke/terms-of-use*

Sasahost,[147] and Nation Media,[148] prohibit online violence, harassment of other users, defamatory content, pornography and content that is illegal or violates intellectual property or other local laws. These intermediaries also exempt themselves from liability in the event that users act on false/misleading information found on their platforms.

Meanwhile, the community standards of global social media platforms like Facebook prohibit bullying, harassment, intimidation, hate speech, threats, pornography or language that incites violence among others.[149] Twitter temporarily blocks or permanently suspends accounts that harass, intimidate, or use fear to silence other voices.[150] Further, Instagram restricts its users from posting violent, nude, partially nude, discriminatory, hateful, pornographic or sexually suggestive photos on its platform.[151] Defaming, stalking, bullying, threatening and impersonating others may also result in the termination of accounts on these platforms.

In May 2016, the YouTube channel NTV Kenya,[152] owned by NTV Kenya, a leading national broadcaster, was taken down in what YouTube referred to as multiple third-party copyright infringement complaints regarding material posted on the channel.[153] A popular Ugandan emailing list, Ugandans-at-heart (UAH), reportedly had its Facebook group with over 67,000 members closed by Facebook in December 2014 for breach of terms of service.[154] The group blamed government agencies keen on censoring speech on the platform for the action.[155]

A challenge that was noted is that while multinational companies such as Vodafone usually have user policies, terms and conditions published or easily accessible from the websites, the same is not the case for their local subsidiaries at national level. For instance, perusal of the websites of Vodacom in DR Congo and Vodacom in South Africa,[156] or MTN Global[157] and MTN Uganda,[158] showed that the telecommunications companies at global headquarters published general terms and conditions regulating the use of services, but those of the local subsidiaries terms were not readily available or accessible online. Further, it has been noted that user knowledge of the existence, and content of policies, terms and conditions generally remains low due to their lack of availability, the technical language in which they are drafted, and the limited efforts by the intermediaries to ensure user awareness of them.[159] This is an area that mobile network operators and ISPs can learn from Facebook and Google, for example, who are making efforts to make their terms simpler and readily available.

In addition, some intermediaries are implementing technical measures to restrict content. CBINET, an ISP in Burundi, provides a service called "Parental Control" on request to its subscribers which allows parents to block access to pornographic websites.

147 *Terms of Service, Sasa Host. https://www.sasahost.co.ke/terms-of-service*

148 *Terms of Service, Daily Nation. http://www.nation.co.ke/meta/1194-1186-byky1n/index.html*

149 *Community Standards, Facebook. https://www.facebook.com/communitystandards*

150 *Twitter Terms of Service, Twitter. https://twitter.com/en/tos*

151 *Community Guidelines, Instagram. https://help.instagram.com/477434105621119*

152 *https://www.youtube.com/user/ntvkenya*

153 *The Star, 'NTV Kenya's YouTube channel terminated for copyright infringement', 13 May 2016. http://www.the-star.co.ke/news/2016/05/13/ntv-kenyas-youtube-channel-terminated-for-copyright-infringement_c1350280 and Capital FM (Nairobi), 'Kenya: NTV Options After YouTube Shuts Down Channel', 25 May 2016. http://allafrica.com/stories/201605260674.html*

154 *Facebook shuts down Ugandans at heart page http://www.chimpreports.com/facebook-shuts-down-ugandans-at-heart-page/*

155 *Interview with James Wire, August 2017*

156 *"Terms and conditions: Plans, bundles, promotions, apps and Internet," Vodafone South Africa. http://www.vodacom.co.za/vodacom/terms/terms-and-conditions*

157 *Terms and Conditions https://www.mtn.com/en/Pages/Terms-and-conditions.aspx*

158 *Terms and Conditions http://uat.mtn.co.ug:81/internet/Mobile%20Internet/PublishingImages/Pages/Forms/AllItems/MTN%20Terms%20and%20Conditions%20and%20FUP%20for%20MTN%20%20Unlimited%20Internet%20010617.pdf*

159 *Should Internet-Based Firms Explain Terms and Conditions to Users?, https://cipesa.org/2016/10/should-internet-based-firms-explain-terms-and-conditions-to-users/*

5.4 Violation of Privacy Rights

5.4.1 Processing and Disclosure of Personal Information

Some intermediaries have developed privacy statements, policies and terms of service that indicate the steps taken to protect the privacy of users and outline the circumstances under which information may be disclosed to third parties. However, in the absence of data protection laws in all the focus countries, except Ghana, it is likely that intermediaries may collect or process more information than necessary, including for target marketing. It also leaves a lacuna in the oversight, collection, usage and security of personal information whether in the custody of governments or intermediaries.

