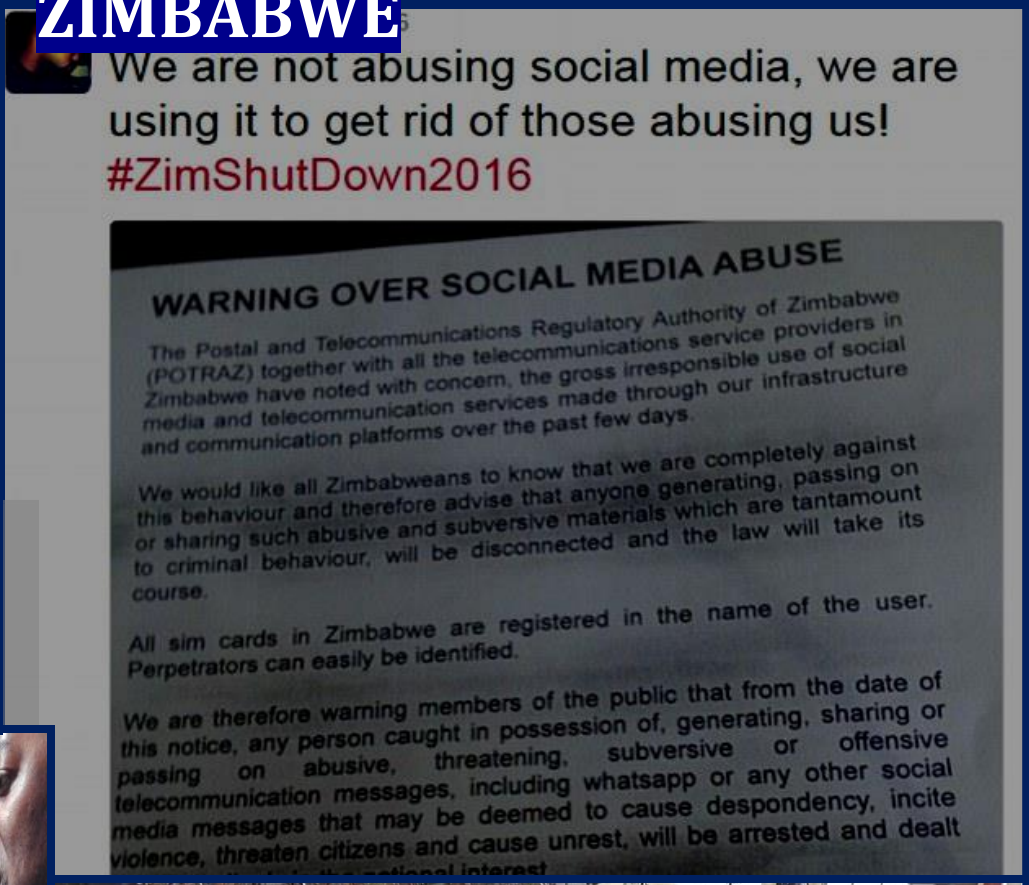
USAID
FROM THE AMERICAN PEOPLE

COUNTERPART
INTERNATIONAL

ORDEALS IN 'THE LONG-WALK TO FREEDOM': THE STATE OF INTERNET GOVERNANCE IN ZIMBABWE

Zimbabwe Democracy Institute

MEDIA CENTRE
Open And Accessible Media For An Open Society



NOVEMBER 2017 REPORT

COPYRIGHT STATEMENT

Zimbabwe Democracy Institute
66 Jason Moyo Avenue,
2nd Floor
Bothwell House
Harare
Zimbabwe
www.zdi.org.zw
zditrustinfo@gmail.com
+263 772 376 532 or +263 713 912 781

Media Centre
66 Jason Moyo Avenue,
2nd Floor
Bothwell House
Harare
Zimbabwe

And our PARTNERS:

Ordeals in 'the long-walk to Freedom': The State of Internet Governance in Zimbabwe:

This report was prepared in partial fulfillment of ZDI & MC consortium's research objective to examine the state of Internet Governance/Freedom in Zimbabwe. It is part of the project titled: "Increasing Political and socio-economic Liberties Online: Support for New Advocacy campaigns and Research on Internet Governance/Freedom in Zimbabwe" funded by USAID and Counterpart International.

As Zimbabwe struggles to transition from authoritarianism, internet freedoms have proven to be salient areas to pin hopes on. The authoritarian state has been aware of this and has put in place serious countermeasures.

Now that the country is bracing for 2018 elections, it is necessary to audit the state of internet governance /freedom because it is this modern space that the government has recently tried so hard to capture. This research was conducted by ZDI and MC team of researchers with the assistance of its country-wide networks.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

ZDI & MC acknowledge the support given by the United States Agency for International Development (USAID) and Counterpart International in making this study possible through financial assistance. This contribution is highly appreciated and thanked.

Our gratitude is also extended to all key-informants of this study. Although they cannot be acknowledged one by one here, it is our hope that mentioning them here will go a long way in showing our thankfulness to them for sacrificing their careers, time and energy talking to us.

We also thank the efforts of the ZDI & MC board members and research team for working tirelessly to make the production of this report a possibility.

LIST OF ACRONYMS

AIPPA	Access to Information and Protection of Privacy Act
ACHPR	African Charter on Human and People's Rights
CI	Counterpart International
CLCRA (CODE)	Criminal Law [Codification and Reform] Act
HRDs	Human Rights Defenders
ICA	Interception of Communications Act
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICC	International Criminal Law
MC	Media Centre
MISA	Media Institute for Southern Africa
POSA	Public Order and Security Act
POTRAZ	Postal Telecommunications Regulatory authority in Zimbabwe
UN	United Nations
USAID	United States Agency for International Development
UDHR	Universal Declaration of Human Rights
ZDI	Zimbabwe Democracy Institute
ZNA	Zimbabwe National Army
ZRP	Zimbabwe Republic Police

SECTION 1: SUMMATION OF THE STUDY

(I) STRUCTURE OF THE PAPER

This paper is an anatomy of internet freedoms and governance in Zimbabwe. It is divided into five main sections each organized in direct correspondence to a specific research objective of this study. The first section introduces the study and presents the research design. The second section examines the extent to which internet freedoms are guaranteed by international law to which Zimbabwe is party. In this section, the study sought to provide an easy-to-understand guideline to human rights defenders at all levels, rights-holders, civic society and other key stakeholders on the same. The third section examines the legal framework governing internet freedoms in Zimbabwe. This section aimed at informing key stakeholders to internet freedoms on what is constitutionally permissible and/or not under domestic law and the extent of illegal clampdown on internet freedoms in Zimbabwe. The fourth section focuses on the institutionalization of clampdown on internet freedoms in Zimbabwe. This fourth section basically exposes the extent to which various institutions of the state have been used to stifle internet freedoms. At the end of the paper (fifth section) are recommendations for improvement of the current state of internet freedoms and governance in Zimbabwe.

(II) SUMMARY OF FINDINGS

Following the upsurge in information communication technologies worldwide, internet governance has become a critical factor in determining the extent of citizens' liberties in a country. This has arisen mainly due to the rising number of citizens relying on the internet to pursue their political, social, economic and other well-being concerns in the 21st century.[1] It has become an international agenda that the internet must be a global public good that is accessible, secure, reliable, trustworthy and capable of enabling the people to change their world.[2] Same applies to internet freedom as a right capable of mortgaging freedom to organize and other first generation rights.[3] Authoritarian regimes have fallen, democracies have been born, human rights have been championed whereas, humanitarian crises have been tackled more effectively than ever owing to various possibilities to freely access and share information, associate and protest, air conscience and thought opened up by the internet.[4] However, this study found that in Zimbabwe, despite guarantees in: *(a)* international law protocols to which Zimbabwe is party and *(b)* the national Constitution; the authoritarian regime has devised various strategies to stifle, capture and control this space.[5] Key authoritarian state machinations put in place to capture and control internet freedoms are: *(i)* Constitutional provisions attaching 'easy-to-

[1] Internet has been recognized as a pertinent resource for mobilizing citizens to demand justice, equality, accountability and upholding human rights. See Frank La Rue, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur's Report), Human Rights Council, A/HRC/17/27, 16 May 2011.

[2] UN Secretary-General, 'Curtailing Freedom Does Not Preserve Order, But Undermines It', transcript of video message to the fourth annual Freedom Online Coalition Conference: Free and Secure Internet for All, Tallinn, Estonia, SG/SM/15808, PI/2088, 29 April 2014.

