THE CYBERCRIME & CYBERSECURITY BILL: Grave Consequences on Internet Freedoms in Zimbabwe!

Advocacy Paper
February 2018

Zimbabwe Democracy Institute

Copyright Statement

Zimbabwe Democracy Institute
66 Jason Moyo Avenue,
2nd Floor
Bothwell House
Harare
Zimbabwe

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 focus group discussions participants 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.

Contents

List of Acronyms

AIPPA	Access to Information and Protection of Privacy Act
CI	Counterpart International
CLCRA (CODE)	Criminal Law [Codification and Reform] Act
COPAC	Constitution Parliamentary Committee
Cybercrime Bill	Cybercrime and Cyber-security Bill
ICCPR	International Covenant on Civil and Political Rights
MC	Media Centre
MISA	Media Institute for Southern Africa
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UDHR	Universal Declaration of Human Rights
ZDI	Zimbabwe Democracy Institute
ZRP	Zimbabwe Republic Police

MAJOR HIGHLIGHTS

Done in partial contribution to ZDI and Media Centre investigation into the state of internet governance/freedom in Zimbabwe, this paper presents findings of the study of the Cybercrime and Cyber-security Bill and its implications on online access to information, media freedom and freedom of speech. It examines: *(i)* The Cybercrime Bill's domestic and constitutional context and; *(ii)* selected key sections of The Cybercrime Bill's highlighting their implications on internet freedoms in Zimbabwe. This was aimed at identifying the flaws associated with The Cybercrime Bill, mapping advocacy areas, informing advocacy on the matter and lobbying for the revision of the Cybercrime Bill to ensure consistency with constitutionally guaranteed freedoms of and international human rights practices before it is enacted into law. Thus, following is a summary of key findings:

- ✓ The political context of the Cybercrime Bill dictates that, in crafting this Bill, the government was driven more by its fear of the citizen power and its desire to protect itself from citizen and civic pressure unveiled by unsuppressed internet freedom than amplifying citizens' security when exercising their freedoms online.
- ✓ The Bill is very repressive and ideas behind it germinated from the ruling regime's realization that internet use in the country is on a growing trend and this has catapulted its use for: *(i)* massive citizen mobilization for accountability advocacy; *(ii)* human rights and accountability monitoring; *(iii)* conduct country-wide civic education, voter education and other electoral purposes and; *(iv)* give citizens alternative sources of information and fact-checking free of manipulation done in the mainstream media.
- ✓ Although with some progressive attempts to curb cybercrime, the Cybercrime and Cyber-security Bill was, to a greater extent, crafted with authoritarian intentions to: *(i)* instigate self-censorship among citizens and thereby cushioning government against citizen oversight; *(ii)* increase government authority and ability to 'legally' violate privacy thereby enabling state interference with communications online and; *(iii)* contain, dissuade and clampdown potential social media revolutions and demonstrations that had proven to be presenting a real platform for citizens' will to be done.
- ✓ The Cybercrime Bill is ultra-vires the founding values and basic pillars of the Constitution since citizens' right to access information and freedom of expression are stifled by the Bill regardless of the fact that these rights are provided for in the Constitution of the country. It is therefore, null and void to the extent of its inconsistency.
- ✓ The Cybercrime Bill gives a superfluous definition of a 'computer device' and computer data storage medium which gives room for investigating officers to seize personal electronic equipment and interfere with personal communications even if devices seized are not linked to cybercrime.
- ✓ The Cybercrime Bill is very unclear about vital legal and institutional safeguards in place to protect individual rights given that it legalises breach of online privacy, and interference with private communications by state agents in their process of collecting evidence or prosecution of cybercrimes.
- ✓ The Cybercrime Bill impacts negatively on the citizens' right to privacy enshrined under 57 of the Constitution because: *(i)* citizens will be subjected to State's searching of their personal possessions; *(ii)* it imposes restriction of personal autonomy. The Cybercrime and Cyber-security Bill infringes human rights as its

provisions run counter to the constitution of Zimbabwe.

- ✓ The Cybercrime Bill has very contentious omissions that render too much volition to state agents to define law for citizens, thus leaving citizens vulnerable to abuse. For instance, there is no clarity or certainty on what the law means by "unlawful" access to information and "unlawful" acquisition of data stipulated in Section 6 of The Cybercrime Bill.
- ✓ There is need for civil society to embark on massive mobilization and sensitization of the people through conducting road-shows to: *(i)* inform citizens about grave implications of The Cybercrime Bill on their internet freedoms; *(ii)* demonstrate against The Cybercrime Bill's repressive provisions and; *(iii)* petition the government to revise and amend The Cybercrime Bill's suppressive provisions before being enacted into law.
- ✓ There is need for media and media support organisations to conduct and promote citizen education and enlightenment on the Cybercrime Bill and initiate much-needed reforms in regard to the statute. Well informed citizens are in a better position to monitor and hold government officials to account for their conduct in public offices.