User registration requirements are also in place at Jamii Telecommunications, an ISP[160] and the Nation media' Group in Kenya, where users are required to provide their name, phone number and email address.[161] Intermediaries like Mascom and Orange[162] in Botswana specify the circumstances under which user information may be disclosed to third parties including for law enforcement purposes, transactions processing, and quality of service provision.[163]

Over and above this, mandatory collection of personal information enforced through legislation is evident in SIM card registration provisions in all 10 countries, where users are required to submit their names, addresses, copies of national ID or passport and dates of birth. For example, in Uganda, following the introduction of the national identification registration system, the Uganda Communications Commission (UCC) directed re-registration of all SIM cards using the National IDs, a mandatory verification and validation against National Identification and Registration Authority database.[164] All the unverified, unvalidated SIM cards were switched off on August 30, 2017.[165] Similarly, article 3 of Burundi's Ministerial Law No 540/356 of March 17, 2016 obliges mobile operators to "take all the necessary measures" to verify if the SIM card users are the "real subscribers" and if they detect an anomaly, to block the SIM card. Telecommunications companies in Burundi are if found culpable, liable under article 29 of the Decree Law 100/97 of 18 April 2014 to a fine of BIF 5,000,000 (USD 2,900) for every unregistered SIM card in use.[166]

Consequently, states have also introduced legislation to prohibit intermediaries from disclosing the collected information. For example, section 17 of Botswana's Cybercrime and Computer Related Act also prohibits the unlawful disclosure by service providers of information collected, and provides a maximum penalty of P40,000 ($3882), or to imprisonment for a term not exceeding two years, or to both. Interference of user data is also an offence under Ghana's Electronic Communications Act, 2008.[167]

However, once the information is collected, governments and any other third parties, are required make lawful requests for user information typically through applications to courts of law, to obtain orders for the disclosure of the information. In Botswana, the legal procedure is provided for under the Cybercrime and Computer Related Act. In Burundi, the procedure is provided under the Ministerial Law No 540/356 of March 17, 2016 and in Article 92 of the Law No. 1/10 of 3 April 2013 on the reform of the Code of Criminal Procedure, but limited to the establishment of the truth during a criminal investigation. Also in Burundi, article 29 of the Law 100/97 of April 18, 2014 on electronic telecommunications, states that service providers should register subscribers, and they have the obligation to disclose those details to the regulator upon request.

160 *Terms of Use, Faiba. https://www.faiba.co.ke/terms-of-use*

161 *Subscribe Today, Daily Nation. http://subscribe.nationmedia.com/custompages/NationMedia/NationMedia_Subscriber.aspx?source=4&eid=b2e3bf7d-7dbe-4277-8e19-6250a4215dff*

162 *Orange privacy policy https://www.orange.com/en/Footer/legal-matters/legal/privacy-policy*

163 *Mascom, Privacy Policy Statement. https://www.mascom.bw/home/web/content/home/Mascom_Corporate_Services/Privacy_Policy_Statement*

164 *Extension of Sim card registration exercise, UCC. http://www.ucc.co.ug/data/dnews/133/PUBLIC-NOTICE:-EXTENSION-OF-THE-SIMCARD-VERIFICATION-EXERCISE.html*

165 *Unregistered Sim Cards to be switched off today midnight – UCC, The Spears News, August 30 2017. http://thespearnews.com/2017/08/30/unregistered-sim-cards-switched-off-today-midnight-ucc/*

166 *Portant fixation des conditions d'exploitation du secteur de communication électroniques http://www.presidence.bi/spip.php?article4674#*

167 *http://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf*

In Kenya, such procedures are provided under the National Intelligence Service (NIS) Act.[168] Further, section 89 of the Kenya Information and Communications Act provides the police power to enter and search premises, with a court order, and this extends to obtaining any article or thing, which can be construed to include customer data. Kenya published a Computer and Cyber Crimes Bill 2017, which now includes provisions of search and seizure of electronic evidence, expedited preservation of data, interception of content data, disclosure of traffic data, and mutual legal assistance. Further, section 8 of Ghana's Electronic Communications Act allows the National Communication Authority (NCA) to authorise network operators or service providers to disclose information such as: lists of its subscribers, including directory access databases, for the publication of directories or for other purposes that the Authority may specify.

However, such procedures can be flouted in cases of emergencies or other special circumstances. This was for instance, the case in Burundi.[169] However, in Zimbabwe, the courts have declared that the right to the privacy of one's communications was a right that existed even between spouses.[170]

Further, there is limited information on the number of requests made by governments to access user information in the custody of intermediaries. This opaqueness and secrecy has led to increased calls for accountability of intermediaries with regards to data protection, requests of user information and content takedowns. The response by intermediaries has been the publishing of periodic transparency reports. These reports have become vital to understanding censorship, surveillance and more importantly the commitment of service providers to protecting the privacy of their users and promoting freedom of expression online. These reports indicate a growing trend among countries, including African governments, of requests for subscribers' data and content removal.

However, based on the transparency reports alone, it remains unclear what the true extent of government's' surveillance of citizens' communications and censorship of content in the focus countries. The situation is further compounded by the existence of local laws that prevent the publication of this information on national security grounds. For instance, Vodafone is unable to publish statistics on its operations in Ghana and Kenya due to laws restricting the disclosure of information related to law enforcement.

5.4.2 Retention of Content Data

In some countries under review, it is not mandatory for intermediaries to retain data or content, while in others there are legal requirements to retain records. In Tanzania, it is not mandatory for intermediaries to retain content and associated information that is removed, filtered or blocked, unless specifically asked to do so. Some of the intermediaries interviewed from Tanzania indicated that they did not log user activity in any form as it would be an expensive and potentially useless undertaking as it only served to violate the privacy of their users.

