State of Internet Freedom in zimbabwe 2019

Mapping Trends in Government Internet Controls, 1999-2019

January 2020

CIPESA

Table of Contents

1 **Introduction** 4
- 1.1 Introduction 4
- 1.2 Aim of the Study 5

2 **Methodology** 6

3 **Country Context** 7
- 3.1 ICT Status 7
- 3.2 Political Environment 8
- 3.3 Economic Status 8

4 **Results** 9
- 4.1 Key Trends of Internet Control Measures in Zimbabwe Over Successive Periods 9
  - .1 Weaponising the Law to Legitimise Actions 9
  - .2 Disrupting Networks – From Social Media Blockage to Internet Throttling 14
  - .3 Surveillance Galore: The Build-Up of States' Capacity 14
  - .4 The Push Towards Determining Identity Amidst Poor Oversight 16
  - .5 Enter the Era of Social Media and Data Taxation 17
  - .6 Deploying Bots, Cyberattacks and Disinformation 18
- 4.2 Key Positive Developments 19
  - .1 Robust Advocacy and Push-back by Non-State Actors 19
  - .2 Repeal of Repressive Legislation 19

5 **Conclusion and Recommendations** 15
- 5.1 Conclusion 15
- 5.2 Recommendations 16

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in Zimbabwe tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. Other country reports for Bostwana, Burundi, Cameroon, Chad, the DRC, Ethiopia, Kenya, Malawi, Nigeria, Rwanda, Senegal, Tanzania, and Uganda. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

CIPESA recognises Natasha Msonza as the main content contributor to this report.

The research was conducted with support from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the Federal Ministry for Economic Cooperation and Development (BMZ).

Editors
Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

State of Internet Freedom in Zimbabwe 2019
Published by CIPESA,
www.cipesa.org
January 2020

1 Introduction

1.1 Introduction

'Digital authoritarianism' – a term coined by Freedom House[1] has become the latest buzzword describing the many ways governments around the world are seeking more control over users' data and behaviours online. As in many African countries, Internet freedom in Zimbabwe has been on the decline over the past years.[2] For a long time Zimbabwe has been classified as a dictatorship, and this has partly contributed to efforts by the government to control public narratives, especially those taking place on the Internet.

In the last 20 years, the Zimbabwean government has adopted policies and practices as well as introduced repressive controls with potential to restrict or affect Internet freedom. It has employed several measures to control Internet usage through among others censorship and monitoring online communications under the guise of safeguarding national security. Specifically, the government has invoked various strategies that include: engineering repressive legislation and policies; increasing surveillance capabilities; facilitating network interference; content blocking and filtering; financial disincentives and deployment of ideological state apparatus advancing curated government narratives and criminalization of individuals' online activities. Most of these measures aimed to quash critical and dissenting voices.

Regressive legislation, including the Interception of Communications and the Access to Information and Protection of Privacy Acts passed in the past 20 years seek to thwart or criminalise online dissent, criticism of the current ruling dispensation and all forms of organising. There has been a marked increase in enhanced surveillance programs and partnerships with foreign governments and private sector actors, often with limited oversight. In recent times, activists and opinion leaders are increasingly being targeted for their online activities, sometimes culminating in arrest or physical harassment. The Zimbabwe government is no stranger to implementing strategies that are being used by other autocratic governments elsewhere to restrict Internet freedom. Such strategies include attempts to regulate sections of the media, social media; content blocking or filtering; bandwidth throttling; partial Internet blackouts or total shutdowns.

1 *Adrian Shahbaz, "The Rise of Digital Authoritarianism: Fake news, data collection, and the challenge to democracy," Freedom House, https://freedomhouse.org/report/freedom-net/freedom-net-2018*
2 *According to Freedom House report: https://freedomhouse.org/country/zimbabwe/freedom-net/2019*

The Zimbabwe government has also been on a path to integrate[3] ICT services in government functions, including introduction of digitalization, e-government and digital identity programmes that require citizens to provide detailed personal information, including biometrics for voter registration records, national identity registration etc. Like many governments, Zimbabwe has mandatory SIM card registration regulations for mobile service subscribers. Unfortunately, few citizens are fully conscious of the implications of several measures implemented by the government in relation to digital rights, simply because the prevailing socio-economic and political environment takes great attention away from these matters.[4] In a push to control the political narrative especially on social media, the government has in incorporated some draconian provisions in the upcoming Cyberlaw tagged as an endeavour to fight fake news and protect national security. For instance in the 2018 election period, Zimbabweans witnessed a new phenomenon of government-backed Internet trolls and paid influencers whose sole purpose was to sway political conversations, spread fake news and advance the government and ruling party narratives using all manner of aggressive means, including stalking, harassing and hounding opinion leaders until they go offline.

As digital authoritarianism grows on the continent, measures introduced have seen a decline in democracy and internet freedom. There is thus an urgent need for Zimbabwean citizens and civil society to pay more attention to developments happening in the regulation or attempts to regulate cyberspace.

1.2 Aim of the Study

The research sought to document government controls and their effect on the levels of internet freedom in Zimbabwe. It traces trends of government regulation and control over a 20-year period, stretching from 1999 to 2019. The study focuses on the proliferation of retrogressive and repressive policies and laws and surveillance capacity of the Zimbabwe government; digitization programmes; censorship; and; new frontiers like the introduction of Internet related taxes. The findings will inform key stakeholders such as law and policy makers, media, academia, technologists, civil society and researchers on the precautionary measures to undertake to better Zimbabwe's digital environment.

3 Aome Rajah, E-Government in Zimbabwe: An Overview of Progress Made and Challenges Ahead, Journal of Global Research in Computer Science, Volume 6, No. 12, December 2015, http://www.rroij.com/open-access/egovernment-in-zimbabwe-an-overview-of-progress-made-and-challenges-ahead-.pdf

4 Key informant interview conducted with Zororo Mavindidze on 3 July 2019.

2 Methodology

This study employed qualitative research methods. Qualitative research was considered most appropriate because in large part the research seeks to discover the correlation between policy and legal frameworks governing Zimbabwe's ICT sector and the state of internet freedom in the country. The study employed a combination of literature review and stakeholder analysis. This was deemed the best way of gauging a historical understanding of the sector to develop an in-depth understanding of factors that have driven the telecommunication sector over the years.