[3] Hillary Rodham Clinton, Remarks on Internet Freedom, 21 January 2010 (on file with the author), available at: http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.h ml. See also R. MacKinnon, *The Consent of the Networked: The Worldwide Struggle for Internet Freedom* (2013).

[4] The social media has been very pivotal in the 2011 Arab Spring revolutions that swept across Egypt, Tunisia, Libya, Syria and the "shut-down-Zimbabwe" demonstrations in 2016 that almost broke-down the state. This has shown authoritarian regimes where they are headed if they do not heed to the people's will and unfortunately, government countermeasures have been draconian internet governance framework in those countries.

[5] An analysis of interview data revealed the following strategies in their descending order of frequent use by the state to stifle internet freedoms: (i) draconian laws (CLCRA, POSA; ICA; AIPPA etc); (ii) security services (police & intelligence services); (iii) threats by top political leadership and; (iv) use of ministries and agencies to regulate access (Interviews, October-November, 2017).

abuse' conditionalities on internet freedoms; *(ii)* Acts of Parliament aimed at delimiting freedoms; *(iii)* institutionalization of clampdown on internet freedoms (through state ministries, agencies and security forces) and; *(iv)* issuing of threats by political leaders in top government positions.[6]

The study also found that, Zimbabwe currently[7] suffers the machinations of an authoritarian regime that fears freeing the private media, social media and the internet in general in belief that doing so will prevent possible public scrutiny, transparency, criticism and exposure of its maladministration crimes to the electorate and consequent electoral defeat.[8] Many restrictive laws, regulations and projects have been put in place to stifle internet freedoms, hinder access to online media, information and hinder freedom of expression, protest, advocacy and other barricades placed by deliberate policy omission.[9] In addition, no clear and serious internet uptake promotions, programs and projects have been done despite decades of government talk shop promises.

(III) Research Strategy

The research strategy used to conduct this study combined key informant interviews with desk research. Twenty-five interviews were carried out with Human Rights Defenders at national and community level, civic society organization leaders, social movement leaders, politicians and journalists. This was done in four major towns of Zimbabwe and these were: Harare, Bulawayo, Mutare and Marondera.[10] Desk research analyzed published data from government agencies, civic society, newspapers, academia and social media blogs. Thematic and content analyses of data collected as described above were used to come up with data discussed in this paper.

(IV) Conceptualization

Internet freedoms are those freedoms enjoyed by persons and are inseparable from them by the fact that they are human regardless of their 'online' or 'offline' statuses. Thus, the difference between basic liberties and internet liberties is that the latter is the practice and enjoyment of the former online. Legal and moral grounds from which these liberties emanate are the same, what differs is the space from which humanity claim those liberties. It is the basic argument in this study that legal and moral foundations of peoples' rights uniformly apply across diverse human spaces, races, gender and status. Thus, international and national protocols guaranteeing people's liberties offline also apply online.

[6] These strategies have been thematic matters in both interview data and secondary data collected during the course of this study.

[7] By the time of writing, the military had captured the government promising to deliver a national democracy project to the people of Zimbabwe from criminals surrounding president Robert Mugabe. It still have to be seen whether securocrats who benefited from Robert Mugabe's 37 years of authoritarian erosion of people's rights will be capable of guaranteeing internet freedoms any-far than the Mugabe regime.

[8] See, Zimbabwe Democracy Institute (2017) *Biometric Voter Registration, Zimbabwe Electoral Commission and the Struggle against Political Decay: A Light at the End of the Tunnel?*

[9] ZDI-MC Key Informant Interviews, October-November 2017.

[10] This study chose these towns guided by the fact that, internet use for promoting human rights and democracy is at the moment popular in major towns of Zimbabwe. These are the most key towns in Zimbabwe where civic activity can easily influence decisions of duty-bearers since key target government agencies are not decentralized. In addition, these are areas where our key informants have offices and do their activities from town and disperse impact to rural areas through their networks of community based organizations. This group of key informants of this nature was chosen for its relevant experience, knowledge, and activities that have a national coverage. It ensured that the real essence of the problem will be well-captured; interviewing the actual human rights defenders gives a clear picture of the state of affairs.

SECTION 2: INTERNATIONAL LAW GUARANTEEING INTERNET FREEDOMS

INTRODUCTION

International law to which Zimbabwe is party provides for internet freedoms and places obligations on states to respect and promote the same. Key international law protocols addressing this matter include: *(a)* the United Nations Charter; *(b)* the International Covenant on Civil and Political Rights (ICCPR), *(c)* the Universal Declaration of Human Rights (UDHR); *(d)* the International Covenant on Economic, Social and Cultural Rights (ICESCR) and; the African Charter on Human and People's Rights (ACHPR). Although Land (2013) [11] argues that some can misconstrue these as only guarantees of freedom in the physical world and that the protocols do not cater for the cyber world,[12] it should be noted that, a mere exclusion of "virtual space" in the text of law is not enough ground to override the fact that these protocols bind and are applicable to states party to then and that states include defined territories that is: land, seas, air and cyberspace, airspace above and the subsoil.[13] The internet is part of the "air and space" of a territory forming a state that is party to international protocols. Thus, international covenants cited above guarantee freedom of expression, opinion and association among others across all sectors of development regardless of frontiers. That is, freedoms are due to humans by virtue of being of human race regardless of their "online" or "offline" status.[14] La Rue (2011)[15] explains correctly that these protocols were drafted prior to most technological advancements but in the foresight to cater for the current and the upcoming future technological developments.[16] Therefore, the UN Charter, ICCPR, UDHR, ICESCR and the ACHPR remain relevant today and equally applicable to new human spaces created by information communication technology such as the internet.

(I) UN CHARTER, 1945

To what extent are internet freedoms guaranteed in international law? The United Nations Charter [1945][17] in Article 1(3) commits UN member states "To achieve international co-operation… in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion." Article 55 (c) also postulates fundamental freedoms due to every human being without distinction as to color, ethnicity, sex or religion, whereas, article 55(a) goes on to commit UN states to promote a right to higher standards of living and suitable conditions of economic and social development. This means that every human being living in UN member states such as Zimbabwe must exercise all his or her fundamental rights without fear of state intervention or other obstacles. Internet access, use and demanding the same are an inexorable condition for the

[11] See, Land, M. (2013). *Toward an International Law of the Internet.* Available at: www.ohchr.org/Documents/Issues/Opinion/Communications/MollyLand.pdf. [Accessed 20/11/2017].

[12] This is a very misleading and/or confusing understanding of the application of law. It is our submission that, law is created to apply in prevalent and prospective circumstances. The fact that the said protocols neither specified their operational scope as "off-line" nor time frame delimitation makes it beyond reasonable doubt that their intent was to apply everywhere anytime

[13] See Brownlie, I. 2008. *Principles Of Public International Law* 16 (7th Ed., 2008:105)

[14] 'Offline status' refers to a state of being out of the internet whereas, 'online status' depicts the state of being in the internet.

[15] SEE, RUE, L (2011) MONITORING FREEDOM OF EXPRESSION: THE APC-LA RUE FRAMEWORK Available at https://www.apc.org/en/pubs/internet-freedom-index-draft-checklist.

[16] Note that, during the drafting of these human rights laws, members of the Human Rights Commission were implored to "take into account the fact that their work concerned the future and not the past; no one could foresee what information media would be employed in a hundred years' time." See, speech by French Delegate to the Sixth Commission on Human Rights, discussing the "media" clause of the article on freedom of expression in the draft human rights covenant on May 2, 1950, Common on Human Rights, 6th Sess., 165th mtg. at 10, U.N. Doc. E/CN.4/SR.165 (May 2, 1950).

[17] See United Nations Charter (1945). Available at :http://www.un.org/en/charter-united-nations/. [Accessed 20/11/2017].

fulfillment of article 55 and promoting all other freedoms. Although all freedoms must be protected, the most important of them all that needs to be monitored is freedom of expression because it is a central and facilitative human right, it safeguards other rights (Joyce, 2015).[18] When people's freedom of expression is respected and protected, people can communicate efficiently and freely hence become well informed and active engaging citizens in a country. The internet is a cheap and legitimate platform for everyone to enjoy this right in a worldwide scale without hindrances and frontiers as envisioned in articles 1(3) and 55 (a & c) of the UN Charter.