Since there is no specific requirement to retain data, intermediaries in Tanzania retain data based on their own specific business needs and for such periods as they deem fit. Smart Telecom, a Tanzanian ISP, indicated that they tracked user activity online only to the extent necessary to ensure that the internet services were reliable and the bandwidth supplied was consistent. In Botswana, telecommunication companies such as Botswana Telecommunication Corporation Limited (BTCL) indicated that they keep call data and browsing records of its customers.

168 *Section 42 National Intelligence Service Act*

169 *Interview with a senior officer from Agence de Régulation et de Contrôle des Télécommunications (ARCT), August 2017*

170 *HH 190-16*

In other countries, the requirement to retain information is contained in legislation. The Kenya Information and Communications Act, for example, in its sections 83H and 83I, provides for the retention of electronic records and the retention of information in original form. Section 9-11 of Uganda's Computer Misuse Act also require service providers to store and preserve data for disclosure at a given time during criminal investigations.[171] In Zimbabwe, ISPs and telecommunications service providers are required under the Interception of Communications Act (ICA) to maintain records of users over a stipulated period. This includes call-related information, that is "information that identifies the origin, destination, termination, duration ... of each communication generated or received by a customer or user ... and, where applicable, the location of the user within the telecommunications system".[172] The challenge with this requirement is that it lacks oversight and clarity on its implementation and may lead to self-censorship.

5.4.3 Surveillance and Interception of Communication

Lawful interception of communications is provided for in a number of countries under review. A key concern is the installation of surveillance tools that would allow unrestricted surveillance without adequate legal safeguards or sufficient oversight from relevant bodies such as the Judiciary. This development is buttressed by the legislative provisions requiring the implementation of interception by operators.

In Uganda, the Anti-Terrorism Act 14 of 2002[173] and the Regulation of Interception of Communications Act[174] allow for interception of communications. The Regulation of Interception of Communications Act, 2010 provides for lawful interception and monitoring of communications in the course of their transmission through a telecommunication, postal or any other related service or system. Section 3 provides for the establishment of a monitoring centre under the oversight of a minister. The act also requires service providers to technically assist government to intercept communications by installing hardware and software to enable interception of communications at all time or when required. Service providers are also required to provide services that render real time and full time monitoring facilities for the interception of communication.[175]

Meanwhile, pursuant to the provisions of the Anti-Pornography Act, there have been reports of acquisition of a pornography detection machine in Uganda.[176] The machine is also seen as a means to crackdown on the use of Virtual Private Networks (VPN) use. It is estimated that at least 1.5 million VPNs were downloaded during internet shutdown on February 2016.[177]

According to Vodafone, all operators in the DRC have been required to allow the installation of a lawful interception capability in accordance with an order dated November 11, 2014 from the Agence Nationale de Renseignement (ANR), Congolese Intelligence Service Agency.[178] In Tanzania, a major telecom company indicated that it had not implemented technical requirements necessary to enable lawful interception and had not received any agency or authority demands for lawful interception assistance. Meanwhile, a middle-box was also detected in operation in Tanzania's StarTel an ISP, though it was not clear whether it was used for censorship or surveillance.[179]

171 *The Computer Misuse Act, 2011 is available at http://chapterfouruganda.com/sites/default/files/downloads/Computer-Misuse-Act-2011_0.pdf*

172 *See the Interception of Communications Act No. 6/2007 of Zimbabwe, section 2.*

173 *See also the Anti-Terrorism Act as amended 2015 and 2016 Part VII sections 18 to 22. The Anti-Terrorism Act is available at http://www.ulii.org/ug/legislation/act/2015/2002; www.vertic.org/media/.../Uganda/UG_Anti-Terrorism_Act_2002.pdf*

174 *The Regulation of Interception of Communications Act, 2010 is available at http://www.ulrc.go.ug/system/files_force/ulrc_resources/regulation-interception-communications-act-2010.pdf?download=1*

175 *See sections 2 and 3 of the Regulation of Interception of Communications Act.*

176 *Uganda's 'Pornography-Blocking Machine' Appears To Be Part Of A Darker Censorship Agenda https://www.iafrikan.com/2016/08/26/ugandas-pornography-blocking-machine-appears-to-be-part-of-a-darker-censorship-agenda/*

177 *VPN downloads in Uganda https://twitter.com/samirasawlani/status/700439009802264578*

178 *"Law enforcement Disclosure," Vodafone, 31 May 2017. http://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_law_enforcement_disclosure_country_demands_2015-6.pdf*

179 *Interview data collected from Small Media Organization, Research Manager. July 2017*

In Malawi, the government, through Malawi Communications Regulatory Authority (MACRA), is expected to commence the implementation of the Consolidated ICT Regulatory Management System (CIRMS), locally known as "Spy Machine". The machine is purportedly aimed at monitoring mobile phone service providers to ensure quality of service and fair pricing. Its implementation was challenged in the High Court by civil society organisations and mobile phone service providers over fears of compromising the privacy rights of users under Article 21 of the Constitution.[180] However, the Supreme Court overturned[181] the High Court decision thus paving the way for MACRA to install the machine by September 2017.[182]

In Kenya, section 36A of the Prevention of Terrorism Act permits the interception of communication by National Security Organs for the purposes of "detecting, deterring and disrupting terrorism" in accordance with procedures yet to be prescribed by the Cabinet Secretary. In January 2017, the Communications Authority of Kenya (CA), having procured a Device Management System (DMS), sought to install a link at the data-centre or mobile switching room of mobile operators to integrate core network elements to the solution.[183] The system was aimed at identifying stolen, counterfeit and non-type-approved phones. However, implementation of the system was halted following a court case[184] where it was alleged that its capabilities extended to interception of calls and text messages.