Specifically, the study analysed the country's policy and legal frameworks as well as the international legal framework governing the ICT sector. Further, the study analysed existing literature of both published and unpublished works on internet freedoms including, government documents and reports, civil society reports and reports of select international organisations.

3 Country Context

3.1 ICT Status

There are currently five Internet gateways in Zimbabwe, namely: Liquid Telecom (79% market share of equipped bandwidth capacity); TelOne (16.3%); Powertel (2.4%); Dandemutande (1.6%) and Africom (0,6%). Two of these: TelOne and Powertel, are state owned. There are 16 officially registered and licensed Internet service providers, but it is estimated that the total in-country could be at least more than 28. Econet currently dominates on mobile subscriptions, holding 69.7 percent of the customer market share as of early 2019. The Mobile phone service license fee which is one of the highest in the region stands at US$ 137.5 million.[5] The fees are a hindrance for new players into the market. Econet is the only operator that has managed to pay the license fees in full. Moreover, there is no action taken against the government operators that cannot afford the required fees.

The Postal and Telecommunications Regulatory Authority (POTRAZ) regulates all the above companies, and produces a quarterly 'sector performance report' that provides statistics related to Internet and telecoms use in the country. Most Zimbabweans accessing the Internet do so through mobile phones, however data costs in Zimbabwe remain high for an ordinary Zimbabwean. In 24 April 2019, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) allowed mobile network operators to legally charge up to 0,05 RTGS cents per megabyte or RTGS $50 per gigabyte before tax. The POTRAZ threshold for data costs translates to about $15 to $20 per gigabyte in United States dollar terms.[6] A regional comparative would show that Zimbabwean data is not that expensive, compared to South Africa where charges are at an average of US$11 per gigabyte of data. Unfortunately, the Zimbabwean situation is made complex by the fact that the cost of services such as the Internet and mobile data have gone up in response to the devaluation of the RTGS dollar, but average salaries or incomes have remained largely stagnant.[7]

5 Statistics obtained from the POTRAZ Postal and Telecommunications Sector Performance Report available here: http://www.potraz.gov.zw/wp-content/uploads/2019/12/Abridged-Sector-Performance-report-3rd-Q-2019-hmed-final.pdf

6 Latest Internet Data Price Increases Unjustified; http://kubatana.net/2019/04/30/latest-internet-data-price-increases-unjustified/#:~:text=In%20a%20statement%20dated%2024,%2450%20per%20gigabyte%20before%20tax.

7 Ibid

3.2 Political Environment

Following the November 2017 coup that removed former president, Robert Mugabe after 32 years in power, Zimbabwe held presidential elections in 2018 to formalise the current president's position. It was yet another questionable election, with allegations of rigging on the part of the ruling party, ZANU-PF.[8] Following the elections, the country is experiencing a protracted economic crisis exacerbated by shortage of both USDs and the local 'currency' called the 'bond notes'. Following protests over increasing fuel prices in January 2019, security forces launched a crackdown in which 12 people were killed and many arrested. During that period, the Zimbabwean government ordered its first countrywide Internet shutdown.[9]

3.3 Economic Status

Zimbabwe's population is currently estimated to be 14.4 million[10] and ranked 156 out of 188 countries in the Human Development Index. The poverty rates in Zimbabwe are estimated to have risen from 29% in 2018 to 34% in 2019.[11] The main income generating activity is agriculture and the gross domestic product (GDP) is 12.8 percent.[12] Zimbabwe continues to suffer very high inflation with annual figure at at 230% in July 2019 with food prices rising by 319%.[13]

Zimbabwe's economic problems have worsened as the country wrestles bad debts; hyper-inflation; currency shortages and high unemployment. Zimbabwe is on record as having one of the world's most informal economies,[14] with its record unemployment, collapsed industries and massive corruption.[15] Corruption for instance led to the firing of the entire board of the Zimbabwe Anti-Corruption Commission.[16]

With these systemic and structural challenges, the Zimbabwean economy and survival of its citizens' hinges upon a robust and functional Internet system. The hyper-inflationary environment means that the economy is heavily dependent on cashless transaction systems such as mobile money platforms, cell phone banking and Internet transfers. This means measures by the government such as internet restrictions and shutdowns have major repercussions that may slow down the already vulnerable economy.

Amidst the rising tensions, the government seems to be moving towards establishing dominion over all aspects of its digital and public spaces. In 2018 the government entered a partnership with the Chinese to deploy facial recognition technology in a move seen to be intended to build a surveillance state.[17] Since the January 2019 protests, there is an ongoing clampdown on popular activists and civil society leaders, by way of arrests, torture and forced disappearances.

8 MKHULULI TSHUMA, "How 2018 elections were rigged twice in 3 days," News Day, August 2018, https://www.newsday.co.zw/2018/08/how-2018-elections-were-rigged-twice-in-3-days/

9 Aljazeera, "Zimbabwe imposes internet shutdown amid crackdown on protests," https://www.aljazeera.com/news/2019/01/zimbabwe-imposes-total-internet-shutdown-crackdown-190118171452163.html

10 World Bank: Zimbabwe https://data.worldbank.org/country/zimbabwe

11 World Bank, "The World Bank in Zimbabwe," https://www.worldbank.org/en/country/zimbabwe/overview

12 Afdb, "Zimbabwe Economic Outlook: Macroeconomic performance and outlook," https://www.afdb.org/en/countries/southern-africa/zimbabwe/zimbabwe-economic-outlook

13 World Bank, "The World Bank in Zimbabwe," supra.

14 Zim has the world's second largest informal economy: IMF https://www.herald.co.zw/zim-has-worlds-second-largest-informal-economy-imf/

15 Zimbabwe ranked the 160th most corrupt country out of 180 surveyed countries according to the 2018 Corruption Perceptions Index reported by Transparency International: https://www.transparency.org/cpi2018

16 Robert Tapfumaneyi, "Mnangagwa fires entire Anti-Corruption Commission," New Zimbabwe.com January 31, 2019, https://www.newzimbabwe.com/mnangagwa-fires-entire-anti-corruption-commission/

17 China is exporting facial recognition software to Africa, expanding its vast database: Quartz March 25, 2018 https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