1. INTRODUCTION

The evolution of the internet with its social media in the last decade has significantly changed the definition of communication and social interaction among various people from diverse social and cultural backgrounds. The internet has unveiled an unprecedented volume of resources for information and knowledge acquisition that open up new opportunities and challenges for expression and participation. Access to information by citizens and information consumption has therefore increased due to use of internet particularly social media platforms such as Facebook, Twitter, YouTube and Whatsapp. This is against a background fact that information, whether accessed online or offline is widely regarded as a foundation of a well-functioning democracy. The most celebrated sphere of human life that has been immensely influenced by this development has been governance and human rights. Internet has opened up development opportunities and its use to share and access information has: *(i)* forced traditionally opaque institutions of government to be transparent; *(ii)* influenced citizens to engage government; *(iii)* given civic society organization the great ease of mobilizing and influencing public opinion whereas; *(iv)* human rights monitoring and reporting has been eased (UNESCO).[1] The provision of information and media content pertaining to local, regional and international political and socio-economic affairs has become easy courtesy to wide use of internet. The internet has, therefore, undoubtedly become a vital piece of infrastructure and a significant avenue for global communication, community formation and governance.[2]

Whereas, internet and information access avenues it created are a good development applauded by many, there is however a growing trend among authoritarian regimes wherein, ceaseless efforts to curtail citizens' access to the internet have been instituted. Various measures including: *(a)* prohibitive legislation; *(b)* use of state police (ZRP); *(c)* internet black-outs sabotage and; *(d)* espionage have been utilized in this regard. Despotic governments have over intensified cyber security in calculated move to get a legal go-ahead to spell the "dos" and "don'ts" online in a veiled ploy to: *(i)* capture the internet and limit access to government information by citizens; *(ii)* shun publicity and transparency; *(iii)* limit accountability pressure enabled by internet platforms and; *(iv)* get unchallenged violation of privacy and personal security online. Thus, internet and digital platforms have been deployed to conduct widespread surveillance of citizens.[3]

It is in this context that Zimbabwe has seen itself being among the most innovative authoritarian regimes to put in motion a legal framework (Cybercrime and Cyber-security Bill, 2017) to control citizens' activities online, monitor online activities and draw boundaries for internet users as far as access to information and information dissemination is concerned. This has come contrary to resolutions of the Internet Security Forum held in Estonia in 2014 and it is a baffling experience which intensify inherent fears foreseen by the then United Nations Secretary General, Ban Ki-moon that:

> *I am disturbed by how States abuse laws on Internet access. I am concerned that surveillance programmes are becoming too aggressive. I understand that national security and criminal activity may justify some exceptional and narrowly-tailored use of surveillance. But that is all the more reason to safeguard human rights and fundamental freedoms. Some argue that they need to curtail*

[1] https://en.unesco.org/themes/freedom-expression-internet

[2] European Journal of International Law, Volume 26, Issue 2, 2015: Available at: https://academic.oup.com/ejil/article/26/2/493/423010

[3] Frank La Rue, 2011.Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/23/40.

freedoms to preserve order. I say they need to protect freedom or they will undermine order.[4]

Since Zimbabwe has went a step further to create a whole Bill aimed at legalizing state surveillance online, it is important to emphasize and make clear the points that: *(i)* internet freedoms are under siege in Zimbabwe and; *(ii)* freedom of expression and human rights monitoring efforts must be applied not only to traditional media but also to the internet and all types of emerging media platforms. The United Nations Human Rights Committee in its updated General Comment on Article 19 has also pointed to the need to take greater account of the internet and digital media particularly the protection of free speech.[5]

Objectives

In light of the Cybercrimes and Cyber-security Bill, this advocacy paper seeks to contribute to the need to ensure that:

a) Citizens are guaranteed easy access to information held by the state and other government institutions as a mechanism of ensuring transparency and accountability;
b) Dialogue on the constitutionality of The Cybercrime Bill is provoked and guided to alert institutions responsible for safeguarding constitutional supremacy on the same.
c) Civic society and other political movements are given advocacy data and encouraged to increase awareness on the implications of The Cybercrime Bill on online privacy, security and freedoms of citizens and;
d) Citizens are equipped with knowledge and enabled to engage duty-bearers to protect their internet freedoms as they plan to enact the Cybercrime Bill into law.

Methodology

This study was purely qualitative in that, it used desk-research, content analysis and focus group discussions with purposively sampled key-informants drawn from the academia, civic society leaders and media practitioners. A group discussion guide was created which had topics on ways through which government can be pressured to ensure that when the Cybercrime Bill comes into law; all threats to human rights online are removed.

[4]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

[5]UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, September 2011, Art. 19: Freedoms of Opinion and Expression.

2. THE CYBERCRIME BILL'S DOMESTIC CONTEXT

The Cybercrimes Bill came at a moment when internet has become an indispensable instrument for promoting grassroots democracy as a platform for airing local issues, providing an alternative source of information to mainstream media outlets and promoting democracy and human rights in the country in Zimbabwe.[6] The wave of "hash-tag" protests against former president Robert Mugabe's government in 2016 were purely organized through the use of social media. For instance, On the 6th of July 2016, Evan Mawarire's #ThisFlag movement almost shutdown the nation as citizens were massively mobilized through social media to stay at home, banks and shops across all towns and cities were closed. The event drew the attention of the whole world. Such mass protests against former president Robert Mugabe were mainly spearheaded by social media particularly Facebook, Twitter and WhatsApp to demand government transparency and accountability, naming and shaming corruption, poverty and injustice. However the government, during the day of mass protests, responded through an unprecedented social media blackout. Subscribers to key mobile telephony service providers such as Telecel, NetOne, ZOL, TelOne ADSL and Econet could not access their WhatsApp accounts. They were denied their constitutional right to access of information particularly on the internet by this blackout.