In March 2017, it was reported that middleboxes may exist on Kenya's Safaricom network,[185] a claim the operator disputed. A recent report revealed that law enforcement officers from the Directorate of Criminal Investigations (DCI) are embedded within mobile network operators to extract and provide user information, then seek warrants later. It was also revealed that the Communications Authority of Kenya procured HIWIRE technology which allows for the capture and analysis of open-source traffic including on social media.[186]

In Burundi it was not immediately clear whether such systems existed. However, Burundi's Ministerial Law No 540/356 of 2016 supports surveillance. A speech by the Minister in charge of Public Security in May 2016 triggered suspicion over government surveillance as it indicated that the sector regulator and service providers should monitor social media, arrest and prosecute individuals misusing platforms.[187] In August 2016, 56 people who were members of a WhatsApp political discussion group were arrested in Bujumbura, Burundi, which reinforced suspicion of government surveillance capability. 46 of them were released but 8 members of the group were detained and were accused of "sending out libellous and insulting writings against institutions and authorities on the social media networks".[188] The arrests and detentions were widely condemned, but they have not deterred the use of Whatsapp, which remains a major source of news on social and political developments in the country, given the clampdown on independent print and broadcast media.[189]

There is concern in DR Congo over the implementation of mass surveillance measures by government agencies without judicial oversight. In May 2017, a New York Times article revealed that Congolese National Intelligence Agency had recorded a phone conversation between a United Nations (UN) contractor and a Congolese Member of Parliament.[190] The Prosecutor General of the Republic admitted to the press that he

180 *"Spy Machine" Brings Telecoms Fears: http://www.biztechafrica.com/article/spy-machine-brings-telecoms-fears/1437/*

181 *Court Nods to Macra's "Spy Machine": http://mwnation.com/court-nods-to-macras-spy-machine/*

182 *Macra Unleashes Spy Machine: http://zodiakmalawi.com/top-stories/macra-unleashes-spy-machine*

183 *Muthoki Mumo, Daily Nation, 'Monitoring of mobile phone networks to take effect - agency says', 18 February 2017. http://www.nation.co.ke/news/Agency-to-proceed-with-communication-surveillance-plan/1056-3817532-lvjbez/index.html*

184 *Geoffrey Mosoku, Standard Media, 'Cord joins bid to stop state's phone tapping plan', 27 February 2017. https://www.standardmedia.co.ke/article/2001230835/cord-joins-bid-to-stop-state-s-phone-tapping-plan*

185 *Middle-boxes usually assume dual-use character in that they can be used for legitimate functions (e.g. network optimisation) while simultaneously being used for traffic manipulation, surveillance and aiding censorship.*

186 *Privacy International, 'Track, Capture, Kill' March 2017. https://privacyinternational.org/sites/default/files/track_capture_final.pdf*

187 *State of Internet Freedom in Burundi 2016: Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights, 2016. See: https://www.opennetafrica.org/?wpfb_dl=60*

188 *Burundian government cracks down on WhatsApp group, IOL News, see: https://www.iol.co.za/news/africa/burundian-government-cracks-down-on-whatsapp-group-2060657*

189 *State of Internet Freedom in Burundi, 2016, CIPESA. https://cipesa.org/?wpfb_dl=230*

190 *KIMIKO de FREYTAS-TAMURA and SOMINI SENGUPTA, "For 2 Experts Killed in Congo, U.N. Provided Little Training and No Protection," The New York Times, 20 May 2017. https://www.nytimes.com/2017/05/20/world/africa/congo-zaida-catalan-michael-j-sharp-united-nations-democratic-republic-of-congo.html*

was not aware of the intelligence agency's interception activities before the New York Times article,[191] but added that there were more individuals under surveillance.[192]

On the other hand, some of Ghana's provisions provide a useful example of an enhanced threshold for interception and surveillance orders. In its Anti-Terrorism Act, 2008 it allows a senior police officer (not below the rank of an Assistant Commissioner of Police) with the written consent of the Attorney-General (AG) and the Minister of Justice to apply to a court for an order to require the interception of communications for the purpose of obtaining evidence of commission of an offence under the Act. However, under, section 100 of the Electronic Communications Act, it is the President permitted to make written requests and issue orders to operators or providers of electronic communications networks or services requiring them to intercept communications, provide any user information or otherwise in aid of law enforcement or national security. The framework under the Anti-Terrorism Act provides several oversight mechanisms, unlike the latter procedure under the Electronic Communications Act, which lacks sufficient oversight as the exercise of such powers are exclusively at the President's discretion.