4 Results

4.1 Key Trends of Internet Control Measures in Zimbabwe Over Successive Periods

4.1.1 Weaponising the Law to Legitimise Actions

The desire to entrench surveillance saw the introduction of provisions requiring mandatory compliance by third parties to government interception requests in several countries. Zimbabwe's Interception of Communications Act (ICA)[18] adopted in 2007 requires telecommunications service providers to have at their own cost, "the capability of interception" and ensure that their services are "capable of rendering real time and full-time monitoring facilities for the interception of communications and storage of call-related information.[19] The law does not provide for independent judicial oversight. Moreover, its supervisory powers are placed in the Office of the President and Cabinet and warrants are issued by the Prosecutor-General. In September 2011, POTRAZ, the Zimbabwean regulator, stopped Econet Wireless from introducing Blackberry Messenger, which provided encrypted messaging services, without a specific license from the regulator.[20]

Legalising Surveillance and Interception of Communication

As early as 2002, repressive pieces of legislation and policies were introduced in the guise of ensuring national security. The most outstanding laws, policies and regulations introduced include: - the Access to Information and Protection of Privacy Act (AIPPA) of 2002; the Criminal Law and Codification Act (CODE) of 2004; the Interception of Communications Act (ICA) of 2007; the Postal and Telecommunications Regulations Statutory Instrument 95 of 2014 (Subscriber Registration) also known as the mandatory Sim Card registration regulation; and the National Policy for Information and Communications Technology.

18 Interception of Communications Act, http://archive.kubatana.net/html/archive/legisl/070803ica.asp?sector=legisl

19 Challenges in promoting privacy and freedom of expression in Zimbabwe, http://nehandaradio.com/2013/06/11/challenges-in-promoting-privacy-and-freedom-of-expression-in-zimbabwe/

20 Econet BlackBerry service 'banned' https://www.telegeography.com/products/commsupdate/articles/2011/06/20/econet-blackberry-service-banned/

The AIPPA was enacted to protect personal information and privacy in relation to information collected and held by public bodies. While the Act lays out some standards regarding the protection of personal information and privacy, it does not secure data collected by private bodies. According to the Act, where there arises conflict in the law, its provisions supersede the former.[21] However, it is largely perceived as a major threat to human rights and freedoms. Indeed, the late former chairman of the Zimbabwe Parliamentary Legal Committee, Dr Edison Zvobgo once described it saying: "I can say without equivocation that this Bill, in its original form, was the most calculated and determined assault on our liberties guaranteed by the Constitution, in the 20 years I served as cabinet minister."[22] It came as a tool to silence the opposition under the leadership of MDC leader Morgan Tsvangirai (RIP) by the then president, Robert Mugabe (RIP).

The rise in Internet usage in Zimbabwe has over the years put the application of AIPPA in the spotlight. The law has been used to inhibit media freedoms including shutting down of media houses that were not formally registered with the Media Information Commission (MIC) in accordance with the requirements of section 66 of the Act.

Under section 29 (b) of the (AIPPA)[23], public bodies are permitted to collect personal information for the purposes of national security, public order and law enforcement. This clause is problematic since it may be used by authorities to breach privacy of the individual such as through facial recognition program partnerships with tech companies under the guise that such technology will assist with policing and protecting the privacy of citizens, yet it could be used in the contrary.

The Interception of Communications Act (ICA) was enacted in 2007, aims to provide for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Zimbabwe; to provide for the establishment of a monitoring centre and related matters.[24] It should be noted that this law was enacted at a time of increased use of the internet to express dissent and criticism of the government.[25] According to the law, "interception" is defined as, "to listen to, record, or copy, whether in whole or in part" communications sent through telecommunications or radio systems and "to read or copy the contents" of communications sent by post.[26]

Additionally, the law raises several concerns regarding the independence in execution of functions. For instance, supervision of the implementation of the law lies with the Office of the President and Cabinet. Further, the Minister by section 5 (2) and section 6 is given unfettered discretion to issue a warrant for interception of communications.[27] Moreover, the law does not provide independent and impartial judicial scrutiny before such warranty is issued.[28] Legal pundits consider the absence of judicial measures on warranties and lack of requirement for notification of the subject of the warrant or surveillance a violation of the rights of the individual.[29]

21 *Section 3(2)*

22 *Owen Gagare, "Mugabe, Moyo's love-hate relationship," Zimbabwe Independent, June 13, 2014, https://www.theindependent.co.zw/2014/06/13/mugabe-moyos-love-hate-relationship/*

23 *A public body may only collect personal information if— (a) the collection of that information is expressly authorised in terms of an enactment; (b) the information is to be collected for the purposes of national security, public order and law enforcement; or (c) the information is to be collected for the purposes of public health; or (d) the information relates directly to and is necessary for an operating programme, function or activity of the public body; (e) the information will be used to formulate public policy.*

24 *Interception of Communications Act, 2007 http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf*

25 *Reporters Without Borders, "All communications can now be intercepted under new law signed by Mugabe," August 6, 2007, https://rsf.org/en/news/all-communications-can-now-be-intercepted-under-new-law-signed-mugabe*

26 *Interception of Communications Act Section 2(2*

27 *Request for record: An applicant who requires access to a record that is in the custody or control of a public body shall make a request, in writing, to the public body, giving adequate and precise details to enable the public body to locate the information so requested.*

28 *Interception of Communications Act section 6(1)(a), (b), (c)*

29 *Interview with Moreblessing Mbire, legal researcher, conducted on 24 July 2019.*

Further, the law requires telecom service providers to ensure that their services have the capability of interception and ensure that their services are "capable of rendering real time and full time monitoring facilities for the interception of communications.[30] This provision opens doors for Internet Service Providers (ISPs) to collect and store large amounts of data and meta-data, a thing that contravenes international human rights standards. Worse still the data collected may not be appropriately protected or secured as the country lacks a data protection and protection law.

In 2017, the Computer Crime and Cybercrime Bill[31] was introduced. The Bill which is championed by the Ministry of ICTs and awaits enactment by the parliament aims to stop "abuse of social media and other computer-based systems."[32] Some critics interviewed for this research believe that the Bill was created for the government to tighten its grip over the control of cyberspace and spy on its citizens, and had been inspired from the sentiments of former president Mugabe after his visit to China and understanding the strategies used by the latter to control its citizens. The Bill has several problematic clauses including vague offences which attract heavy penalties and prison sentences when one is convicted. It among others penalises dissemination of communications of certain communications (clause 16) such as what is labelled as intended to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress". This is potentially intrusive and poses more threats to privacy of the individual. Further, it proposes for a Cybersecurity Centre (clause 3) that is intended to among others promote and coordinate activities focused on improving cybersecurity and preventing cybercrime by all interested parties in the public and private sectors.