Following the above stated internet aided mass protests, the leader of #ThisFlag movement, Pastor Evan Mawarire, was then arrested on the 12th of July 2016 by the Zimbabwe Republic Police and charged with inciting public violence online. This followed after the government has sent serious threats to the citizens for using social media. For instance, on the 9th of July 2017, three days after the mass protests, the then Minister of Information, Media and Broadcasting Services Christopher Mushohwe said "authorities were watching all those who abuse social media to provoke trouble in the country." The government consistently threatened citizens stating that it will arrest anyone sharing subversive material on social media. Now, given this role of the internet in Zimbabwe to mobilize people for demonstrations calling for justice, equality, accountability and greater respect of human rights, the government has swiftly responded through enacting the Cybercrime and Cyber-security Bill aimed at punishing social media users.

Of late, the minister of ICT and Cyber-security has revealed to the Parliamentary Committee on Media, Information Communication Technology and Cyber Security on 8 February 2018 that, working with the office of the Attorney General, his ministry is in the process of creating an omnibus Cyber-security Bill merging the draft Data Protection Bill and the Electronic Transactions and Electronic Commerce Bill and the Cyber security and Cybercrimes Bill.[7]

The new Constitution of Zimbabwe extensively guarantees internet freedoms which the Cybercrime Bill threatens to stifle. The Constitution states that the "Constitution is the supreme law and any law, practice, conduct or custom inconsistent with it is invalid to the extent of its inconsistency."[8] Given the inconsistency of the Cybercrime Bill's provisions with the Constitution, as shall be demonstrated hereinafter, its invalidity can and must be declared.

The preamble to the Constitution recognizes the need "to entrench democracy, good, transparent and accountable governance and the rule of law"; it reaffirms the people's commitment to "upholding and defending fundamental human rights and freedoms"

[6] ZDI-Media Centre Focus Group Discussion, February 2018

[7] http://kubatana.net/2018/02/23/omnibus-cyber-bill-muddies-fundamental-rights/

[8] Section 2(2) of the Constitution of Zimbabwe (Amendment No 20) Act)

and the resolve "to build a united, just and prosperous nation, founded on values of transparency, equality, freedom, fairness, honesty and the dignity of hard work.[9] Enshrined in the same constitution is the right to privacy, access to information and freedom of expression which are under threat as a result of the Cybercrime Bill. Section 57 of the constitution provides that:

> *Every person has the right to privacy, which includes the right not to have (a) their home, premises or property entered without their permission, (b) their person, home, premises or property searched; (c) their possessions seized; (d) the privacy of their communications infringed; or (e) their health disclosed.*

Thus, search and seizure in the Cybercrime Bill clearly indicate its inconsistency with the Constitution, hence invalidity. In addition, Section 61 (1) provides that: "every person has the right to freedom of expression, which includes-(a) freedom to seek, receive and communicate ideas and other information; (b) freedom of artistic expression and scientific research and creativity; and (c) academic freedom."

The Cybercrime Bill is silent on safeguarding citizens' liberties and enhancing accountability in the process of combating cybercrimes. This entails that the powers behind this Bill were solely preoccupied with their desire to monitor and regulate citizens' use of internet and thwart their ability to harness internet opportunities to claim all other liberties.[10]This desire has been pursued further through the establishment of the Ministry of Cyber security, Mitigation and Threat Detection which has however been merged with the Ministry of Information Communication Technology following the military-aided overthrow of former President Mugabe's government. On paper, such actions by the government of Zimbabwe give a misleading impression that the regime is taking serious measures to combat any potential cyber threat when in actual fact; it is trying to protect the interests of the State – to shun public surveillance and accountability.

Thus, this paper: *(i)* samples and analyses key sections of the Cybercrime and Cyber-security Bill which have gravest implications and threats to internet freedoms of persons in Zimbabwe and; *(ii)* presents 'way-forward' advocacy recommendations to civil society, media, political movements among others that were deduced from insights gathered by this study through interviews.

[9]Zimbabwe Legal Information Institute: An Analysis of Constitution of Zimbabwe Amendment (No. 1) Bill 2016)
[10] See 1 above

3. THE CYBERCRIME BILL & ITS IMPLICATIONS ON INTERNET FREEDOMS IN ZIMBABWE

Section 3: Interpretation

For any law to be upheld, its comprehension by targeted subjects is important as this prevents punishing citizens for violating the laws they do not know or understand. To prevent this, laws must have clear and unambiguous definitions of technical and controversial terms and set parameters of law. This is a 'must do' when it comes to laws that pose direct interference with the fundamental rights of humanity as the Cybercrimes Bill does. Although section 3 of the Cybercrimes Bill gives some definitions, two main shortcomings that are injurious to internet freedoms of citizens are noticeable and should be addressed before it comes into law. These are: (i) although aiming at protecting citizens using every electronic device, it assigns a superfluous conception of the main subject of regulation 'computer device and data' in such a way that actually incorporates the most private and personal communication gargets such as smart phones as targets of state seizure and search as provided in Section 33 (1)(b)and; (ii) it has incomplete definitions that left key technical terms needed for comprehending law and avoiding criminality undefined and in the hands of law enforcement agents to define.