Governments were also noted to be implementing technical measures to censor content. The Ugandan government is believed to be working on a proposal to limit the number of internet gateways by requiring that they are routed through the Uganda Internet Exchange Point (UIXP).[193] Other proposals include requiring the hosting of content, websites, databases, and any other applications within the country. Such a move would allow greater government control and monitoring ability of internet traffic and content from an infrastructure level. On June 6, 2017, www.desc-wondo.org, a DRC website publishing military and political analysis, was blocked and was only accessible through the use of VPNs. The website was accessible a month afterwards but nobody claimed responsibility for tampering with it. The website owners indicated that it was not the first time the website was blocked and encouraged users to use VPNs to circumvent the blockage.

5.4.4 Poor Accountability of Intermediaries

Whereas a growing number of intermediaries with operations across the globe issue transparency reports, only a few operators on the continent release such reports. According to a CIPESA Policy Brief in July 2017, Orange has reported on the approximately 1,000 user information requests made Botswana and a similar number by DR Congo.[194] The brief further states that Vodafone reported on the 933 metadata requests made by Tanzania, and the 506 requests made by DR Congo in 2015.

In 2016, the brief notes that several governments made information requests regarding user accounts to Facebook, Google and Twitter. For example, Facebook reported on a total of 40 requests by Ghana, Kenya, Uganda and Tanzania with Botswana alone accounting for 21. Since 2013, Google has reported on the user information requests received from Ghana and Kenya. Twitter also granted user information or content removal requests and "emergency requests", made by Kenya.

The Luxembourg-based Millicom operates in five African countries – Chad, Ghana, Rwanda, Senegal and Tanzania, all under the Tigo brand, having sold its DR Congo operations to Orange in 2016. Millicom states that it received a total of 5,000 metadata requests in 2015 and 7,000 in 2016 from governments in the countries in which it operates. The number of interception requests received by Millicom from African governments was the same for both years five, while those related to Mobile Financial Services decreased by 28 from 354 in 2015 to 326 the following year. Millicom does, however, acknowledge that its 2015 and 2016 request figures are not directly comparable as the figures recorded in 2015 include requests made by the government of DR Congo, while 2016 excludes this data but includes requests made to Zantel. In its transparency reports, Millicom does not publish data regarding compliance to any of the requests received.

191 *Actualite.CD Live Tweet, Twitter, 26 June 2017. https://twitter.com/actualitecd/status/879292792715038721*

192 *Christophe Boisbouvier, Alexis Thambwe Mwamba: en cas de convocation, «je me rendrai» chez le juge, Radio France International, 21 June 2017. http://www.rfi.fr/emission/20170621-cas-convocation-juge-rendrai-declare-alexis-thambwe-mwamba*

193 *EXCLUSIVE: Leaked Document Reveals UCC Proposal to Limit International Gateways http://pctechmag.com/2017/01/exclusive-leaked-document-reveals-ucc-proposal-to-limit-international-gateways/*

194 *The Growing Trend of African Governments' Requests for User Information and Content Removal From Internet and Telecom Companies, CIPESA Policy Brief July 2017. https://cipesa.org/?wpfb_dl=248*

In its 2016 Annual Sustainability Report, MTN reaffirmed its support for human rights including access to information, freedom of expression, privacy and security of its users' communications and information.[195] However, despite being one of the largest service providers in Africa with a presence in 19 countries, it provides no information about how it handles requests from governments and private parties for user information or surveillance support. Similarly, MTN provides little information about its processes for handling such requests. It also does not disclose any data about the number of requests it receives or complies with, which places it a rank lower than the likes of Millicom, Vodafone, and Orange when it comes to transparency about its policies relating to users' freedom of expression and privacy. In countries like Zimbabwe, the government's interest in leading operators such as NetOne and Telecel likely hinders transparency efforts.

Whereas companies such as Google, Facebook and Twitter can be commended for periodic and disaggregated disclosure, more could be done in terms of frequency of the reports and details on specific cases. Facebook's report also includes requests related to other Facebook products such as Messenger, WhatsApp and Instagram.[196] These intermediaries also provide notifications to users whenever their content is reported or usage restricted. Besides the case of Jamii Forums in Tanzania cited above, where the forum was bold enough to publicly resist to disclose user information, none of the local intermediaries in the other countries had in place such measures - often proceeding to moderate or altogether remove content use without notification. In its list of commitments, Orange DR Congo indicated that it has signed up to GSMA's Mobile Alliance Against Child Sexual Abuse Content, set up to combat child pornography on the internet.[197] Intermediaries are also encouraged to embrace emerging best practice and also implement UN Guiding Principles on Business and Human Rights.[198]

5.5 Inadequate Complaint Handling Frameworks and Remedies

In most of the countries surveyed, there are no separate procedures for reporting complaints arising out of the violation of rights online. Therefore, the usual channels such as the police, for criminal complaints; copyright agencies for intellectual property offences; and specialised agencies e.g. National Cohesion and Integrity Commission in Kenya for hate speech. Internet intermediaries e.g. Facebook, Twitter and YouTube have developed specialised technical mechanisms within their platforms for reporting complaints, which are also handled within their platforms by their respective departments.

Social networks such as Facebook, Twitter, Instagram and Google services like YouTube, offer robust complaint handling mechanisms for their users to report any misconduct on their web-based platforms and their various applications. They are uniquely advantaged given the fact that users spend time on their online platforms to use the services as opposed to ISPs and telecommunication companies, who users only visit their websites mostly when they have queries. Nonetheless, the complaint handling mechanisms of these global intermediaries can be improved to provide a variety of reporting options for complaints as opposed to the limited number of categories that exist, which might not take into account the nuances within each country in which they operate.