The bill if passed in its current state, would, among other things, allow authorities to remotely install spying and forensic tools onto the devices of individuals of interest. Such actions would theoretically be authorised by a magistrate if satisfied, based on an application by a police officer, indicating that there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in the Bill, but is reasonably required for the purposes of a criminal investigation. The bill generally has broad authority and discretionary powers in the police, which can be highly prone to misuse and abuse, and which potentially makes oversight and accountability difficult.

Civil society groups like MISA-Zimbabwe have been actively engaging with the bill and raising concerns over problematic clauses[33] to ensure that the bill once passed meets and addresses the needs of the citizens.

30 Interception of Communications Act section 12; see also, Challenges in promoting privacy and freedom of expression in Zimbabwe, http://nehandaradio.com/2013/06/11/challenges-in-promoting-privacy-and-freedom-of-expression-in-zimbabwe/

31 http://www.veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf

32 Zimbabwe Independent, "Cybercrimes Bill: Its flaws, remedies," January 13, 2017, https://www.theindependent.co.zw/2017/01/13/cybercrimes-bill-flaws-remedies/

33 Hazel Ndebele, "Cybersecurity Bill a threat to human rights: Misa," Zimbabwe Independent, January 26, 2018, https://www.theindependent.co.zw/2018/01/26/cybersecurity-bill-threat-human-rights-misa/

Rise of National Security and Terrorism as Justification for Repressive Laws

In Zimbabwe, lawful interception of communication is allowed following issuance of a warrant by a judge if there is "reasonable grounds" for interception to take place. This includes "an actual threat to national security or any compelling national economic interest" or "concerning a potential threat to public safety or national security."

The former editor at the state-owned Sunday Mail newspaper, Edmund Kudzayi, was arrested in June 2014 on accusations of running the 'Baba Jukwa' Facebook account, on charges of intention to subvert the government through waging "cyber-terrorism" through the Facebook account and was released two weeks later with a USD $5,200 cash bail.[34] At the same time, a controversial yet popular Facebook page, Mugrade Seven was also deactivated.[35]

Silencing Dissent and Criticism through Criminalising Free Speech

Enforcing Insult laws

Since 2014, Zimbabweans started to witness an increase in arrest of individuals, based on online activities. In the absence of a robust cyber law regime, the Criminal Law and Codification Act (CODE), popularly known as the 'insult law' has been used by the government since the colonial times as a weapon against critics both online and offline.[36] The law exposes ordinary citizens to risk of arrest for exercising freedom of speech and expression through dissent or criticism both online and offline.

For instance, sections 31 and 33 of CODE criminalise the publication or communication of false statements considered to be prejudicial to the state or that undermines the authority of or insults the President. These provisions have been severally used to arrest and charge individuals for statements made publicly or privately. Citizens' concerns have usually been fronted by civil society through challenging the legality and constitutionality of the law in light of the evolution of democracy.[37] They have severally stated that the law is out-dated and too vague that it only serves the purpose of curtailing freedom of speech and expression.

The Zimbabwe Lawyers for Human Rights (ZLHR) have since July 2014, reported to have provided legal aid to more than 200 people arrested for posts made on social media sites like Facebook and Twitter. The charges have mainly related to the 'insult law'. In November 2017, Martha O'Donovan, an American working in Zimbabwe was arrested for calling former President Robert Mugabe a "sick and selfish man" on Twitter.[38] She was detained and charged with subversion and attempting to overthrow the Mugabe government, an offence which carries a sentence of up to 20 years in prison.

Following the various arrests of online activists, many citizens now use pseudonyms on social media to discuss political topics. On the other hand, others have resorted to self-censorship in fear of the state's capacity to seek out the identities of pseudonymous individuals.[39]

34 Charles Laiton, "Sunday Mail Editor 'is Baba Jukwa," The Standard, June 22, 2014, http://bit.ly/1Lyv02G

35 Mugrade Seven was also a pseudonymous Facebook character with over 200,000 followers, who referred to him/herself as a 'Fearless Journalist' who was in the business of 'informing the nation nonstop, 24/7'. The page notoriously used to publish damaging information about prominent government officials.

36 CODE https://www.unodc.org/res/cld/document/zwe/2006/criminal_law_codification_and_reform_act_html/criminal_law_codification_and_reform_act.pdf

37 Legal Expert and Blogger, Alex Magaisa in: "Why Zimbabwe's Presidential Insult Law is Unconstitutional: A critical Analysis of Section 33 of the Criminal Code" http://alexmagaisa.com/2016/07/31/why-zimbabwes-presidential-insult-law-is-unconstitutional-a-critical-analysis-of-section-33-of-the-criminal-code

38 An American was just jailed in Zimbabwe for mean tweets about Mugabe https://www.washingtonpost.com/news/worldviews/wp/2017/11/04/an-american-was-just-arrest-in-zimbabwe-for-mean-tweets-about-mugabe/?noredirect=on&utm_term=.1b57067c02a0

39 After the Baba Jukwa arrest story broke, a reader wrote on our NewsDay-Zimbabwe Facebook page: "What if they hack into my account like they did with BJ? I am not sure if it is worth the risk to send in pictures of a failed service delivery system and they discover who I am." John Mokwetsi, "Cyber freedom: Have we started to censor ourselves?" The Standard, July 13, 2014, http://bit.ly/1jIMmPE : Cited in the Freedom House, Freedom on the Net Report, 2015.

False News / Misinformation

In 2002, Access to Information and Protection of Privacy Act (AIPPA) became the leading weapon of the government and the ruling ZANU-PF party in their campaign to stifle the opposition Movement for Democratic Change (MDC) and independent media reporting. The law granted wide-ranging powers to the government-controlled Media and Information Commission, imposed registration and licensing requirements on media outlets, and imposed strict content restrictions on the media by introducing section 64 on "Abuse of freedom of expression", and section 80, on "Abuse of journalistic privilege". Within 10 weeks of AIPPA being enacted, 13 journalists were arrested, and by the end of 2002, 44 media practitioners had been arrested.[40] Section 80 was amended in October 2003 and its application limited, making it an offence to publish false information if the author knew it was false or did not have reasonable grounds for believing it is true and if published recklessly, or with malicious or fraudulent intent.