On superfluous definitions, section 3 of the Cybercrimes Bill reads;

> *"**computer device**" means any portable and non-portable electronic programmable device used or designed, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or critical information infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions*
>
> *"**computer data storage medium**" means any device or location from which data is capable of being reproduced or on which data is capable of being stored, by a computer device, irrespective of whether the device is physically attached to or connected with the computer device;*
>
> *"**data**" means any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data;*

In light of this conception of data and computer device, mobile phones can reproduce data and fit under the definition assigned to 'computer devices' and they are categorized by the Cybercrimes Bill as "computer data storage mediums.' As argued in MISA (2017), the 'definition needs to be amended as it considers any device that can either produce data, or be used to store data as a computer data storage medium…' and this gives room for investigating authorities to seize mobile phones, even if there is no evidence that they had been connected to any computer device of a person under investigation.

On incomplete definition of technical term, the Bill seems to insinuate that only a 'magistrate' can authorise a 'police officer' who is investigating a serious crime to interfere with third party computer devices, data and data storage systems provided there are reasonable grounds to permit this. This is not enough. There is a void of legal parameters in the meaning of "unauthorised", "unintentional" and "unlawful" required to understand criminalised acts of 'access, interception, acquisition, interference, disclosure and use' of computer devices, data and storage mediums in Section 6 to 12 of the Cybercrime Bill. The Bill should at least: *(i)* specify who (natural or juristic) is 'legally permitted' to authorise and

legalise above acts on a computer device owned by another particularly in employer-employee and family interactions and; *(ii)* state what amount and sort of proof of authorisation should one possess to prevent cases where someone decides to cause arrest of people whom he/she allowed to access or someone without authorisation to access private computer devices falsely claims authorisation. Can the state prove illegality in cases where consent is rendered through dialogue? This creates indistinctness that leaves the Bill vulnerable to: *(i)* abuse by state agents who might falsely claim access authorisation; *(ii)* abuse by citizens who might falsely deny that access was authorised if there is no set-down procedure of providing proof and; *(iii)* cause unfair arrests and prosecution of citizens for unintended violations.

Section 6: Unlawful access

Section 6 (1) of Cybercrime and Cyber-security Bill states that,

> *Any person who unlawfully and intentionally secures unauthorized access to data, a computer programme, a computer data storage medium or the whole or any part of a computer system shall be guilty of unlawful access and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or both such fine and such imprisonment.*

Three advocacy points should be emphasized regarding loopholes for and allowance of encroachment of internet freedoms inherent in this section. First, the law creates a room for justifying 'unlawfully' securing 'unauthorized' access to stated computer technologies and data on grounds of intent. Someone can be exonerated after arguing that unlawful access was not intentional even if in actual fact it was intentional. Unless there is a mechanism put in place by the government of Zimbabwe to objectively diagnose human intentions and prove them otherwise beyond reasonable doubt, internet freedom violators will always use this loophole to spy on citizens, intercept communications, interfere with data storage, hack passwords, sabotage networks and get exonerated. This is more prone in an authoritarian state like Zimbabwe where surveillance and controlling information access has been a norm for the past years.

Secondly, the law creates an impression that the government sought to legislate the practice of 'lawful' and 'intentional' securing of 'unauthorized' access to computer technologies owned and used by citizens which is a classic example of 'authorizing' spying, surveillance and interference with citizens' communications, privacy and freedoms. Although there can be good intentions of identifying cybercrime, the law does not go to greater lengths to draw the parameters to which this interference can be allowable. There is no set procedure in this Bill or anywhere to be followed as a yardstick to be satisfied to ensure justice is maintained after authorizing unauthorized access to citizens' computer data and technologies. The same applies to interception, acquisition, interference, disclosure and use of computer devices, data and data storage mediums in section 7-12.

Thirdly, the law is not clear on what constitutes a 'lawful' or 'authorized' access to computer technologies by second or third parties apart from permission granted to investigating authorities by a court or magistrate. This creates uncertainty as to what the law does not forbid. There is no clarity on who authorizes access or confers right of access to information by citizens or journalists intentionally held by state institutions. This leaves state institutions with unlimited power to deny access to computer-related information whereas government can be authorized by the court to seize and search computer devices owned by citizens and private companies. This section

also imposes limits on access to information, incites self-censorship and hinder citizens' rights to hold duty-bearers accountable using computer technologies as the law requires citizens to get a legal order and/or sanction for one to access and share information in 'computer devices' and systems.[11] Such stringent top-down conditions to access information reflect authoritarianism and should therefore be condemned in strongest terms.

This section contradicts constitutional law of Zimbabwe which requires that activities of public officials must be open to public scrutiny and therefore access to information pertaining to those bureaucrats must not be determined by the same officials who have interests in concealing it. In the same line with this, international human rights norms such as resolution 59 of the UN General Assembly adopted in 1946, as well as Article 19 of the Universal Declaration of Human Rights (1948) state that the right to freedom of expression encompasses freedom to seek, receive and impart information and ideas through any media and regardless of frontiers.[12] In Zimbabwe, section 6 of the Cybercrime Bill proves to be a frontier hence a violation of international human rights norms due to citizens online or offline.

Section 62 (1) of the Constitution of Zimbabwe provides that "every Zimbabwean citizen or permanent resident, including juristic persons and the Zimbabwean media, has the right of access to any information held by the State or by any institution or agency of government at every level, in so far as the information is required in the interests of public accountability."[13] In summary, section 6 of the Cybercrime Bill violates section 61 and 62 of the Constitution which guarantee *(i)* freedom of expression and *(ii)* access to information respectively. This law creates contentious interpretation circumstances which can be exploited by the state to intercept communications, interfere with data, block transparency, accountability and human rights monitoring by citizens and CSOs and spy on online activities of citizens.