(II) UDHR, 1948

Article 19 of the UDHR[19] states that, "everyone has the right to freedom of opinion and expression…" including "… freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[20] Article 20(1) of the UDHR adds that, everyone has the right to peaceful assembly and association. This means, hindering activities online by whatever means, be it legislation, institutional regulation, decree or sanctioning state agents to interfere in peoples' peaceful association (online or offline) which necessitate seeking, receiving and imparting information without frontiers is in itself a frontier and thus a breach of international norms. Freedom of expression provided for by the UDHR (more importantly, with great ease of exercising it provided by the internet) is a crucial catalyst for democratization in that, it enables people to have the power to hold duty-bearers accountable, transparent, and responsible in issues affecting them be it social, economic and political (Gallacher, 2013).[21] With this, power is distributed among well informed citizens, therefore democracy prevails.

(III) ICCPR, 1966

The ICCPR[22] in Article19 (2) states that everyone must exercise his or her right to freedom of expression; this right shall include freedom to gather, receive and use information and ideas of all kinds, regardless of frontiers, either verbally, in print, in the form of art, or through any other media of his/her choice. Article 17 emphasizes on the right to privacy and its protection by law whereas article 22 the right to association. If any of the rights or freedoms recognized within the ICCPR is violated, a person must have access to an effective judicial remedy even if the violation was done by the state (Article 2(3). Some of the provisions guaranteeing the rights and freedoms in the ICCPR also allows the possibility of state parties restricting or derogating from them under particular circumstances such as during a legally declared state of emergency in a country.[23] For example, in exercising the

[18] See Joyce, D. (2015). Internet freedom and Human Rights. Volume 6 issue 2. Available at: https://academic.oup.com/ejil/article/26/2/493/423010. [Accessed 09/11/2017].

[19] The UDHR is a non-binding declaration that has metamorphosed into a source of customary international law and human rights law. Some of its clauses have attained the status of peremptory norms (ius cogens) justifiable under the International Criminal Court. See, Universal Declaration of Human Rights (1948). Available at http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf. [Accessed 09/11/2017].

[20] The ICCPR also reiterates this right although it widens its scope as shall be discussed below. The Human Rights Committee updated General Comment on Article 19 has emphasized that this free expression should be understood to include freedom of the Internet and digital media and protection. See, UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, September 2011, Art. 19: Freedoms of Opinion and Expression.

[21] See Gallacher (2012) in Davis, A, Bergu, G, Lundy, A. (2014) *Young people's engagement in strengthening accountability for the past-2015 agenda.* Available at:http://www.un.org/youthenvoy/wp-content/uploads/2014/09/YouthAccountabilitypost-2015Report.pdf.

[22] See ICCPR (1966), Available at online:https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf [Accessed 11/11/2017].

[23] Article 4 states that: "1 In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, color, sex, language, religion or

right to freedom of expression in article 19(3), certain restrictions apply in order to ensure respect of the rights or reputation of others or to protect national security, public order, public health or morals necessary for peaceful co-existence. Article 19 is also limited in article 20 which prohibits any propaganda of war or any advocacy of national, racial or religious hatred that constitutes incitement of discrimination, hostility or violence. However, this should not be misconstrued to authorize any form of infringement or stifling of civil and political freedoms offline and online which is inconsistent with the substance and spirit of the law authorizing that restriction.[24] Land (2013) opines that this protocol caters for all media even the internet as it is also a medium.[25] Restrictions placed by governments should therefore not ultra-virus the enabling articles. Restricting freedom of expression violates international law unless such restrictions are consistent with permissible restrictions done to serve the interests of humanity and done without procedural improprieties.

(IV) ICESCR, 1976

The International Covenant on Economic, Social and Cultural Rights (ICESCR) [1976][26] also supports the universal respect for and observance of human rights and freedoms. The ICESCR in Article 1, states that every person has the right to self-determination, the right to determine their political status and freely pursue their economic, social and cultural development. This cannot be fully realized without freeing the internet and allowing people to pursue these goals online as they do offline. In Article 15, it states that 'everyone has the right to take part in cultural life [and]… enjoy the benefits of scientific progresses.' The internet is a scientific progress that needs to be celebrated not suffered as the protocol provides. Takanyuki (1999) explains that the intent in this clause was to emphasize that people must be 'free men', they have to decide the laws and policies of their country by themselves. Thus, as argued earlier, the internet provides the platform for people to exercise this power on matters affecting their livelihoods. Restricting it by commission or omission deprives them of their enjoyment to the rights guaranteed by international law to which Zimbabwe is party.

(V) ACHPR, 1986

The African Charter on Human and People's Rights [1986] (ACHPR),[27] in article 9 (1&2) states that, every individual is entitled to the right to 'receive information, express and disseminate his opinions within law.'[28] Article 10(1) supports the respect of freedom of association while Article 11 advocates for the right to assemble. According to Amnesty International (2006), the right to express and disseminate opinion entails that, citizens or the media have a right to use any form of media to communicate their ideas to the public without restrictions as long such actions are within the law.[29] This shows that the ACHPR guarantees only those rights provided in law of a member state and that law is constitutional law of each member state.

social origin. 2. No derogation from articles 6, 7, 8 (paragraphs I and 2), 11, 15, 16 and 18 may be made under this provision."

[24] Article 19(3) states that restrictions placed "… shall only be such as are provided by law and are necessary."

[25] See Land, M. (2013). Toward an International Law of the Internet. Available at: www.ohchr.org/Documents/Issues/Opinion/Communications/MollyLand.pdf.

[26] See ICESCR (1976). Available online at: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

[27] See, ACHPR (1986). Available online at: http://www.humanrights.se/wp-content/uploads/2012/01/African-Charter-on-Human-and-Peoples-Rights.pdf.

[28] In Media Rights Agenda and Others v. Nigeria, Comm. 105/93, 130/94, 128/94, the African Commission for Human and Peoples' Rights, (1998) ruled that, "freedom of expression is a basic human right, vital to an individual's personal development and political consciousness, and to his participation in the conduct of public life in his country."

[29] See, Amnesty International (2006). *Undermining Freedom*. Available at: https://www.amnesty.org/download/Documents/80000/pol300262006en.pdf.

CONCLUSION

As discussed above, internet freedoms are guaranteed in international law. They are governed by same international statutes and principles governing freedoms of humans 'offline'. Above stated protocols are justiciable and victims of internet freedom infringement by their state have a right to appeal to international bodies such as the International Criminal Court (ICC), the African Commission for Human and People's Rights among others if domestic remedies are captured and stifled by the state.

SECTION 3: LEGAL FRAMEWORK GOVERNING INTERNET FREEDOMS IN ZIMBABWE

INTRODUCTION

In Zimbabwe, internet freedoms are guaranteed by the Constitution of the country which is the supreme law of the land.[30] All other laws, regulations, customs and conducts that violate the rights stipulated in the Constitution are invalid and unconstitutional. However, the government of Zimbabwe has neither been guided by this notion of constitutionalism nor constitutional supremacy. It has failed to repeal or amend many pieces of legislation that are inconsistent with internet freedoms guaranteed in the Constitution. Actually, the government has often relied on unconstitutional legislation to punish, imprison, harass and scare citizens who exercise their constitutionally given internet freedoms.

(I) CONSTITUTIONAL GUARANTEES

Apart from affirming application of customary international law found in protocols discussed above as part of law applicable in its territory,[31] Zimbabwe's 2013 Constitution, here after referred to

[30] See section 2(1) of the Constitution of Zimbabwe.

[31] Zimbabwe has adopted the doctrine of incorporation stance when it comes to application of international law in its domestic sphere; Acts of Parliament and the Constitution of the country are supreme to international treaties until such an international law is reproduced by domestic legislature. For instance, *(ii)* Section 326(1) of the Constitution of Zimbabwe states that "Customary international law is part of the law of Zimbabwe, unless it is inconsistent with this Constitution or an Act of Parliament; *(ii)* Section 327(2) adds that international treaties concluded by the President or his representatives do not bind Zimbabwe until the Parliament approves them, and they still do not form part of Zimbabwean law until they are incorporated through Acts of Parliament. However, internet freedoms in Zimbabwe have been incorporated in the constitution despite the presence of Acts of Parliament inconsistent with them. It follows that, subject to lawful limitations imposed by the Constitution, internationally recognized internet freedoms are guaranteed by the constitution of Zimbabwe; and by that virtue, Acts of Parliament inconsistent with internet freedoms are inconsistent with the Constitution that

as the 'Constitution', guarantees freedom of expression and all other internet and media freedoms.[32] In section 2(1&2), the Constitution invalidates all acts, customs, laws, and conducts that are inconsistent with it and the rights therein and mandates all state agencies to ensure that this law is followed. This clearly outlaws all legislation, conduct by state institutions and officials that violate constitutional rights enjoyed by citizens regardless of their 'online or offline' status. In section 44 of the Constitution, the state and every person or institution in Zimbabwe is obliged to protect and fulfill human rights. Section 57 of the Constitution, in line with Article 2(3) of the ICCPR and other international protocols cited above, stipulates promotion and respect of people's right to privacy. Section 57(d) specifically states that the right to privacy guaranteed in the constitution includes the right not to have "the privacy of communications infringed…" This is an unambiguous prohibition of spying, interference and seizure of equipment used by citizens to pursue their political and civil rights online. Also, section 58(1) guaranteeing freedom of assembly and association left the meaning of 'association' and 'assembly' provided for in law as general as possible to accommodate all spaces of assembling and associating that exist today and in the life to come including the internet.