Excessive and Punitive Responses

Pastor Evan Mawarire who was one of the leaders of the successful hashtag #ThisFlag cyber movement in Zimbabwe, was arrested in June 2016 for "inciting violence and disturbing the peace" and "overthrowing or attempting to overthrow the government by unconstitutional means," but the court acquitted him of the charges.[41] The prominent Pastor was arrested in January 2019 and released on a USD 2,000 bail, but faces charges of subversion and incitement to violence, punishable by up to 20 years in prison.[42]

In February 2019, the Zimbabwean Cabinet approved the Maintenance of Peace and Order Bill, to repeal the Public Order and Security Act (POSA), a controversial and draconian law to align it with the constitution[43] as well as to respond to court rulings which declared some of its provisions unconstitutional.[44] However, the bill has been criticised as portraying only a titular change as opposed to substantive reform, as it has retained the vast majority of the provisions of POSA thus it is likely to sustain the legislative assault on democratic freedoms despite claiming the contrary.[45]

In the spirit of continuing to stir fear-mongering among citizens and social media users, the state media in August 2016 turned up its propaganda machinery when it published a shocking top story headline in the Herald newspaper that read: "Social media terrorists exposed."[46] This portended the possible start of a more targeted clampdown on social media users perceived as troublemakers. Some critics believe that these trumped-up accusations of social media abuse against few scapegoats[47] was intended to justify the stringent social media regulation laws that the government is expected to include in the 2017 Computer Crime and Cybercrime Bill. The 'social media terrorists' were three Zimbabweans allegedly exposed in the government's latest 'cyber-terrorism probe' whose preliminary findings unearthed 'subversive and inflammatory' messages allegedly originated by them.

40 *MISA Factsheet: Application of AIPPA to date: https://crm.misa.org/upload/web/zimbabwe_access-to-info-law_factsheet-7.pdf*

41 *Zimbabwe activist pastor Evan Mawarire walks free from court after charges dropped https://www.dw.com/en/zimbabwe-activist-pastor-evan-mawarire-walks-free-from-court-after-charges-dropped/a-19398310*

42 *Zimbabwe pastor Evan Mawarire leaves prison on bail https://www.dw.com/en/zimbabwe-pastor-evan-mawarire-leaves-prison-on-bail/a-47302613*

43 *Media Reform Bill Approved by Zimbabwean Cabinet https://www.prnewswire.com/news-releases/media-reform-bill-approved-by-zimbabwean-cabinet-300852354.html*

44 *Bills Digest On The Maintenance Of Peace And Order 2019 Https://Www.Parlzim.Gov.Zw/Component/K2/Bills-Digest-On-The-Maintenance-Of-Peace-And-Order-2019*

45 *An Analysis of the Maintenance of Peace and Order Bill, 2019 https://www.thezimbabwean.co/2019/07/an-analysis-of-the-maintenance-of-peace-and-order-bill-2019/*

46 *Social Media Terrorists Exposed, http://www.herald.co.zw/social-media-terrorists-exposed*

4.1.2 Disrupting Networks – From Social Media Blockage to Internet Throttling

Internet Shutdowns and Blackouts.

In January 2019, Zimbabwe ordered a countrywide internet shutdown following massive protests against a 150% fuel price hike and the struggle for economic justice.[48] The shutdown was in effect for six days and was allegedly aimed at protecting national security. President Mnangagwa justified the shutdown on Twitter stating that: "social networks (were) being used to plan and incite disorder and to spread misinformation leading to violence. In response, the decision was taken to temporarily restrict access to prevent the wanton looting and violence, and to help restore calm."[49] During this period, government efforts to contain the anti-government protests saw unleash of a wave of terror, killing over a dozen under the cover of the Internet blackout by the security forces.

The Zimbabwe chapter of the Media Institute of Southern Africa (MISA) successfully challenged the January 2019 Internet shutdown and the High court ruled the shutdown was illegal.[50] The shutdown was one of the government's "most brazen attacks on Zimbabwe's constitutional liberties".[51] There are continued threats and fears that internet shutdowns could be relentlessly used by the government as a weapon to threaten, suppress and curtail people's human rights and freedoms such as access to information and freedom of expression, freedom of association and assembly, and the right to privacy with impunity.

However, this is not the first time Zimbabwe government ordered a network disruption. Earlier in July 2016, the government had ordered telcos and ISPs to block access to social media platforms, as a way to disrupt online organising and strikes organised by the #ThisFlag social movement.[52]

4.1.3 Surveillance Galore: The Build-Up of States' Capacity

Despite the existence of several provisions within the legal and policy frameworks, by 2005 reports of surveillance and interception of communication in Zimbabwe were few. However, the government in successive periods enhanced its technical capacity to intercept and conduct surveillance.

Going High-Tech to Implement Surveillance

In January 2015, Zimbabwe's former president Robert Mugabe received a 'gift' from Iran comprising various cyber-surveillance technologies, including International Mobile Subscriber Identity (IMSI) catchers.[53] The equipment that make it possible to intercept mobile phone traffic as well as track the location data of mobile phone users and was said to aid the government to keep its foreign policy foes at bay, and ratchet up suppression and snooping on political opposition and other organisations it considered a national security threat.[54]

47 At the time of the accusation, one of the accused so-called social media terrorists (@rimbe_t) had not posted a Tweet in over a year. The article also did not stipulate which laws these 'terrorists' allegedly broke.

48 First total internet shutdown in Zimbabwe, https://bulawayo24.com/index-id-news-sc-national-byo-153712.html

49 President Mnangagwa Justifies Internet Shut Down, Although "He Deeply Believes In Freedom Of Speech And Expression", https://www.techzim.co.zw/2019/01/president-mnangagwa-justifies-internet-shut-down-although-he-deeply-believes-in-freedom-of-speech-and-expression/

50 IOL, "Zimbabwe High Court court rules internet shutdown illegal," IOL, January 21, 2019, https://www.iol.co.za/news/africa/zimbabwe-high-court-court-rules-Internet-shutdown-illegal-18898174

51 Interview with key informant – Zororo Mavindidze, conducted on 3 July 2019.

52 "Totalitarian Regime blocks WhatsApp," New Zimbabwe, July 6, 2016, http://www.newzimbabwe.com/news-30060-Totalitarian+regime+blocks+WhatsApp/news.aspx

53 Iran gives Mugabe Spy-Technology https://bulawayo24.com/index-id-news-sc-national-byo-61558-article-iran+gives+mugabe+spy-technology.html

54 Telephony eavesdropping devices used for intercepting mobile phone traffic and tracking movement of mobile phone users.