Section 17: Transmission of false data message intending to cause harm

Section 17 of the Cybercrime Bill outlaws the transmission of false data message intending to cause harm, otherwise known as criminal defamation and previously criminalised by Section 96 of the Criminal Law (Reform and Codification) Act. It reads:

> *Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes data to any other person concerning an identified or identifiable person knowing it to be false with intend to cause psychological or economic harm 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 law presents a grotesque spectacle of a legislated exposure of ordinary citizen to politically sponsored attack on their freedom of expression, access to information and media freedoms online by governing authorities. Why is this so? It is very hard for ordinary citizens to confirm authenticity of online information about their public officials, thus using online data to inform accountability, human rights monitoring and transparency activism is prone to cause arrests of citizens on ground that they are using 'false information to cause psychological and economic harm'. In other words, this sections outlaws access to information and dissemination unless such information is: *(i)* lawfully acquired, generated as authorized and; *(ii)* tried and tested to be true. This adversely affects internet freedom and democracy in following ways: *(a)* whistle blowers relying on social media to expose human rights violations in

[11] ZDI-Media Centre Focus Group Discussion, February 2018
[12] United Nations and the Rule of Law, Freedom of Information. Available at: https://www.un.org/ruleoflaw/thematic-areas/governance/freedom-of-information/: Article 19 of the Universal Declaration of Human Rights (1948): Resolution 59 of the UN General Assembly adopted in 1946.
[13] The Constitution of Zimbabwe, 2013

remote rural areas are in danger of arrests, and ineffectiveness as mainstream media will have to spend time to prove the truthfulness of the data and legality of its accessing before capturing their reports; (b) this either exposes the source to victimization or defeats the idea of instant reporting of corruption and human rights violations as they occur and; (c) citizens are forced into self-censorship and fear to challenge human rights abuses and hold public officials to account or exonerate themselves from allegations of abuse of public office. Despite above mentioned shortcomings, if the law can protect persons against psychological and economic harm, why is it not also outlawing cases of disseminating false information with the intent of causing social and political harm?

The law therefore gives room for unconcealed violation of freedom of expression through criminalizing the posting of allegations on the internet. The arrest of United States citizen, currently working in Zimbabwe, Martha O'Donovan on Friday, 3 November 2017, should be viewed in this context. Martha was arrested in connection with a tweet which allegedly insulted the person of the President. She was charged under Section 33 (2) of the existing Criminal Law (Codification and Reform) Act [*Chapter 9:23*] which criminalizes the making of statements undermining the authority of the President. Such an arrest was the first one to be effected in connection with online statements since the establishment of cyber-security element in the Ministry of Information Communication Technology and Cyber Security.

Criminalizing free expression online is unreasonable and unconstitutional in a democratic society like Zimbabwe. The constitutional Court of Zimbabwe made it very clear that pieces of legislation that criminalize free expression and transmission of falsehoods and other forms of communication are unconstitutional.[14] The then Deputy Chief Justice Luke Malaba emphasized that "a strong Constitutional protection of freedom of expression cannot tolerate the imposition of self-censorship on free speech and the press through fear of lengthy sentences of imprisonment for offenses of publishing or communicating false news.[15] The United Nations Special Rapporteur for Freedom of Expression in a report to the United Nations Human Rights Council declared that any attempt to criminalize freedom of expression as a means of limiting or censoring that freedom must be resisted.

Like highlighted elsewhere in this paper, the constitution of Zimbabwe is very clear on freedom of expression and the freedom of the media. Section 61(1) provides that very person has the right to freedom of expression, which includes freedom to seek, receive and communicate ideas and other information, freedom of artistic expression. Nevertheless, the Cybercrime Bill provides convenient cover for government to persecute online activists and their supporters and there is a high risk that the legislation, once it becomes law, will be used to stifle online space, especially for online social movements and other dissenting voices under the pretext of protecting national interests.

Section 22: Unlawful remaining

This section of the Cybercrimes Bill stipulates that:

> *Any person who unlawfully and with intent to defraud—*
> *(a) exceeds his or her lawful authority to access a computer or information system by unlawfully remaining or attempting to remain logged in to a computer or information system or part of a computer or information system; or*
>
> *(b) continues to use a computer or information system beyond the authorized period or purpose;*

[14] See, *Chimakure, Kahiya and Zimlnd Publishers v The Attorney General* case.
[15] MISA-Zim Advocacy Paper on Access to Information and Protection of Privacy Act (AIPPA), 2014

shall be guilty of an offence and liable to a fine not exceeding level ten or imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

This section insinuates that an offence is committed only when "unlawful remaining" is intended to "defraud". However, remaining logged into a paid network after expiration of purchased data minutes is in its own a 'defrauding' commission and it follows that the intent will easily be labeled as such even if 'illegal remaining' concerned and 'defrauding' observed was unintentional.[16] For instance, an individual can be lawfully given a password to access an internet network using a mobile phone, some days later, that same individual visits the area and the phone automatically connects to the network and starts using data illegally without the owner's notice, this person would have committed a crime under this section. Under these circumstances, it cannot be proven that this kind of access was unintentional given that the mobile phone, like users, will intentionally remember the password and self-login. There is need for revision of this section to protect "unintentional" violators and those violations caused by "automatic self-service' done by computer devices such as remembering passwords without notice by the user.