Internet freedoms are also provided for in Section 59 of the Constitution which guarantees the right to peaceful demonstration and petition. The law must be understood and applied as is written, its silence on whether these rights are delimited to "offline" spaces or not was purposefully meant to allow online and offline demonstration and petition. In addition, most internet based demonstrations and petitions are short of mechanisms of violent demonstrations precluded in this section.

Section 60 (1) paragraph (a & b) states that, everyone has the right to 'freedom of thought, opinion, religion or belief' and 'freedom to practice and propagate and give expression to their thought, opinion, religion or belief, whether in public or in private and whether alone or together with others.' The Constitution is in sync with international standards regarding this right such as Article 19 of the UDHR and Article 1(3) of the UN Charter which also guarantee this freedom. In addition, Section 61 provides for free expression and media freedom which is in line with Article 19 of the UNDHR which promotes freedom of speech. Specifically, section 61(1) (a-c) stipulates 'freedom to seek, receive and communicate ideas and other information', artistic and scientific research and expression and academic freedom. This was intended to guarantee citizens their right to freely engage in discussions, investigations, publication of findings and sharing of information of journalistic, scientific, artistic and/or academic form for any reason.

In section 61(2), the constitution also guarantees freedom of media and protection of journalists' sources of information. In this regard, internet freedoms have been provided by the Constitution. Many civic society organizations, human rights defenders and citizen rights-holders would like to utilize the internet to access, share, seek and communicate information and they would like to be given privacy, confidentiality and protection whenever they release information. The Constitution has these clearly guaranteed in Zimbabwe. However, Section 61(5) delimits the rights stated in section 61(2), section 61(5) by stating that freedom of expression and freedom of the media excludes, 'incitement of violence', 'advocacy of hatred or hate speech', 'malicious injury to a person's reputation or dignity' or malicious or unwarranted break of a person's right to privacy. The fact that there is nowhere in the Constitution where we can find fixed definition of these conditions, an opportunity for legalizing violation of freedoms has been opened. Authorities are given leeway to determine what constitute information that 'incites violence', is 'advocacy of

incorporated them into law, and thus invalid to the extent of their inconsistency (Section 2(1).

[32] See, The Constitution of Zimbabwe (2013), available online at https://www.constituteproject.org/constitution/Zimbabwe_2013.pdf. [Accessed 03/11/2017].

hatred' or 'injurious to reputation and character.'[33] Thus, those defending the rights of peoples against the state can be conveniently imprisoned through partisan bending of these clauses to effectively stifle internet freedoms. Reality hits, does Zimbabwe in action adhere to the provisions of the international legal framework and the constitution?

(II) CRIMINAL LAW [CODIFICATION AND REFORM] ACT, 2004

There are pieces of Zimbabwean legislation designed particularly to undermine these freedoms and in practice, the Zimbabwean government has frequently deployed such legislation in clear disregard of what the Constitution prescribes. The Criminal Law (Codification and Reform) Act [2004] (CLCRA)[34] was set to regulate a number of citizens' freedoms online and offline. In section 33 (2b), CLCRA states that if anyone either citizen or foreigner 'makes any abusive, indecent or obscene statement about or concerning the President or an acting President, whether in respect of the President personally or the President's office; shall be guilty of undermining the authority of the president or insulting the office.' This act contradicts Section 60 (1) paragraph (a) of the Constitution, Article 19 of the UDHR and Article 1(3) of the UN Charter. Due to the severity of this Act, Martha O'Donovan, a United States national working at Magamba Network Trust was arrested and released on bail awaiting trial accused of undermining the authority of and plotting to overthrow the government of Robert Mugabe using social media. The police arrest warrant read:

> "Magamba Network Trust is believed to be in possession or control laptops, computers and printers … which were or on a reasonable ground believed to be connected in the commission or suspected commission of an offence of subverting a constitutionally-elected government as defined in section 22 (2)(a)(I) of the Criminal Law (Codification and Reform) Act, chapter 9;23."[35]

As a result, laptops and other communication devices were confiscated. This law was also used on Mashonaland civil servant Ernest Matsapa who was alleged of distributing whatsapp images and voice clips which depicted the old age of President Mugabe. This shows that freedom of expression is unconstitutionally prohibited by this law as citizens' opinions and thoughts are easily blacklisted as insults. Anyone who critiques president's conduct or exposes misconduct and/or incapacity of the president can be imprisoned under this law since there is no known, fixed and objective list of acts that constitute 'abusive, indecent or obscene statement' outlawed here.

(III) INTERCEPTION OF COMMUNICATIONS ACT, 2007

The Interception of Communications Act (ICA) [2007] is another legislation fashioned against internet freedoms in Zimbabwe.[36] Section 5(1) authorizes Commissioner of the police, Director General of the Central Intelligence Organisation and Chief of Defense Intelligence to apply to the responsible Minister and be authorized to intercept any information and communication channel in Zimbabwe whereas section 8 nullifies evidence obtained in ways contrary to section 5. Section 11 states that, authorized persons can declare disclosure of private information if it appears to them that such information endangers national

[33] According to the De La Salle University 'National security is a state or condition where our most cherished values and beliefs, our democratic way of life, our institutions of governance and our unity, welfare and well-being as a nation and people are permanently protected and continuously enhanced': Available at http://www.dlsu.edu.ph/offices/sps/rotc/pdf/ms1/threat-NatlSecurity.pdf. [Accessed 08/11/2017].

[34] See, CLCRA (2004), Available online at:http://www.refworld.org/docid/4c45b64c2.html.

[35] See, News Day Zimbabwe. 15/11/2017. Police intensify social media crackdown. Available at: https://www.newsday.co.zw/2017/11/police-intensify-social-media-crackdown. [Accessed 07/11/2017].

[36] See, interception of Communications Act (2007), document available online at: http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf.

security, necessitates detection of a serious crime or is necessary for economic wellbeing in Zimbabwe. The ICA also states that ICT or telephony service providers must give services that can be intercepted by lawful authorities (Section 12). This Act is a gateway allowing state officials to intercept telephonic and electronic communications and to monitor their content to prevent a so called 'serious offense' or a 'threat to national security' [37] The law ought to set parameters on what constitutes a 'serious offense' and/or 'treat to national security' so as to prevent leaving state officers with unlimited powers to determine what falls under these act criminalized under these terms or not. This contradicts Section 57 (d) of the Constitution which prohibits interference with citizen's communications and article 2(3) of the ICCPR which commits states to respect citizen's right to privacy. Regardless of the international legal framework and constitutional provisions, Zimbabwe remains a place where expression online endangers state crackdown since communications can be intercepted anytime although the constitution ought to render these laws invalid to the extent of their inconsistency (Lee, 2013).[38] Under such unconstitutional conditions, people are left with no right to freedom of expression and their privacy is being invaded by the same people who are supposed to protect them.