In 2007 the government introduced a repressive policy restricting the use of encryption technology while invoking a clause within the Interception of Communication Act (ICA) to restrict access to encrypted services that allow people to communicate anonymously and privately. Although the Act does not specifically ban the use of encryption technology, POTRAZ has taken advantage of the vague legislation to ban encrypted services. In September 2011, POTRAZ banned Blackberry Messenger – then an encrypted messaging service provided on Blackberry phones.[55] The basis for the ban was that the Act requires telecommunication companies to have hardware and software with the ability to carry out surveillance for the government. As of July 2019, the ban on Blackberry Messenger was still in effect.

It should be noted that bans on the use of encryption technology violates the right to privacy and the right to freedom of expression. The Special Rapporteur on Freedom of Expression noted in 2015, "encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attack."[56] However, the ban on Blackberry Messenger services was never challenged because it was not of major relevance to ordinary Zimbabweans.

In 2017, the government introduced a new Ministry to oversee Cybersecurity, Threat Detection and Mitigation. Though now disbanded, the ministry had been formed under the instructions of former president, Robert Mugabe, to catch "rats" that were getting up to mischief using cyberspace.[57] According to the presidential spokesperson, George Charamba, the new ministry was to learn from the experience of countries like China and Russia, which he described as having "done well in ensuring some kind of order and lawfulness in the area of Cyberspace.[58] Both China and Russia are known for their censorship of social media platforms. While the government described the new ministry as "protective" i.e. playing a defensive role, there were concerns that it was aimed at limiting the use of social media. The idea of this ministry was conceived at a time when the former president was the butt of several bad jokes and memes in African social media spaces for "protecting his eyes"[59] during important events, tripping over[60] and reading a wrong speech.[61]

The ministry was well timed to curtail online freedoms ahead of the 2018 presidential election campaigns. Indeed, the Ministry was short-lived for a purpose having been formed in October 2017 and ending promptly when the Mnangagwa government took over in November 2017 after the coup.

55 *The Zimbabwean, "Telecommunications Regulatory Authority maintains a ban on the tool" June 5, 2012, https://www.thezimbabwean.co/2012/06/blackberry-messenger-a-dream/*

56 *Report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 2015, Para 16.*

57 *Chronicle, "Cyber Security Ministry meant to enhance national security,"October 14, 2017, https://www.chronicle.co.zw/cyber-security-ministry-meant-to-enhance-national-security/ In this article, the former president is quoted in Shona highlighting that this ministry is the trap needed to catch 'rats' in the cyberspace.*

58 *Ibid.*

59 *Abdi Latif Dahir, "Robert Mugabe isn't sleeping through meetings—he's protecting his eyes from "bright lights," Quartz, May 11, 2017 https://qz.com/africa/981636/photos-all-the-times-zimbabwes-president-robert-mugabe-was-caught-on-camera-sleeping-in-conferences/*

60 *Omar Mohammed, "The fall of Robert Mugabe may not be televised—but it has already been ruthlessly photoshopped," Quartz, February 5, 2015, https://qz.com/339844/the-fall-of-robert-mugabe-will-not-be-televised-but-shared-again-and-again/ -*

61 *Lily Kuo, "Zimbabwe's 91-year-old president delivered the wrong speech to parliament,"Quartz, September 15, 2015, https://qz.com/africa/502598/zimbabwes-91-year-old-president-just-delivered-the-wrong-speech-to-parliament/*

AI, the Game Changer

The use of Artificial Intelligence was also reported in Zimbabwe. In March 2018, the government had 'strategic' partnership[62] with the Chinese company – Cloudwalk Technology, for the conduct of a large-scale facial recognition programme primarily used in traffic management, security and law enforcement and with the possibility to be extended to other public programmes. Under the project, the government will build a national facial database, and then share it with the Chinese government, to help it "train the racial bias out of its facial recognition systems."

However, it was not clear how the facial recognition program would be implemented. It seemed also possible that the government would turn over to the use of data already in its possession, e.g. data collected for purposes of issuing national identity cards, passports, driver's licenses, and lately during the biometric voter registration exercise.

Civil society organisations such as MISA-Zimbabwe have expressed concerns of violation of citizens' privacy rights.[63] Concerns mainly dwell on the lack of information about the security, use and storage of the facial database by China. Most importantly, there are fears that this relationship between China and Zimbabwe will see the former's model of authoritarianism spread to the latter. Worse still, fears continue to linger as to the future of internet freedoms, with China having been rated the "worst abuser of Internet freedom in 2018" by the think tank Freedom House.[64]

4.1.4 The Push Towards Determining Identity Amidst Poor Oversight

Once a government can intercept communication, resolving the identity question then remains just a matter of time. Measures have been introduced progressively in Zimbabwe to enable the government identify any telecommunication services user with precision. From SIM card registration, the government has since adopted digital identities and incorporated biometrics and artificial intelligence, albeit with poor or no oversight.

SIM Card Registration

In 2010, the Postal and Telecommunications Regulatory Authority issued directives requiring all mobile phone subscribers to register their details with the respective service providers.[65] The Postal and Telecommunications Regulations Statutory Instrument 95 of 2014 (Subscriber Registration) of Zimbabwe requires all telecommunications companies to create a centralised subscriber database of all their users.[66]

62 https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

63 Media Institute of Southern Africa (MISA) Zimbabwe, "Digest: Facial Recognition Technology and its Possible Impact on Privacy Rights," MISA Zimbabwe, May 29, 2018, http://zimbabwe.misa.org/2018/05/29/digest-facial-recognition-technology-privacy-rights/

64 Freedom of the Net 2018 https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

65 Zimbabwe: Sim Card Registration Raises Growth Fears https://allafrica.com/stories/201006220268.html

66 Replaced Statutory Instrument 142 of 2013 "Postal and Telecommunications (Subscriber Registration) Regulations, 2013".

The database is managed by POTRAZ who claim to use it, among other things, to assist law enforcement agencies to safeguard national security, as well as authorising access for the purposes of research in the sector. The government through POTRAZ in June 2016, issued threats to the public, highlighting the fact that perpetrators of "abusive and subversive materials" would be identified, disconnected and arrested.[67] The database should be accessible to the government and should be regularly updated with new user information. Further, a telecommunications licensee, such as an ISP, is required to supply information to government officials upon request.