Section 33: Search and seizure

The Cybercrime Bill's Section 33 (1)(a & b) clearly states that search and seizure involves "taking possession of or securing a computer" and "securing a computer system or part thereof or a computer-data storage medium". In application, seizure and search authorized by this section 33 (2) is as follows:

A magistrate may, on an application by a police officer..., order that—
(a) a person in Zimbabwe in control of the relevant computer system produce from the system specified computer data or a printout or other intelligible output of that data; or
(b) an electronic communications service provider in Zimbabwe produce information about persons who subscribe to or otherwise use the service.

(3) An application referred to in subsection (1) shall be supported by an affidavit in which the police officer shall set out the offence being investigated, the computer system in which it is suspected to be stored, the reasonable grounds upon which the belief is based, the measures that will be taken in pursuance of the investigation and the period over which those measures will the taken.

This means that the magistrate has the power to block access to computer data by police officers and protect citizens' privacy until they give reasonable grounds for suspicion. This stands if the courts systems are not compromised by political interests and are independent. If not, the ruling elite will continue to frog-match magistrates to give seizure and search warrants to police officers targeting their critics even if there are no objective grounds for suspicion. Given the history of politicization and lack of independence in the judiciary system in Zimbabwe, this means political opponents will soon have their emails, social media platforms and mobile communications interfered with through state sponsored abuse of privacy and internet freedoms.[17] Internet service providers like Econet Wireless, NetOne, TelOne, ZOL and others will be compelled to disclose the source of any content that is considered labeled as cyber-crime, while the courts will be expected to accept electronic evidence when culprits are arraigned before them.[18]This undoubtedly impacts negatively on the citizens' right to privacy enshrined under 57of the Zimbabwe Constitution because*: (i)* citizens will be subjected to State's searching of their personal possessions with or without their knowledge and consent and; *(ii)* restriction of personal autonomy. Section 57 (d) of the Zimbabwe Constitution states that that "every person has the right to privacy, which

[16] Views from a Focus Group Discussion, February 2018.

[17] View from a Focus Group Discussion: February 2018.

[18] The Herald Newspaper, 17 August 2016: Available at: https://www.herald.co.zw/cyber-crime-bill-the-details/

includes the right *not* to have the privacy of their communications infringed."[19] For instance when Pastor Evan Mawarire of #ThisFlag movement was arrested on 12 July 2016 for his mass protest on the 6th of July 2017, the police went to his home and searched the house and office in violation of the Pastor's right to privacy. Similarly, during investigations in the Martha O'Donovan case in November 2017, police investigating officers seized her mobile phone along with her laptop.

It can be stated that the Cybercrime Bill's envisioned purpose is focused more on criminalizing social media use and giving the state interference and surveillance powers. It therefore has little or no focus on the need for protecting individual liberties, or accountability in the processes of combating cybercrime. The absence of expressed intention to safeguard basic human rights raises fears that the Cybercrime Bill is solely intended to police internet use at the expense of people's freedoms.[20] The Cybercrime Bill has, in fact, an adverse impact on the human rights entitled to the citizens of Zimbabwe. For instance, it: *(i)* restrict free speech in violation of the international law;[21] *(iii)* severely threatens journalists, whistleblowers and online political activists and; *(iii)* suppresses dissent by criminalizing legitimate information sharing and networking activities.[22]

Section 36: Collection of traffic data

Section 36 of The Cybercrime Bill deals with the disclosure of information or collection of data pertaining to people suspected to have committed cybercrimes. Section 36 of The Cybercrime Bill states that:

> *"A magistrate may, on an application by a police officer in the prescribed form, that in an investigation relating to or concerning an offence listed in subsection (10) or as may be prescribed, there are reasonable grounds to believe that essential evidence cannot be collected in any other way provided for in this part but is reasonably required for the purposes of a criminal investigation, authorize the police officer to utilize remote forensic tools…*

This section authorizes police officers to utilize remote software to monitor, search, interfere and capture private and protected computer data, mobile phone data and communications of citizens suspected of committing crimes stipulated in section 10 of the Cybercrimes Bill. Although an affidavit giving details on the reasons for use of forensic tools, targeted computer, and duration must accompany the officer's application seeking authorization from a magistrate to ensure maximum protection of citizens, this is prone to abuse.[23] It is public knowledge that Zimbabwean magistrates are grossly compromised. Politicized procedures followed to be enrolled to do studies as a magistrate leave it thinkable that like police officers, they are prone to front political persecutions of opponents and critics of the ruling government.[24] In this regard, human rights activists, opposition political parties and social movements can easily find their online accounts legally hacked, shutdown or blocked by police officers in one of many politically sponsored trump investigations that have become a political culture in Zimbabwe. It should be noted that this deployment of remote forensic tools to spy, intercept and conduct surveillance of citizens' internet activities meant to apply to suspects of serious crimes stated in section 10 such as murder, treason, money laundering, deals in dangerous drugs, human trafficking, terrorism, insurgency or banditry. However, the need for use of remote forensic tools to collect private computer data must pass the reasonableness test conducted by the

[19] The Zimbabwe Constitution, section 57 (d)
[20] Media Institute for Southern Africa – Zimbabwe, MISA Zimbabwe: Commentary on Cybercrime and Cyber security Bill Issue 4, 2017
[21] Zimbabwe Independent Newspaper (13 January 2017). Available at: https://www.theindependent.co.zw/2017/01/13/cybercrimes-bill-flaws-remedies
[22] ZDI-Media Centre Focus Group Discussions, January – February 2018
[23] Focus Group Discussions, February 2018.
[24] Views of a prominent human rights activist: Focus Group Discussion, February 2018.