(IV) PUBLIC ORDER AND SECURITY ACT, 2002

The Public Order and Security Act (POSA) [2002] is another legislation used by the government of Zimbabwe to limit or prohibit public gatherings which are said to bring alarm and despondency.[39] In section 24, POSA obliges anyone who organizes a public gathering to give at least four days' notice to the police. This has been construed by police officers to mean that organizers 'must' apply for and get a police clearance or permission for such gatherings to be legal while in reality, the law simply requires notification. As a result, police officers have prohibited enjoyment of freedom of assembly. Section 26 of POSA states that, if the gathering is measured by the responsible ruling authorities to cause harm, it is prohibited and any person going against the ruling is punished. Section 29 (1) (a & b) allows police officers and anyone assisting them to do 'anything' to disperse a public gathering that seems 'to them' capable of causing disorder or unlawful including apprehending persons. In section 29(2), it is stipulated that if a police officer with the assistance of anyone, kills a person in the course of dispersing an unlawful gathering, such killing is not a crime but a lawful killing. Giving unfettered powers to police officers and anyone assisting them to do 'anything' to civilians to disperse any gathering that appears dangerous 'to them' condones arbitrary violation of human rights. With rampant partisanship in the police services of Zimbabwe, these sections have been used to block gatherings by human rights defenders and opposition political forces, arrest, intimidate and brutalize them and ZANU-PF militia has been allowed to kill opponents under the guise of assisting police officers who happen to be recruited from the same militia.[40] MISA notes that during 2003, over 1 200 people were arrested under POSA, these arrests were politically

[37] See also, Freedom House (2016). Available online at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwjWuf3Cn8_XAhVH8CYKHYNNC50QFgg9MAQ&url=https%3A%2F%2Ffreedomhouse.org%2Freport%2Ffreedom world%2F2016%2Fzimbabwe&usg=AOvVaw0jbESZyykwhF1zez0Ehnjd.

[38] See, Lee, R. (2013). *Threat to media freedom and freedom of expression in SADC.* Available online at: http://www.osisa.org/media-and-ict/regional/threat-media-freedom-and-freedom-expression-sadc.

[39] See, POSA (2002). Available online at: http://hrlibrary.umn.edu/research/zimbabwe-POSA.pdf

[40] Interviews, November 2017.

motivated and mostly targeting the members of the Movement for Democratic Change and some who were even neutral.[41]

To prove that laws drafted with deliberate silence on internet spaces really apply to these spaces, POSA was invoked in 2016 to arrest Evan Mawarire for gathering Zimbabwean citizens from different geographic spaces 'online' aiming to act against the falling economy.[42] POSA ultra-vires section 60 (1) paragraph (a) of the Constitution of Zimbabwe which states that every citizen has the freedom to 'practice and propagate their thoughts, opinion, religion or belief, whether **in public** or in private and whether alone or together with others' and section 59 of the constitution which reads 'every person has the right to demonstrate and to present petitions, but these rights must be exercised peacefully.' The constitution grants every citizen the right to assembly which is not recognized by POSA.

(v) Access to Information and Protection of Privacy Act, 2002

The Access to Information and Protection of Privacy Act (AIPPA) [2002][43] requires all journalists and media companies to register, the responsible minister deciding on their operations. AIPPA also states that practicing journalism without a license is a criminal offence punishable by a sentence of up to two years in prison or more and that state agencies can deny access to information (MISA, 2004). This has made it very difficult for awareness on human rights situations, corruption and election events to be done through citizen journalism as all citizens will have to be registered or risk this sentence. According to this Act, citizens have no right to access information in public bodies unless authorized by heads of such bodies. In addition, public officials can holdback requested information for 30 days following a request and this makes journalists' work impracticable. "This 30-day period may be extended by another 30 days with the permission of the responsible Commission" (MISA, 2004). AIPPA provisions were put in place to control mainly the outflow of information in privately owned media houses so as to create doomed mindsets of citizens (Amnesty International, 2004).[44] This Act is inconsistent with section 62 (1) of the Constitution which states that every citizen and the media have the right of 'access to any information held by the state or by any institution agency of government at every level, in so far as the information is required in the interests of public accountability.' This makes it clear that every citizen or permanent resident of Zimbabwe can access any form of information without any restrictions. Thus AIPPA stands invalid and government reliance on it is an unconstitutional conduct.

(vi) Postal and Telecommunications Act, 2000

The Postal and Telecommunications Act [2000],[45] in section 88 (a-c) prohibits sending messages that are 'grossly offensive, ''indecent, obscene or threatening', false, causing annoyance, 'inconvenience or needless anxiety'. The same section imposes 'a fine not exceeding level five or… imprisonment for a period not exceeding six months or' both. The Act also stipulates that communications service providers should intercept private

[41] See, MISA. (2004). *The Access to Information and Protection of Privacy Act: Two Years On* Available online at: https://www.article19.org/data/files/pdfs/publications/zimbabwe-aippa-report.pdf.

[42] Freedom House (2017). Available online at: https://freedomhouse.org/report/freedom-net/2017/zimbabwe.

[43] See, AIPPA. (2002). Available online at: www.parlzim.gov.zw/acts-list/access-to-information-and-protection-of-privacy-act27

[44] See, Amnesty International. (2004). *Case Summary: Journalists.* Available .online at: file:///C:/Users/MYACCO~1/AppData/Local/Temp/afr460082004en.pdf.

[45] See, Postal and Telecommunications Act. (2000). Available online at : http://www.potraz.gov.zw/images/documents/Postal_Act.pdf.

communications and give information when requested by authorities. Although this might seem as meant to protect private citizens and facilitate the course of justice and/or criminal investigations, it should be noted that these clauses have been used to interfere with citizens' emails, social media communications and to detain or block communications of perceived political opponents by the ruling government. There is nowhere in this Act where a clear and fixed definition of what constitutes 'offensive, threatening, false, annoyance' messages. These are left subject to subjective definitions that can easily be manipulated to thrash internet freedoms. A mere expression of opinion, critique and demand for accountability can easily be painted as 'annoying', 'false', and causing 'needless anxiety' and in this way, citizen right-holders and HRDs find themselves fined or thrown to jail for six months. This leaves people's right to privacy, freedom of expression, assembly and protest uncertain and open to state clampdown.

(VII) CYBERCRIME AND CYBER SECURITY BILL, 2017

The Computer Crime and Cyber Crime Bill hereinafter referred to as the Bill is another restrictive maneuver crafted by government to guarantee securitization of internet freedoms as far as they apply to a citizen-to-citizen interaction, monitor and censor information particularly online and authorize breach of internet freedoms of citizens by the state.[46] Although this Bill has tightly secured and ensured protection of privacy and security of communications, financial affairs, and activities of citizens and anyone in Zimbabwe (internet freedoms), it only does this in its horizontal application to citizen-to-citizen relations but not in cases of citizens vis-à-vis their government.[47] Thus, this paper limits its focus to those clauses that endanger citizens' freedoms through authorizing state interference and arbitrary breach of privacy and security.

Firstly, the Bill criminalizes "unlawful" and "intentional" interferences which means, intentional interference with internet communications and/or activities of citizens is not a crime in Zimbabwe unless such interference is not 'authorized' by law.[48] In other words, authorized state agents or service providers acting under directives of these officers can intentionally do all the prohibited acts criminalized by section 9(1)(a-h) of the Bill. Worse, section 8(e-g) criminalizes 'interference', 'obstruction' and blocking' of authorized use and access to a computer and data therein. Once authorized persons demand interference, internet users loose the right to delete data, encrypt, corrupt, shut-down their computers or internet and derogation shall attract level 10 fine or a maximum of 5 years in jail.

Section 11(2) of the Bill renders persons authorized by law or one legally effecting an extradition of a person arising from violation of

[46] See, Cybercrime and Cyber Security Bill. Available at: https://news.pindula.co.zw/wp-content/uploads/2017/08/CYBERCRIME-AND-CYBERSECURITY-BILL2017.pdf.

[47] Section 9(1) of the Bill lists the following unlawful and intentional interferences online as a criminal offence in a horizontal interaction of citizens in Zimbabwe:
(a)damaging, corrupting, impairing or deteriorating computer data; or
(b)deleting computer data ; or
(c)altering computer data; or
(d)rendering computer data meaningless, useless or ineffective; or
(e)obstructing, interrupting or interfering with the lawful use of computer data; or
(f)obstructing, interrupting or interfering with any person in the lawful use of computer data; or
(g)denying, hindering, blocking access to computer data to any person authorized to access it; or
(h)maliciously creating, altering or manipulating any data, programme or system in whole or in part which is intended for installation in a computer; shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment. This surely ensures internet privacy and security key to the exercise of internet freedoms without fear.

[48] Section 9(2) of the Bill stipulates that "Any person who contravenes subsection (1) in any of the aggravating circumstances described in section 13 is liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment." The so called aggravating circumstances include use of internet and its data to violate the Bill, assist violators in organized crime, obstructing the course of justice, sabotaging an aircraft or computer system of the security services of Zimbabwe, drug trafficking, extortion and fraud among others.

the Bill immune from consequences of criminal acts such as communicating access codes, computer data or program to unauthorized persons; activating or downloading and installing programs aimed at destroying, mutilating and modifying original data or programs in another's computer; creating, altering or destroying passwords or any other identification used to access a computer or its network. These crimes are also waivered for a police officer who has been authorized by a warrant after applying to a Magistrate to access private data, printout addresses, identification information and intercept communications or get assistance from service providers if the officer suspects or is investigating criminal activities. This means, the agents of the Central Intelligence Organization are authorized by law to exercise their statutory powers to interfere with citizens' internet freedoms without being authorized by magistrates. This is a serious exposure of online activities to any form of sabotage, espionage, threats and victimization by state intelligence agents.