The Regulations stipulate the penalty of imprisonment of up to six months for failure to register a SIM card or providing of incorrect information. Although the 2014 regulations introduced the requirement that a warrant or court order is required for POTRAZ to release information to law enforcement agents, there is no assurance that these procedures are followed.[68] While a judge or magistrate may issue a court order, police officers designated as justices of the peace,[69] can also issue warrants.

These regulations have been occasionally used to instil fear in citizens. For example, in July 2016, Zimbabweans held a stay home demonstration in protest to failing policies of President Robert Mugabe.[70] The government, through POTRAZ, issued a veiled threat through a public notice in the press stipulating that people who were sharing "abusive and subversive materials" would be" disconnected… arrested and dealt with accordingly in national interest." The public notice went on to warn further that: "All SIM cards in Zimbabwe are registered in the name of the user. Perpetrators can easily be identified."[71]

Notably, compulsory SIM card registration and retention of data about mobile phone users in a centralised database threatens the right to privacy in Zimbabwe, especially in the absence of data protection and privacy legislation. It undermines peoples' ability to communicate anonymously, organise, and associate with others, and it infringes their rights to privacy and freedom of expression.

4.1.5 Enter the Era of Social Media and Data Taxation

Zimbabwe was an early adopter of such brazen measures. In August 2016, the government increased mobile data prices overnight by 500%. The move was part of government efforts to quash activism on social media around the #ThisFlag movement.[72] The government, through POTRAZ, also ordered mobile networks to suspend data bundle promotions until further notice.[73] In January 2017, the government increased the cost of the data tariffs by a further 2,500%.[74] The move caused an uproar amid speculation that it was part of the government's sinister way of forcing millions of users off social media platforms. It was criticised as retrogressive, insensitive and politically-motivated onslaught on freedom of expression ahead of the 2018 elections. In June 2018, the government made almost a 60% reduction in the cost of mobile data.[75]

67 *Nation heeds stay away call https://www.newsday.co.zw/2016/07/nation-heeds-stay-away-call/*
68 *Postal and Telecommunications (Subscriber Registration) Regulations, 2014, Section 9(2).*
69 *Justices of Peace are judicial officers appointed by means of a commission to keep the peace. Bill Watch 29/2014, http://veritaszim.net/node/1059*
70 *Nation heeds stay away call, https://www.newsday.co.zw/2016/07/nation-heeds-stay-away-call/*
71 *Nigel Gambanga, "Here's the Zimbabwean government's warning against social media abuse," TechZim, July 6, 2016, http://www.techzim.co.zw/2016/07/heres-zimbabwean-governments-warning-social-media-abuse/#.V4jc5o6zDaY*
72 *Zimbabwe data prices hiked by up to 500% to curb social media activism and dissent https://mg.co.za/article/2016-08-05-zimbabwe-data-price-hiked-up-by-up-to-500-to-curb-social-media-activism-and-dissent*
73 *Mobile operators suspend data bundles promotions https://www.newsday.co.zw/2016/08/mobile-operators-suspend-data-bundles-promotions/*
74 *Uproar over data tariff rise https://www.newsday.co.zw/2017/01/uproar-data-tariff-rise/*
75 *MISA Zimbabwe Position on Reduced Mobile Data Rates http://kubatana.net/2018/06/20/misa-zimbabwe-position-reduced-mobile-data-rates/*

However, in August 2019, NetOne, a telecom company increased the cost of data bundles by 300%.[76] Operators had increased the cost of bundles in April 2019, citing the high cost of doing business.[77]

Irrespective of the reasons behind the data hikes, during August 2016 and January 2017, there were violations of human rights and freedoms including access to information, freedom of expression, assembly and association. Many Zimbabweans were temporarily forced to go offline due to the highly unaffordable costs of the internet. It should be observed that due to anger and uproar in response to the data price, in August 2016, the prices were reversed.

4.1.6 Deploying Bots, Cyberattacks and Disinformation

A common excuse for curtailing internet freedom is the need to fight what countries variously term misinformation, disinformation, hate speech, or fake news, among other terms.

In August 2016, the state-owned Herald newspaper published a headline story with the title, "Social media terrorists exposed".[78] The 'social media terrorists' were three Zimbabweans exposed in the government's 'cyber-terrorism probe' whose preliminary findings unearthed 'subversive and inflammatory' messages allegedly originated by trio. The article was a message communicating the possible start of a more targeted clampdown on social media users and to justify the stringent social media regulation through the Computer Crime and Cybercrime Bill.

In July 2018, there emerged several new social media accounts on Facebook and Twitter to advance the Zimbabwean government and ruling party ZANU-PF propaganda,[79] manipulate conversations, target and harass online activists and disrupt political conversations by the opposition. The influencers self-identifying as 'Team Varakashi'[80] are state propaganda machinery, who led a spirited dis-information campaign targeting both domestic and foreign audiences by amplifying and magnifying government talking points through hundreds of accounts.

In an unpublished investigation on information manipulation on social media ahead of the 2018 Zimbabwe Presidential elections, the Digital Society of Zimbabwe (DSZ) identified[81] a pattern in tweets collected at the time, that a small number of influencer accounts played a crucial role in hijacking conversations about the president or ruling party, and the rest of the 'Varakashi' accounts would retweet, like or reply to advance the propagandist messages.

The 'Varakashi' strategy appeared to be an effective part of a large-scale effort by government-backed users to stop human rights activists and opponents of the state from being heard.[82] It succeeded in silencing many critical conversations online as activists became aware that everything political tweet they posted was being closely observed and sometimes culminated in threats of violence on their lives. The presence of 'Varakashi' with their disruptive and harassment tendencies led to a lot of self-censorship in a context where some citizens have historically been arrested for 'insulting the office and person of the president'. Some users felt targeted and were temporarily hounded off social media platforms.

76 Hard-pressed Zim telecos hike data bundle tarrifs http://www.itwebafrica.com/ict-and-governance/273-zimbabwe/246257-hard-pressed-zim-telcos-hike-data-bundle-tariffs

77 Zimbabwe: Data Tariffs Soar As Crisis Bites https://allafrica.com/stories/201904280094.html

78 Social Media Terrorists Exposed, http://www.herald.co.zw/social-media-terrorists-exposed

79 Video https://twitter.com/Wamagaisa/status/984637362020978689

80 Loosely translated, 'rakasha' is a word in Shona language that means to attack and vanquish one's enemies.

81 Key informant interview with Tawanda Mugari – held on 11 July 2019.

82 Interview with key informant, Tawanda Mugari – Digital Security Trainer, held on 11 July 2019.

4.2 Key Positive Developments

Despite the negative trends witnessed in Zimbabwe, there were notable developments that were indeed positive and that support the enjoyment of internet freedom. The two major developments included the robust advocacy and push-back by non-state actors, and the repeal of repressive legislation.