magistrate and it should be hoped that those magistrates are reasonable and impartial in their running of those tests or else citizens with dissenting voices will always fall victim to such state sponsored violation of internet security and privacy. There is need to carefully strike a balance between net anonymity and security issues.[25]

The presidential spokesperson George Charamba revealed that the Bill is a government trap for catching mischievous 'rats' on social media. He went further to explain that the Cybercrimes Bill:

> *... is coming against the background of the abuse that we saw not too far back on social media, where the social media then causes some kind of excitement to the country, not on the basis of fact, but generation of copy which is in fact calculated to trigger a sense of panic in the economy, and that in itself suggests that it is indeed a major threat to State security.*[26]

It was emphasised by the government of Zimbabwe that the Bill and subsequent ministry are as a result of lessons on monitoring cyberspace drawn from countries such as Russia, China and "the Koreans."[27] This was clearly a chilling admission given the fact that these three nations are notorious for stifling online rights and freedoms, with China going as far as setting up its own parallel internet network from the rest of the global internet. ICT experts have consistently expressed fears towards the Cybercrime Bill that it was established for the government to tighten its grip over the control of cyber space and spy on its citizens particularly as the nation inches closer to the 2018 elections.[28]

[25] Focus Group Discussions, February 2018.

[26] See: http://www.chronicle.co.zw/cyber-ministry-a-high-security-brief-charamba/.

[27] See, http://crm.misa.org/upload/web/Cybersecurity%20%20Analysis%20Issue%202.pdf.

[28] Views from the Focus Group Discussion, February 2018.

4. CONCLUSION & RECOMMENDATIONS

Conclusion

The Cybercrime and Cyber-security Bill evidently infringes human rights as its provisions run contrary to the constitution of Zimbabwe. For example, section 6 of the Cybercrime Bill defies section 62 the country's constitution which provides that every citizen of the country has the right of access to any information held by the State or any institution of the government. The Cybercrime Bill's elusiveness on classifying *access to information as* lawful/unlawful and authorized/unauthorized can be abused by the State to persecute political opponents and breaching constitutionally enshrined human rights. As the country nears the 2018 elections, the Cybercrimes and Cyber-security Bill will provide convenient cover for government to use in the persecution of online activists and their supporters. Particularly, such sections of the constitution as section 2 (supremacy of the constitution), section 57 (right to privacy), section 61 (right to freedom of freedom of expression) and section 62 (right of access to information) are severely threatened by the Cybercrime Bill. By and large, the Cybercrime Bill is vividly a menace to democracy and development owing to its vague provisions that allow the State to harshly punish online free expression that government deem hostile to its supreme political, economic and security interests. More so, the Cybercrime Bill compromises constitutionalism and development by criminalizing legitimate information sharing and networking activities that embrace open debate and electoral participation by the citizens. There is need to revise its key sections to align them with the constitution and international human rights standards.

Recommendations

To guarantee the enjoyment of online freedoms currently threatened by the Cybercrime and Cyber-security Bill in

Zimbabwe, this paper recommends the following to key internet freedom stakeholders:

Government

- ✓ The Cybercrime and Cyber-security Bill's purpose of criminalizing offences related to "unlawful" and "unauthorized" access to information be revised in such a way that it takes into cognizance the need to safeguard the individual rights in the process of collecting evidence or prosecuting cybercrimes. The Cybercrime Bill's purpose should therefore be widened to include protection of fundamental rights and freedoms as enshrined in the constitution.[29]
- ✓ Should come up with a clear and comprehensive definition of "unlawful", "unintentional" "unauthorized" access, acquisition, use and interference with computer devices, data and storage mediums. A clear and comprehensive definition on such a Bill's section would be to promote *democratic and human rights principles of* the constitution of Zimbabwe particularly section 62 (1) which provides that "every Zimbabwean citizen or permanent resident, including juristic persons and the Zimbabwean media, has the right of access to any information held by the State or by any institution or agency of government at every level, in so far as the information is required in the interests of public accountability."
- ✓ The statute should read in accordance with International Covenant on Civil and Political Rights (ICCPR) Article 19 (2) which 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.
- ✓ Should maintain consistency with the constitution on Bill's section 33 (1a & b) and 33 (2b) that allows seizure or securing an individual computer and compelling internet service providers to disclose the source of any content that is considered cyber-crime from persons who subscribe to or otherwise use the service. Moreover, the grounds for search and seizure should be substantiated and not based on belief only without some laid down criteria linked to court orders of statutory instruments.
- ✓ Amending section 17 to have a clear definition of 'false' messages and who defines them. In a political and socio-economic environment that prevails in any constitutional democracy, free expression by citizens may be true or false. Sharing online allegations and speculation is never a crime in a democratic country. Such a clear definition of the term, therefore, should plainly read in consistency with the supreme law of the land under section 61 (1) which provides that "every person has the right to freedom of expression, which includes (a) freedom to seek, receive and communicate ideas and other information.[30]

Civil Society

- ✓ The Zimbabwe civil society, as a crucial element of any democratic system, should effectively play their watchdog role and fight for the respect of internet freedoms by responsible authorities. They should do such through petitioning the government to prioritize the promotion of multi-stakeholder and multi-actor approaches both in action and dialogue in crafting the Cybercrime Bill.
- ✓ Civil society should embark on massive mobilization of the people through conducting road shows to demonstrate against the Cybercrime Bill's repressive provisions and lobby the government to

[29] Suggestions of a Focus Group Discussion: February 2018.