Several telecommunication companies and Internet Service Providers offer users 24-hour call support or physical assistance in their offices. Others such as Safaricom in Kenya, have made use their website and social media platforms such as Facebook and Twitter, to receive and follow-up on customer complaints with their services. Some of the intermediaries though do not provide adequate support from their websites

195 *MTN Sustainability Report, 2016. https://www.mtn.com/MTN%20Service%20Detail%20Report%20archive/MTN%20Group%20Sustainability%20Report%202016.pdf*

196 *About the report, Facebook. https://govtrequests.facebook.com/about/*

197 *https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance*

198 *UN Guiding Principles on Business and Human Rights. See: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf*

making it difficult for aggrieved clients to get in touch with them. Further, where the complaints relate to civil or criminal matters, users are directed to local law enforcement, especially in countries where there isn't a proper notice and takedown procedure. This has its challenges in the sense that some local law enforcement do not have the capacity to respond to complaints that emanate from the online environment.

Laws in some of the countries under review, are yet to provide sufficient remedies to tackle new forms of crime online. Incidences of cyber harassment and stalking especially of women, cyber bullying on social media networks are common. An example is an incident involving viral video capturing the verbal harassment and undressing of a woman in Botswana in May 2017 by a group of men because of her dress code. Although the police case was opened and investigations, the case is yet to be concluded.[199] In Tanzania, there was concern in June 2017 over the posting on YouTube, Facebook and Instagram of a viral video of a woman being harassed by men for wearing a miniskirt during the fasting season of Ramadan.[200] While the YouTube video has since been taken down, the episode constituted harassment of women, and no reliefs were available to the victim.

In the circumstances, users do not have sufficient protection or remedies for the violation of their rights while using the services of intermediaries. They are in most cases victims of the business interests of the service providers on the one hand, and the demands by government on the other. This is further complicated by the absence of updated legislation or clear and comprehensive procedures by intermediaries to address such complaints as and when they arise.

5.6 Pushback Against Violations and the Promotion of Rights

In some of the countries there have been actions by civil society groups, and other actors to respond to the challenges in order to improve the protection of, and defend human rights.

In DR Congo, telecommunication operators made a statement exposing irregularities contained in a proposed ICT bill in 2017. The Ministry of ICT acknowledged their submissions opposing the reinforcement of "exclusivity" of reference network favouring the state, and the reinforced power of the national intelligence agency.[201] Further, in December 2016, 33 Congolese civil society organizations spoke out against what they called "violation of freedom of expression of foreign media operating in DRC and the establishment of a strong control of NGOs in DRC".[202] In February 2017, explicit images of well-known public figures in the DRC leaked online igniting public calls for them to be blocked given the conservative and religious nature of Congolese society.[203] An online campaign through hashtag #JeNeVeuxPasVoir,[204] meaning "I don't want to see" was stated on Facebook and Twitter calling on others not to share those images but to delete them from their devices.

Over the past 3 years, Google has declined 63% of the of 21 requests made by Kenya relating to 32 user accounts. In June 2016, Kenya's Safaricom declined to provide unrestricted access to the Kenya Revenue Authority (KRA) of user information and records relating to its mobile money platform MPesa.[205]

199 *Lebogang Mosikare, Lesedi Mkhutshwa, BBTTA condemns stripping of women, Mmegi Online, 26 May 2017. http://www.mmegi.bw/index.php?aid=69102&dir=2017/may/26*

200 *Harassment of a woman in Kariakoo City Market during the fasting season of Ramadan. https://www.youtube.com/watch?v=WSK5hvxnKCE*

201 *"Le projet de loi sur les télécommunications et les TICs en RDC inquiète les opérateurs du secteur," Radio Okapi, 29 April 2017. http://www.radiookapi.net/2017/04/30/actualite/societe/le-projet-de-loi-sur-les-telecommunications-et-les-tic-en-rdc-inquiete*

202 *"RDC : l'accord politique s'attaque aux libertés d'expression, dénoncent 33 ONG," Radio Okapi, 21 October 2016. http://www.radiookapi.net/2016/10/21/actualite/politique/rdc-laccord-politique-sattaque-aux-libertes-dexpression-denoncent-33*

203 *"Sextape: entre victimes condamnables et condamnations sélectives", Politico.CD, 25 February 2017. http://www.politico.cd/actualite/la-une/2017/02/25/sextape-entre-victimes-condamnables-condamnations-selectives.html*

204 *Twitter search of #JeNeVeuxPasVoir campaign https://twitter.com/search?q=%23JeNeVeuxPasVoir*

205 *Safaricom rejects bid for free access to taxpayers MPesa, Business Daily http://www.businessdailyafrica.com/news/Safaricom-rejects-KRA-bid-for-free-access-to-taxpayers-M-Pesa/539546-3251892-99ywedz/index.html*

In opposing the move by KRA to bypass the court process, the company cited the provisions of the Constitution and the National Payment Systems Act, 2011 as barring it from disclosing such information without court orders. However, Safaricom usually does grant lawful requests for information approved by the Courts. An official from a Burundi ISP indicated that the company declined a government request to install surveillance equipment in their network.