4.2.1 Robust Advocacy and Push-back by Non-State Actors

In January 2019, the Zimbabwe chapter of the Media Institute of Southern Africa (MISA) successfully challenged internet shutdown in Zimbabwe, which the High Court ruled as illegal.[83]

In February 2016, the Constitutional Court outlawed and struck down Section 96 of CODE on 'criminal defamation', which had long been used to criminalise freedom of expression and terrorise media practitioners. MISA-Zimbabwe had made an application challenging the legality of the section and seeking confirmation that criminal defamation was no longer part of the law. This followed the judgment in the case of Madanhire and others v Attorney General[84] in 2013, in which the court ruled that Section 96 of the CODE was inconsistent with the provisions of Sections 61 and 62 of the constitution, which protect the right to freedom of expression. Section 96 was therefore declared void. Specifically, the courts held that Section 96 of CODE was void ab initio (from the beginning). The court found that the applicants had discharged the onus of showing that the impugned provision was not reasonably justifiable in a democratic society within the contemplation of s 20(2) of the Constitution.

4.2.2 Repeal of Repressive Legislation

In February 2019, the Zimbabwean cabinet approved the repeal of the draconian Access to Information and Protection of Privacy Act (AIPPA),[85] to give way for the enactment of an Access to Information Bill, the Zimbabwe Media Commission Bill and the Protection of Personal Information and Data Protection Bill. In July 2019, the Zimbabwean government gazetted the Freedom of Information Bill which repeals sections of AIPPA.[86]

83 Zimbabwe High Court court rules internet shutdown illegal, https://www.iol.co.za/news/africa/zimbabwe-high-court-court-rules-internet-shutdown-illegal-18898174

84 Madanhire and Matshazi v Attorney General, CCZ 2/2015 https://veritaszim.net/node/1403

85 Zimbabwe: Cabinet Approves AIPPA Repeal https://allafrica.com/stories/201902130504.html

86 AIPPA repealed in new era for media https://www.herald.co.zw/aippa-repealed-in-new-era-for-media/

5 Conclusion and Recommendations

5.1 Conclusion

From this study, it is evident that over the years, the Zimbabwean government has used a range of strategies to limit Internet freedom in the country. These strategies have included the introduction and use of repressive legislation and policies that violate privacy, infringe on freedom of expression and undermine digital rights. These are also partly because of the current global trends of measures taken by states to regulate and limit internet freedom. Additionally, colonial laws such as the Criminal Law and Codification Act (CODE) have been employed due to the delimiting nature arising from vague provisions.[87]

Besides legislation, the government has also employed technology and ideological state apparatus to target and limit the enjoyment of online freedoms. Some of the key effects of state apparatus is self-censorship which continues to sweep across the country. Despite the repressive and delimiting measures, there have been limited or no reactions from many affected individuals. Indeed, only civil society organisations have come out strongly against the shrinking digital space. This is partly explained by ignorance and lack of prioritization in the face of competing social and economic priorities.

87 *Section 33 of CODE that provides against insulting the president.*

5.2 Recommendations

Government

- Quickly draft a Cybercrime Bill and meaningfully involve other stakeholders from civil society, the technical sector and academia to ensure that all rights and needs that potentially arise from it are addressed. This will lead to a universally acceptable and effective legislation.
- Prioritise revision of several ICT related repressive pieces of legislation, particularly, the Interception of Communications Act (ICA); the Access to Information and Protection of Privacy Act (AIPPA) and the Criminal Law and Codification Act (CODE). Review will ensure that the said laws are consistent with the Constitution and meet minimum international human rights standards.
- Strengthen the independence of the judiciary to ensure that it effectively checks executive powers, especially digital rights, specifically, around surveillance and the respect for privacy of the individual.
- Establish an independent mechanism for complaints about misconduct by the security forces as outlined in the constitution.
- Enact an effective data protection and privacy law that meets international minimum standards on data protection and privacy. This law will ensure that the privacy of the individual is protected within the required principles and standards.

Companies

- Establish mechanisms for input from civil society and experts, to help them develop rights based approaches to content moderation, government requests, and countering disinformation. This will align their work with the business and human rights principles.
- Incorporate democratic principles into their decision-making by promoting public participation and open deliberation in their proposed strategies and policies before adoption and implementation. This will promote client satisfaction and trust.
- Implement and comply with government directives or policies which do not have adverse effects on the rights and freedoms of their customers or clients.

Media

- Play a more active role in highlighting and keeping on the public agenda, the various controls introduced by the government to restrict Internet freedom. This is especially important in a context where citizens have so many distractions.
- Self-educate on the implications of different controls such as facial recognition technology; subscriber database registrations etc, and simplify these issues for ordinary individuals why they should care and how these measures affect them in the simplest terms.
- Objectively report on the developments in the digital space, specifically on laws that affect the citizens' rights and freedoms and the duties and obligations of the citizens.

Academia

- Undertake evidence based research on digital rights and freedoms to help the citizens, media, technical community, governments and civil society understand the technical and psychological drivers of internet rights and freedoms as the established standards.

Technical Community

- Collaboratively work with other stakeholders to ensure that digital rights and freedoms continue to be enjoyed without raising aspects of conflict between the State and the citizens.

Civil Society

- Engage in innovative initiatives to raise awareness and inform the public about government censorship and surveillance efforts, as well as best practices for protecting Internet freedom.
- Monitor the government's collaboration with other States and governments and actors like tech companies to ensure that any emerging investments; infrastructure developments; training; technology sales and user data transfers do not adversely affect the citizens.
- Expose any evidence of bilateral collaborations that could potentially result in violation of Internet freedoms or human rights, and advocate against governmental adoption of such measures.
- Facilitate public awareness raising programs through publicity and trainings of the public to develop a better understanding and appreciation of digital rights and Internet freedom.
- Undertake more collaborative advocacy and strategic litigation on digital rights and freedoms including on laws and policies and government actions and measures.

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