Except for business-to-customer interactions,[49] Section 18 (b & c) of the Bill criminalize intentional use of protected computer system or use of pseudo headers to send multiple emails in a manner that hides track of the source or sender's details without 'lawful excuse or justification.' This section, read together with section 11(2) entail that citizens will attract a year in prison, level 5 fine or both if they utilize privacy enhancing software with the intention of blocking state surveillance, interference and sabotage since state agents have statutory power to lawfully interfere with internet freedoms in this Bill. In summation, MISA (2017) has concluded that the Bill intended to serve as a strategic obstacle to online democracy. The formation of this Bill following the 2016 online based demonstrations and mobilization by #Tajamuka and #ThisFlag movements indicate that the government saw that people were mostly relying on the anonymity feature of the internet to mobilize, demonstrate and express themselves freely hence took action to block this tool from democratizing the nation.

CONCLUSION

Internet spaces in Zimbabwe are governed with ironfisted laws despite the fact that these draconian laws are inconsistent with the Constitution. The government has shown no intention to respect the Constitution and repeal or amend unconstitutional legislation; rather, it has acted in a manner that entail supremacy of such legislation over dictates of the Constitution.

[49] See section 18(2) of the Bill.

SECTION 4: INSTITUTIONALIZATION OF CLAMPDOWN ON INTERNET FREEDOMS

INTRODUCTION

Internet freedoms in Zimbabwe are currently under state capture. Findings of the study identified three key pillars in the Zimbabwean government's strategy for stifling internet freedoms and these are: *(i)* deliberate increase of data costs, *(ii)* reliance on repressive legislation and, *(iii)* deployment of repressive state institutions. Through this trinity, journalists, HRDs, pro-democracy political players, social movements and general rights-holders have been silenced or deterred online. Key institutions in this clampdown have been: the Postal and Telecommunications Regulatory authority of Zimbabwe (POTRAZ), the Ministry of ICT, The Ministry of Home Affairs and its Zimbabwe Republic Police among others (Freedom House, 2016). The newly found ministry-Ministry of Cyber Security was also created to govern internet freedoms.[50] Rights-holders and Human Rights Defenders (HRDs) have suffered continuous crackdown on their internet freedoms due to work of these institutions.

STATE OF INTERNET FREEDOMS IN ZIMBABWE

The state of internet freedom and/or governance in Zimbabwe shows a serious level of derogation from the provision in international and constitutional laws that guarantee such liberties. 'Freedoms are partially curtailed. People are only free to enjoy internet freedoms but afterwards they will be in trouble with Mugabe's police or secret agents.'[51] It was established that 'there is too much interference by the state and communication rights are violated.'[52] It was also discovered that HRDs' expression of opinions is being turned into criminal acts and some are even arrested after airing their views.[53] Thus, there was a 94 % agreement among interviewed key informants that internet freedom in Zimbabwe is semi-guaranteed. Supporting this assertion is a rise in arrests targeting social media users and HRDs who use internet to execute their programs. For instance, Ernest Mudzengi the director of Media Centre was arrested and interrogated after his organization covered a story on a plot to bomb Gushungo Diaries.[54] The study found that the state has institutionalized a network of strategies to stifle internet freedoms and this has posed a serious challenge to the full realization of these rights. Key challenges as shall be discussed below include: a deliberate increase in data costs to limit internet use, use of draconian legislation to limit and interfere with citizens' liberties online and use of state institutions to clampdown civic liberties online.

MAIN CHALLENGES FACED BY HRDS AND DEMOCRACY ACTIVISTS UNDER INTERNET GOVERNANCE IN ZIMBABWE

(A) DELIBERATE INCREASE OF DATA COSTS

Although internet penetration has been commendable in major towns where research was carried, it was observed that data costs have increased following government regulations and directives in a measure to counter social media demonstrations aided by affordable data costs in the mid 2016.[55] Seventy percent of

[50] It should be noted that after this paper had been written and was awaiting publication, the ICT and Cyber Security ministries were merged by the junta government that deposed former president Robert Mugabe through military coup d'état into one ministry of ICT and Cyber Security. The minister in charge is the same ICT minister who presided over the Cyber Crime Bill. So, this paper argues that the previous ministry exists as a department under the current one for and its raison d'être has not yet changed, the junta is satisfied with the work done by the minister to stifle internet freedoms under the previous regime.

[51] Interview with a lady from a Marondera community based organization(29/10/2017)

[52] This view was raised in all interviews held across main urban cities of Zimbabwe (ZDI&MC Interviews, October-November 2017).

[53] Interviews, November 2017.

[54] See Voice of America. 2016. Available at: https://www.voazimbabwe.com/a/zimbabwe-politics-police-media-centre-mudzendi-zimbabwe-sentinel/3275013.html.

[55] ZDI&MC Interviews, October-November 2017.

interviewed key respondents stated that data costs are no longer affordable and this came following 2016 social movement demonstrations that utilized the internet and social media for mobilization and citizen journalism.[56] 'Due to directives from POTRAZ, telecommunications and internet service providers are pricing their data products beyond the reach of the ordinary Zimbabweans.'[57] This was also stressed by HRDs' community Based Organization official from Mutare who stated that:

> … the government's directive to increase internet data prices has limited use of and access to internet. We do not have resources to conduct online human rights and democracy promoting activities because of financial limitations. We cannot afford to be on the internet using Econet for more than 30 minutes, it's very expensive'.[58]

Of all interviewed officials in Bulawayo, Mutare, Harare and Marondera, 85% stated that the high charges pressed on mobile data are a worrying issue that has reduced people's visibility in online platforms particularly social media.[59] As shall be revealed below, POTRAZ has been on record issuing threats to social media users and coercing mobile telephony service providers to increase data charges to stifle internet use for human rights promotion.[60]

(B) Use of State Institutions

In addition to deliberate clampdown on ease of internet access, the state has deployed various state institutions and agencies to unleash internet clampdown and stifle internet freedoms. Following are key findings on what the study identified as key institutions stifling internet freedoms in Zimbabwe.

(i) Ministry of ICT & POTRAZ[61]

The Ministry of Information and Communications Technology, Postal and Courier Services has been very visible through its internet stifling handle – POTRAZ, a regulatory authority under this ministry.[62] POTRAZ has used its powers to fix and regulate service charges to stop service providers from giving data bonuses, free voice calls and increased data costs amid revelations that this was in partial fulfillment of government strategies to deal with activism on social media.[63] POTRAZ issued a public notice in the eve of social media demonstrations in 2016 stating that: it is against it, labeling them as subversive, and threatening to use 'sim card' registry data to identify users and prosecute them.[64] In addition, POTRAZ's decision to arm-twist telecommunication service providers to stop programs that gave cheap access to mobile telephony was clearly aimed at limiting the number of citizens who access social media due to cheap data charges given by these operators.[65] The move by POTRAZ was to stifle freedom of expression by reducing users of internet.

(ii) Ministry of Home affairs & ZRP

The Zimbabwe Republic Police (ZRP) has been a very fierce arm of government under Ministry of Home Affairs that has been used to clampdown internet freedoms so far.[66] This notion had a 96% frequency in interviews held during this study. Following the uptake and reliance on social media for activism and free expression in 2016, reports show that more than 31 journalists were assaulted, harassed, arrested or detained while reporting on

[56] See supra note 53.

[57] ZDI&MC Interview with a Civil Society Official in Bulawayo, 29/10/2017.

[58] Interview with a community based organization worker in Mutare (30/10/2017).

[59] Analysis of data collected through interviews with officials from social movement leaders, HRDs' organizations, journalists, CBOs and politicians.

[60] See ZimEye, 10/08/2017. *Mandiwanzira Bans Internet Data Bundles*. Available at: https://www.zimeye.net/mandiwanzira-bans-internet-data-bundles/.

[61] See supra note 50 .

[62] ZDI&MC Interviews, October-November 2017. See also, Regulatory Determination No 1 of 2016.