Civil society groups in Kenya have also undertaken in advocacy to develop sector laws and policies; litigation against unconstitutional legal provisions; training and engagements on internet rights, child online protection and fake news, and online safety of women. Academic institutions also conduct research on ICT and intellectual property. The Communications Authority and Ministry of ICT have, in the processes of developing new legislation, collaborated with other actors in the training of lawyers, law enforcement and judicial officers. In June 2017, online activism and reports by Kenyans on Twitter (@kot, #KOT) led to the suspension of the Twitter account of @kimindiri for posting nudes photos of his ex-girlfriend on his timeline.[206] In August, 2016, the Kenyan High Court awarded Roshana Ibrahim, a former Miss World Kenya 2016 model, Kshs 1 million in damages for breach of privacy after her nude photos were leaked by former partner Frank Zahiten.[207]

Civil society in Malawi were also credited with the passing and enactment of the Access to Information Act, 2017.[208] The process took 12 years of advocacy for the government enact the law. In addition, freedom of expression campaigners such as MISA Malawi[209] continue to defend and advocate for favourable legal framework for the protection human rights. In Zambia, whereas Civil society organisations have not been outspoken on internet freedom, they have raised alarm about the suppression of press freedom and freedom of expression in the country. A number of CSOs continue to issue statements expressing concern and discontent over the deteriorating state of press freedom and freedom of expression in the country.[210]

Katswe Sistahood a Zimbabwean civil society organisation[211] and some individual activists started a campaign in 2016 to raise awareness and advocate for the criminalisation of non-consensual distribution of intimate images, commonly known as 'revenge porn' as a form of violence against women online. The organization also petitioned Parliament to amend the law, a process that is still ongoing.

206 *Eddy Kagera, Nairobi News, KOT DISH OUT POETIC JUSTICE ON MAN WHO TWEETED HIS BABY MAMA'S NUDES, 16 June 2017. http://nairobinews.nation.co.ke/news/kot-baby-mamas-nudes/*

207 *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others [2016] eKLR. http://kenyalaw.org/caselaw/cases/view/129282/*

208 *This Law is available at https://www.malawilii.org/mw/legislation/num-act/2017/13/num_act_2017_13.pdf*

209 *Media Institute of Southern Africa: http://malawi.misa.org/resource-centre/access-to-information/*

210 *Media Institute of Southern Africa, "Zambia Chapter, 4th quarter 2016 State of the Media Report" MISA Zambia, 31 December 2016. http://crm.misa.org/upload/web/State%20of%20the%20Media%202016%20Q4_Final_Version.pdf*

211 *https://www.facebook.com/KatsweSistahood*

6.0 Conclusion and Recommendations

6.1 Conclusion

Internet freedom is still under siege, and despite the progress made so far, countries in Africa still have additional hoops to jump before internet freedom is fully realised and enjoyed openly, freely and securely in the continent.

The ever-increasing interest and persistence by governments to implement measures that limit the rights to freedom of expression, information and rights to privacy remains of concern. The incidences highlighted above indeed do demonstrate the extent of freedom of expression and privacy violations in the countries under review. It has been observed that not only are governments amending the laws to enable censorship and surveillance, they are also making significant investments in technical measures to achieve their ends. While states will not willingly reveal the extent of the censorship and surveillance, it is evident that the online activities of users are indeed tracked as governments have the capacity to access information with or without the facilitation of local intermediaries. And where intermediaries are aware, they are gagged.

The problem, is that despite the public interest and good intentions of the governments to provide security, fight crime and maintain law and order in their respective countries, such measures should not be implemented in direct violation of human rights. Further, laws should not be used to perpetuate illegalities or for political expediency.

Intermediaries on the other hand, have important roles to play. Whereas their difficult position is understood, they have been noted to put their economic interests ahead of the interests of their customers. It is not enough for intermediaries to blame governments or acquiesce to bad practices by governments. It is also noted that measures imposed by governments impose an additional cost burden on intermediaries, while those directly implemented by the government are a burden on the taxpayer.

Governments and intermediaries alike should strive to uphold human rights by insisting that laid down processes and procedures are followed. The policies, practices and procedures adopted by intermediaries should be transparent and accountable. Efforts should be put in place towards a common approach and standardise the policies. In addition, civil society should as part of their mainstream work, actively and keenly monitor and highlight these practices, including government procurement that threatens human rights. All stakeholders should challenge the enforcement of bad laws, including policies and practices by intermediaries.

Finally, emphasis should be placed on improving access to the internet and making the online space free, open and secure, while respecting human rights. Further, compliance with international human rights standards, including the three-part test provided by the Report of the Special Rapporteur on the Promotion and Protection of the right to Freedom of Opinion and Expression, and the UN Guiding Principles on Business and Human Rights already cited above, are crucial starting points and a useful compass to safeguard human rights online.

6.2 Recommendations

From the foregoing discussion and research findings, a number of recommendations can be drawn for the specific stakeholders in order to promote intermediaries' ability achieve internet freedom in the reviewed countries. They include the government, ICT companies, the media, academia, technical community and civil society.