[30] Suggestions from a Focus Group Discussion, February 2018.

change those provisions and ensure their fair enforcement.

- ✓ Civic organizations should conduct community dialogue meetings to educate the citizens on their online freedoms and raise awareness of the critical aspects of the Cybercrimes Bill. This can be done through conducting political and civic communication symposiums at grassroots and national level.
- ✓ Civil Society should join hands with legislators and other key stakeholders and hold consultative meetings aimed at drafting a people centric Bill and hand it over to the parliament and Information Communications Technology Ministry and resort to litigation and challenging the government in court.

Media& Media-support Organizations

- ✓ The media as watchdog and guardian of public interest should expose the Cybercrime Bill's stringent provisions and incite demands for its urgent revision. It should carry out this through writing stories directly linked to the flaws of the Cybercrime Bill, give media coverage to internet governance stakeholders' meetings and publish them across various social media platforms to reach a large audience.[31]
- ✓ The media should contribute to public education and enlightenment on the Cybercrime Bill and initiate much-needed reforms in regard to the statute. Well informed citizens will be in a position to hold the government accountable.
- ✓ The media should serve as a conduit between the government and the citizens and as an arena for public debate that leads to more intelligent decision-making pertaining to the Cybercrime Bill.
- ✓ The media should provide voice to those marginalized or ill-informed citizens because of gender, or ethnic or religious affiliation. By giving these groups a place in the media, their views and their complaints about the Cybercrime Bill will become part of mainstream public debate and hopefully contribute to a political and social consensus on the final Cybercrimes law.
- ✓ To embark on investigative reporting on possible human rights violations by the Cybercrime Bill and other forms of wrong doing. This will help to build a culture of accountability in government and strengthening democratic principles in Zimbabwe.

Political Parties

- ✓ Political parties should put immense pressure on government, through the use of social media, to expedite the process of aligning the Cybercrime Bill's provisions with human rights provisions enshrined in the constitution.
- ✓ Embarking on massive civic education and awareness campaigns on online liberties.
- ✓ They should increase awareness of the Cybercrime Bill and its unconstitutional provisions amongst all citizens of the country from grassroots to national level using their physical and virtual communication structures and networks across the country.
- ✓ Should attend dialogue meetings organised by civic society to share strategies of influencing revisions and have a common understanding of the implications of the Cybercrimes Bill on their ability to freely conduct their political activities in Zimbabwe.[32]

[31] Suggestions from a Focus Group Discussion, February 2018.

[32] Suggestions from a Focus Group Discussion, February 2018.

BIBLIOGRAPHY

Articles & Reports

Rue, L.*Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. 2011. (Special Rapporteur's Report), Human Rights Council, A/HRC/17/27.

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: 12/02/2018].

Media Institute for Southern Africa-Zim & Digital Society of Zimbabwe. 2016. *Position paper on Proposed Draft Cybercrime and Cyber-security Bill.(Online). Available on: https://news.pindula.co.zw/wp-content/uploads/2017/01/MISA_DSZ-Position-Computer-Crimes_2016.pdf?title=news/wp-content/uploads/2017/01/MISA_DSZ-Position-Computer-Crimes_2016.pdf*. [Accessed: 09/02/2018].

Media Institute for Southern Africa – Zimbabwe. 2017. *Commentary on Cybercrime and Cyber security Bill Issue 4*. [Online]. Available at: http://zimbabwe.misa.org/2018/01/22/cybersecurity-commentary-issue-4-now-available/. [Accessed: 11/02/2018].

Media Institute for Southern Africa – Zimbabwe. 2017. *Commentary on Cybercrime and Cyber security Bill Issue 4*. [Online]. Available at: http://zimbabwe.misa.org/2018/01/22/cybersecurity-commentary-issue-4-now-available/. [Accessed: 11/02/2018].

Zimbabwe Independent Newspaper. 13 January 2017. [Online]. Available at: https://www.theindependent.co.zw/2017/01/13/cybercrimes-bill-flaws-remedies. [Accessed: 09/02/2018].

The Herald Newspaper, 17 August 2016: Available at: https://www.herald.co.zw/cyber-crime-bill-the-details/. [Accessed: 12/02/2018].

Legal Protocols

Government of Zimbabwe. 2017. *Computer Crime and Cyber Crime Bill*. [Online]. Available at:https://t792ae.c2.acecdn.net/wp-content/uploads/2017/08/CYBERCRIME-AND-CYBERSECURITY-BILL2017.pdf. [Accessed: 11/02/2018].

The Constitution of Zimbabwe. 2013. [Online]. Available at https://www.constituteproject.org/constitution/Zimbabwe_2013.pdf. [Accessed: 09/02/2018].

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

UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, September 2011, Art. 19: *Freedoms of Opinion and Expression*

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 (Cited in Joice, D. 2015).

United Nations and the Rule of Law, *Freedom of Information*. Available at: https://www.un.org/ruleoflaw/thematic-areas/governance/freedom-of-information/: Article 19 of the Universal Declaration of Human Rights (1948): Resolution 59 of the UN General Assembly adopted in 1946. [Accessed 12/02/2018].

The Constitution of Zimbabwe. 2013. [Online]. Available at https://www.constituteproject.org/constitution/Zimbabwe_2013.pdf. [Accessed: 09/02/2018].