[63] See ZimEye, 10/08/2017. *Mandiwanzira Bans Internet Data Bundles.* Available at: https://www.zimeye.net/mandiwanzira-bans-internet-data-bundles/.

[64] See POTRAZ Public Notice. 2016. Available at: https://pbs.twimg.com/media/CmrnPt7WcAATYcO.jpg:large.

[65] ZDI&MC Interviews, October-November 2017.

[66] 70% of interviewed Key informants reiterated this point (ZDI&MC Interviews, October-November 2017).

protests in that year and the ZRP was used to execute these assaults on internet freedoms.[67] It is through the work of ZRP that Martha O'Donovan a United States national working at Magamba Network Trust was arrested and released on bail awaiting trial for undermining the authority of and plotting to overthrow the government of Robert Mugabe using social media.[68] Pastor Evan Mawarire, a leader of #ThisFlag movement and #Tajamuka social movement leaders has been victimized and brutalized by ZRP for exercising their rights peacefully and legally online and off-line.[69] Despite clear and incontrovertible evidence of clampdown on citizens' liberties, the Zimbabwe Republic Police is on record saying it does not believe POSA is a draconian piece of legislation but a good law for maintaining law and order in the country.[70]

The duty of the ZRP is to maintain peace and order in the country but their conduct mostly tend to stifle people's freedoms in defense of ZANU-PF interests. This has been the line of thinking among the Zimbabwe National Army leadership too. In an unveiled reference to peaceful demonstration by social movements and opposition political parties, General Phillip Valerio Sibanda, the ZNA commander in August 2016 stated that social media use by insurgents and regime change agents has emerged as a security threat and that ZNA is,

> … already dealing with these threats. As an army, at our institutions of training, we are training our officers to be able to deal with this new threat we call cyber warfare where weapons — not necessarily guns but basically information and communication technology — are being used to mobilize people to do the wrong things. We will be equal to the task when the time comes.[71]

In this regard, the future of internet freedoms looks bleak since the same ZNA has flexed its muscles in determining who succeeds President Robert Mugabe and the composition of persons to constitute that government.

(III) Ministry of Cyber Security, Threat Detection & Mitigation[72]

The study also highlighted growing fears following the creation of the Ministry of Cyber Security, Threat Detection and Mitigation. This ministry was created following President Mugabe's revelation of his plan to implement measures similar to those of Japan, Korea and China in order to 'ban those who abuse the internet' – a serious promise to stifle internet freedoms.[73] Respondents argued that its mere presence and obscurity surrounding its actual role has deterred many citizens from using internet in fear of their personal lives. 'As a result, many people are afraid to speak out on human rights and democracy issues due to fear of being nabbed by the government'[74] It was also revealed that Martha O'Donovan was arrested to send a clear message that the ministry is out to interfere with citizens' internet affairs, capture critics of the government and jail them.[75] To make matters worse, George Charamba, a spokes person of the president Mugabe told The

[67] MISA (2016). This was also reiterated in an interview with a social movement activist in Harare (31/10/2017) who noted that 'The Police have arrested people and the courts of law have prosecuted them for exercising their rights. Evan Mawarire was arrested by the police several times and brought before the courts again on numerous occasions.'

[68] See DailyNews. 05/11/2017. *Zim police arrest US citizen over tweet* Available at: https://www.dailynews.co.zw/articles/2017/11/05/zim-police-arrest-us-citizen-over-tweet.

[69] See, New Zimbabwe.28/11/2016. Police Arrest Tajamuka Leadership Over Bond notes Briefing. Available at: http://www.newzimbabwe.com/news-33504-Harare+police+arrest+Tajamuka+leadership/news.aspx .

[70] Chifera, I. (2014). *Zimbabwe Police Say POSA Key in Maintaining Law, Order*. 02/07/2014. Available at: https://www.voazimbabwe.com/a/zimbabwe-public-order-and-security-act-police-want-posa-to-/1949211.html.

[71] See Nehanda Radio, 05/08/2016

[72] This is now under Ministry of ICT and Cyber Security.

[73] See Daily News 05/04/2016. Available online at https://www.dailynews.co.zw/articles/2016/04/05/mugabe-s-plan-to-ban-social-media-condemned.

[74] ZDI&MC Interview with a Civil Society worker, 29/10/2017.

[75] Analysis of interview data, November 2017.

Herald that, 'the Ministry of Cyber Security, Threat Detection and Mitigation is a protective portfolio aimed at protecting the nation from cyber threats posed by the abuse of social media.'[76] This 'abuse of social media' and 'cyber threats' was a reference to democratic and peaceful civic and social movement activism. People are afraid of being arrested, tortured or detained after they express themselves hence find it better and safe to self censor. 'People are therefore reserved in terms of using social media to post anything related to the democratic rights entitled to them', said a respondent. Directly or indirectly, this ministry goes along with the Computer and Cyber Crime Bill discussed above. Thus, the Bill together with the Ministry of Cyber Security, Threat Detection and Mitigation are tools used to suppress people's freedom of expression (MISA, 2017).

(C) Repressive Legislation

The study also identified repressive legislation as part of the trinity of war against citizens' internet freedom used by the state.[77] Key legislation used to suppressed internet freedoms as indicated by respondents are as presented above. Although this repressive legal framework has been exhaustively examined hereinbefore, it is important to present a summary of views captured during interviews. 'The Cyber Security Bill limits interactions online through the fear factor. People are afraid of being caught on the other side of the law.'[78] One interviewee[79] added that the Bill is not yet commissioned but it is perceived to aim at limiting freedom of opinion, association among other freedoms on enjoyed online. The government of Zimbabwe passed the Cyber Security Bill (still in process) to directly monitor the internet so as to eliminate dissent. Citizen journalists from visited towns added that laws like CODE, AIPPA, POSA and ICU also threaten journalists even in this digital era.[80] The government of Zimbabwe continues to monitor and infringe freedom of expression and media freedom.

Conclusion

In conclusion, internet freedoms are not enjoyed as expected in Zimbabwe. The government has put in place an authoritarian state craft for the purpose of clamping down internet freedoms through arrests, intimidation, spying, threats, deterrence and blocking access. Thus, the Zimbabwean internet space still needs liberation.

[76] See, The Herald. 11/10/2017. Govt Explains Cyber Security Ministry Role. Available At: Http://www.herald.co.zw/govt-explains-cyber-security-ministry-role. /

[77] ZDI&MC Interviews, October-November 2017.

[78] Interview with a social movement lady, Bulawayo (31/10/2017)

[79] Interview with a female journalist in Mutare(30/10/2017)

[80] ZDI&MC Interviews, October-November 2017.

SECTION 5: CONCLUSION AND RECOMMENDATIONS

CONCLUSION

This study concludes that, the internet governance legal and institutional framework in Zimbabwe is currently prohibitive and combative to rights-holders and human rights defenders online. Enjoyment of internet freedoms is limited and fiercely challenged by the governance system in place. The Constitution has gone a step further in localizing international internet freedom standards to the extent that, when it is implemented to its full iota and doter, internet governance will cease to be authoritarian. However, the government has failed to repeal or align inhibitive Acts of Parliament to make them consistent with the Constitution. These pieces of legislation have been relied upon by many government institutions to stifle internet freedoms. As a result, rights-holders, HRDs, social movements, pressure groups, political parties and religious movements continue to suffer police brutality, arrests, threats, insecurity and interferences orchestrated by the authoritarian internet governance structure in Zimbabwe. This has made human rights and democracy promotion initiatives very difficult.

RECOMMENDATIONS

To enhance internet freedoms under authoritarian internet governance framework in Zimbabwe, this study recommends the following to key stakeholders:

GOVERNMENT

- Repealing or amendment of authoritarian legislation such as CODE, POSA, AIPPA, ICA among others to make them consistent with the Constitution of Zimbabwe. This will pave way for internet democracy and enjoyment of peoples' liberties online.
- There is need to conduct compulsory constitutional law trainings in the public service, security services and government ministries to restore respect of the Constitution and human rights due to citizens online.
- Government should encourage private sector, public sector and civil society engagements and interfacing platforms to share ideas on best internet governance practice that will open opportunities for enjoyment of internet freedoms while ensuring security of the state and its citizens' interests.
- Internet freedoms awareness must be enhanced through inclusion of internet freedom content in the education curriculum at primary school level. This will ensure the creation of a generation of democratic, active, and free citizens who are aware of their liberties online and responsibility to protect them.