6.2.1 Government

- Fast-track the development, review and adoption of policies and legislation on media and telecommunications sectors to ensure they comply with international human rights standards, including protecting the rights to privacy, information and freedom of expression in an online environment; provide for 'notice and takedown procedures', and new cyber offences.
- Take steps to review and comply with best practices contained in the: African Declaration on Internet Rights and Freedoms and Budapest Convention on Cybercrime and the UN Guiding Principles on Business and Human Rights.
- Engage in open and candid public and private discussions through a multistakeholder approach for instance, in IGFs, with other arms of government, companies, civil society, academia, technical community, public and other key stakeholders in the process of regulating the ICT sector in order to promote transparency and accountability and build trust in a conducive environment.
- Should not unnecessarily, mandatorily or arbitrarily undermine or restrict Internet freedom through practices such as filtering, content controls, surveillance, information requests, outside the allowable legal limits. Further, decisions on such issues should be publicly accessible.
- Conduct awareness campaigns for the public on online safety, cyber offences and the available remedies for victims. The capacity of law enforcement officials should also be enhanced to enable them detect and investigate cybercrimes.
- Collaborate with intermediaries and other stakeholders to develop and implement effective complaint reporting frameworks and remedies for victims for the violation of their rights online.
- Promote improved access to the broadband Internet and ICTs, by ensuring reasonable costs, sufficient infrastructure and quality of service by intermediaries.
- Ensure political stability and respect for democracy in the country which is a key for the development of ICTs.
- Develop local capacity and promote research on ICTs to inform policy and law making.

6.2.2 Intermediaries

- Review and jointly develop common or standard policies, practices and terms and conditions that respect internet freedom and comply with UN Guiding Principles on Business and Human Rights.
- Simplify their policies and terms and conditions for their users or customers, and include information on available content restrictions, the processes through which information requests or takedowns are handled, and how user data in their custody is protected.
- Intermediaries including banks should educate their customers on cybercrimes such as phishing, encryption, passwords etc. to protect their privacy.
- Publish comprehensive and standardised transparency reports on a regular basis to demonstrate their accountability and transparency in the implementation of their policies, processes and actions regarding user information or content while detailing government requests and the compliance rates.
- Embrace self-regulation and the responsibility to police their services by developing and implementing terms of service and community standards that promote internet freedom and human rights generally while also providing safeguards and remedies for their users including the vulnerable groups online such as women and children.
- Regularly update and communicate to users or clients the changes made to policies and the terms and conditions or of service.
- Allow users to use their services anonymously and without links to their government-issued identity.
- Resist unjustified, irregular and unlawful restrictions of the internet or demands by governments. Only implement lawful orders or requests.
- Review tariffs to promote access to the internet by the public.

6.3.3 Media

- Media houses should defend media freedom and protect their journalists to enable them work without fear of job loss, harassment or intimidation.
- Journalists should be sensitised on digital safety.
- Defend internet freedom through its role as a government watchdog.
- Inform, educate and mobilize the public to practice and demand for internet freedom.
- Adhere to professional ethics to ensure their platforms are not used to violate rights of others.
- Implement safeguards on their platforms to ensure the content therein doesn't contribute to the violation of the rights of others.
- Highlight violations on internet freedom and support advocacy initiatives to promote internet freedom.

6.3.4 Academia

- Conduct research and produce well informed papers on emerging issues to influence policy, legislation and regulatory actions by the state and its agents.
- Disseminate research findings and educational materials to the public in simple and popular publications that can be easily understood, including on the proper use of the internet and how to defend their rights online.
- Be strong advocates of internet freedom and support actions by other stakeholders by providing critical information and intellectual contributions to their causes.

6.3.5 Technical Community

- Develop cost-effective software and programmes that will enhance internet usability and access by more citizens.
- Develop local technological solutions and platforms to enable people effectively engage in technological developments and the corresponding usage with minimal threats.
- Develop innovative technologies to advance internet freedom and circumvent inter alia, restrictions and surveillances.
- Conduct Cyber Security trainings for the stakeholders including the public to raise their awareness levels on emerging concerns such as cloud computing, malware, social media etc.

6.3.6 Civil Society

- Implement education and sensitization programmes for the public on areas such as: internet rights, cyber safety, cyber-bullying in schools, child protection, roles of intermediaries,
- Develop programmes to monitor human rights violations on online platforms and also highlight and respond to cases of cyberbullying, VAW, hate speech etc.
- Advocate for media freedom and against practices such as harassment, intimidation or arrests of journalists.
- Engage in the formulation and implementation of policies and laws to safeguard online rights including expression, information and privacy.
- Challenge policies, laws and practices that undermine human rights on the internet, with the same vigour as other human rights.
- Engage government, its various arms and agencies, and all other stakeholders to promote good governance, including of the internet.
- Recognise the importance of, and prioritise telecommunications as a mechanism for the protection of human rights.
- Hold government and intermediaries such as telecom companies accountable for their actions.
- Get more civil society involved in the defence of online rights.

6.3.7 Public

- Continue to engage all stakeholders on the issues that affect them.
- Learn about digital security and build solidarity and support each other especially the victims of online offences, and those persecuted or whose rights are generally violated online.
- Learn about the laws, rules and standards that govern online spaces and have the discipline of not abusing them.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, 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