CIVIL SOCIETY AND HUMAN RIGHTS DEFENDERS

- Civic society and human rights defenders should claim and defend internet freedoms through petitioning government, mobilizing citizen demonstrations, taking matters of violation of internet freedoms to the Constitutional court and other regional and international remedy forums.
- Civil society and HRDs should raise awareness on online liberties through creation of social media sensitization forums, conducting civic education forums at national and community levels and conducting road shows on the same. People need to be made aware of their internet freedoms in order to eliminate fear.
- Educating members of the public on the privacy settings that can be applied on social media is crucial. This should include cross-country community based civic education platforms wherein skills and strategies will be imparted to the people and encourage citizen journalism to expose violations and enforce accountability among duty-bearers.

- Civic organizations and HRDs across the country should create dense networking systems using modern ICTs through which to share ideas, skills and disseminate information and establish lasting solutions to internet freedom challenges.

JOURNALISTS

- There is need for civic education targeting journalists to enhance their professionalism and adherence to human rights in their profession online.
- Journalist forums, education and networking forums should be increased to link practitioners at national level to their fellows at grassroots levels across the country. This will enhance sharing of skills and strategies and increase coverage and transparency of internet governance practices across the country.
- Journalists should write and verify news for authenticity before publishing to avoid misinforming the public. Many interviewees advised journalists to stick to the pillars of ethical journalism: objectivity, truth, balance, impartiality, fairness, accuracy and lack of bias.
- There is need to create a dense network of journalists in public media, private media, social media, freelance and citizen journalists at grassroots levels. This will enhance efficient reportage.
- Journalists should be trained on best ways to securitize their operations online to galvanize them against espionage, interference and sabotage.
- Journalists should network and coalesce to petition parliament on institutional and legislative reforms necessary for freeing internet based journalism.

POLITICIANS AND SOCIAL MOVEMENTS

- Increase awareness of internet freedoms amongst citizens in all political party structures from national to grassroots levels. Should never grow weary in educating their constituencies on importance of taking advantage of online information sharing.
- Encourage uptake of internet tools for monitoring, informing, and demanding accountability from leaders and keeping representatives updated on citizens' demands and human rights situations.
- Pressure should be mounted on top leadership to align oppressive legislation with internet freedom standards stipulated in the Constitution.
- Spread timely information on abuse and violation of rights
- Education campaigns for human rights awareness and advocacy should be maintained.

PRIVATE SECTOR

- There is need to secure internet liberties of citizens in all services provided and spaces of interaction in the private sector. This sector should promote internet freedoms through adoption of policies, regulations and culture.
- Private internet service providers should protect the privacy of service users and adopt technologies that hinder interference by spies and saboteurs
- Engagement with civic society and government should be done continuously for the purpose of finding best ideas that can be adopted to protect and promote internet freedoms. The private sector should assist in pressuring government to review authoritarian laws that infringe internet liberties.
- Service providers should not charge users in prohibitive manner.

- The private sector should also assist in exposing violation of liberties and jealously protect people's accounts, transactions and communications in their custody.

INTERNATIONAL COMMUNITY

- The international community should receive internet freedom reports and grievances from civic society and other players and assist in pressuring governments to resolve them.
- Facilitating civic engagements and dialogues at regional and international levels to find strategies through which internet liberties can be enjoyed in such a way that does not compromise peace and security.
- Internet freedom must be adopted and emphasized as values not separate from offline freedoms and its security should be guaranteed under existing regional and international mechanism.

BIBLIOGRAPHY

ARTICLES & REPORTS

Amnesty International. 2004. *Case Summary: Journalists. [Online].* Available at: https://www.amnesty.org/download/Documents/92000/afr460082004en.pdf. [Accessed: 14/11/2017].

2006. *Undermining Freedom.* [Online]. Available at: https://www.amnesty.org/download/Documents/80000/pol300262006en.pdf [Accessed: 08/11/2017].

2017. *Zimbabwe: arrest over 'insulting' Mugabe tweets marks new assault on internet freedom.* [Online]. Availableat:https://www.amnesty.org/en/latest/news/2017/11/zimbabwe-arrest-over-insulting-mugabe-tweets-marks-new-assault-on-internet-freedom/. [Accessed: 08/11/2017].

Freedom House. 2016. *Freedom House 2016.* [Online]. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwjWuf3Cn8_XAhVH8CYKHYNNC50QFgg9MAQ&url=https%3A%2F%2Ffreedomhouse.org%2Freport%2Ffreedomworld%2F2016%2Fzimbabwe&usg=AOvVaw0jbESZyykwhF1zez0Ehnjd. [Accessed: 08/11/2017].

2017. *Freedom on the net 2017*. [Online]. Available at: https://freedomhouse.org/report/freedom-net/2017/zimbabwe. [Accessed: 13/11/2017].

Gallacher, H. 2012. in Davis, A, Bergu G &Lundy, A. 2014. *Young people's engagement in strengthening accountability for the past-2015 agenda*. [Online]. Available at:http://www.un.org/youthenvoy/wp-content/uploads/2014/09/YouthAccountabilitypost-2015Report.pdf. [Accessed: 09/11/2017].

Joyce, D. 2015. *Internet freedom and Human Rights*. Volume 6 issue 2. [Online]. Available at: https://academic.oup.com/ejil/article/26/2/493/423010. [Accessed: 05/11/2017].

Land, M. 2013. *Toward an International Law of the Internet.* [Online]. Available at: http://www.ohchr.org/Documents/Issues/Opinion/Co

mmunications/MollyLand.pdf. [Accessed: 08/11/2017].

Lee, R. 2013. *Threat to media freedom and freedom of expression in SADC.* [Online]. Available at: http://www.osisa.org/media-and-ict/regional/threat-media-freedom-and-freedom-expression-sadc. [Accessed: 09/11/2017].

MISA. 2004. *The Access to Information and Protection of Privacy Act: Two Years On. [Online].* Available at: https://www.article19.org/data/files/pdfs/publications/zimbabwe-aippa-report.pdf[Accessed: 16/11/2017].

Rue, L. 2011. *Monitoring freedom of expression: The apc-la rue framework. [Online].* Available at: https://www.apc.org/en/pubs/internet-freedom-index-draft-checklist. [Accessed: 06/11/2017].

Solidarity Peace Trust. 2004. *"Disturbing the peace" : An overview of civilian arrests in Zimbabwe: February 2003 –January 2004*. [Online]. Available at: https://www.scribd.com/document/35878974/Disturbing-the-Peace. [Accessed: 09/11/2017].

LEGAL PROTOCOLS

Government of Zimbabwe. 2002. *Access to Information and Protection of Privacy Act*. [Online]. Available at: www.parlzim.gov.zw/acts-list/access-to-information-and-protection-of-privacy-act27. [Accessed: 03/11/2017].

2002. *Public Order and Security Act.* [Online]. Available at: http://hrlibrary.umn.edu/research/zimbabwe-POSA.pdf. [Accessed: 14/11/2017].

2002. *Postal and Telecommunications Act*. [Online]. Available at : http://www.potraz.gov.zw/images/documents/Postal_Act.pdf. [Accessed: 15/11/2017].

2004. *Criminal Law [Codification and Reform] Act.* [Online]. Available at: http://www.refworld.org/docid/4c45b64c2.html[Accessed: 13/11/2017].

2007. *Interception of Communications Act*. [Online]. Available at: http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf. [Accessed: 08/11/2017].

2013. *The Constitution of Zimbabwe*. [Online]. Available at https://www.constituteproject.org/constitution/Zimbabwe_2013.pdf. [Accessed: 09/11/2017].

2017. *Cyber crime and Cyber Security Bill*. [Online]. Available at: https://news.pindula.co.zw/wp-content/uploads/2017/08/CYBERCRIME-AND-CYBERSECURITY-BILL2017.pdf. [Accessed: 08/11/2017].

OAU 1986. *African Charter on Human and People's Rights.* [Online]. Available at: http://www.humanrights.se/wp-content/uploads/2012/01/African-Charter-on-Human-and-Peoples-Rights.pdf. [Accessed: 05/11/2017].

UN. 1945. *United Nations Charter*. [Online]. Available at: http://www.un.org/en/charter-united-nations/. [Accessed: 13/11/2017].

1948. *Universal Declaration of Human Rights*. [Online]. Available at http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf. [Accessed: 13/11/2017].

1966. *International Covenant on Civil and Political Rights*. [Online]. Available at: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. [Accessed: 06/11/2017].

1976. *International Covenant on Economic, Social and Cultural Rights. [Online].* Available at: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. [Accessed: 09/11/2017].