State of Internet Freedom in Zimbabwe 2016

Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights

December 2016

OpenNet Africa

CIPESA

State of Internet Freedom in Zimbabwe | 2016
Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights

Credits

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) as part of the OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes Internet freedom in Africa.

The report presents the findings of a study on what the government in Zimbabwe is doing to inhibit citizens' access to ICT, for example content blocks, censorship, filtering, infrastructure control, law-making, court cases; using ICT activity and data to monitor citizens; and how government bodies and functionaries are using propaganda, impersonation, threats, cloning, and other tactics to shape online content in their favour. Other country reports for Burundi, Democratic Republic of Congo, Ethiopia, Kenya, Rwanda, Somalia, Tanzania, Uganda and Zambia as well as a regional State of Internet Freedom in Africa 2016 report, are also available.

CIPESA recognises Natasha (Stash) Msonza of the Digital Society of Zimbabwe as the main contributor, and acknowledges the contributions of Otto Saki, Arthur Gwagwa and Kuda Hove.

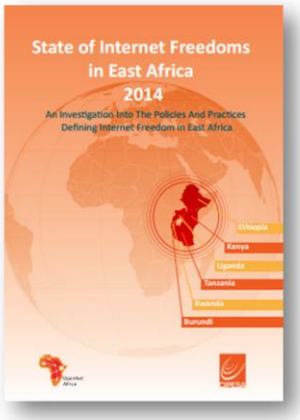
The research was conducted with support from Facebook and Google.

Editors
Ashnah Kalemera, Lillian Nalwoga, Juliet Nanfuka, Wairagala Wakabi (PhD)

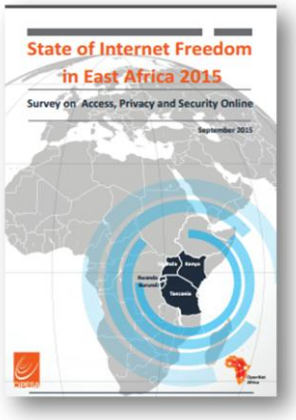
Design
Ish Designs
muwonge_issa@yahoo.com

State of Internet Freedom in Zimbabwe 2016: Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights
Published by CIPESA | www.cipesa.org
December 2016

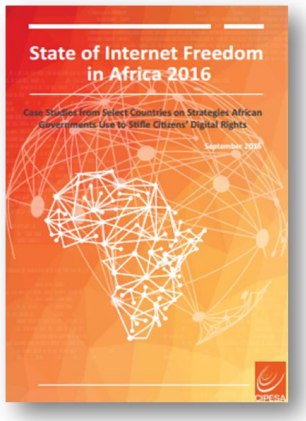
Reports in the State of Internet Freedom in Africa Series



[State of Internet Freedom in East Africa 2014]



[State of Internet Freedom in East Africa 2015]



[State of Internet Freedom in Africa 2016]

Country reports are also available on the CIPESA [Resources] page

Follow **#InternetFreedomAfrica** to see what others are saying and to share your thoughts.

Contents

1. Introduction 4
2. Research Methodology 5
3. Country Context 6
   3.1 Access 6
   3.2 Laws and Policies Affecting Internet in Zimbabwe 7
4. Findings 11
   4.1 Using and Abusing Courts of Law to Stifle Internet Freedom 11
      4.1.1 Prosecutions and Detentions Related to Online Activities 12
   4..2 Blockages of Access to Social Media and Mobile Phone Networks 14
   4.3 Website Blockages and Content Removals 16
   4.4 Pushing Government's Propaganda Online 18
   4.5 Digital Activism 19
5. Conclusion 21
6. Recommendations 22
   6.1 Government 22
   6.2 Civil Society 22
   6.3 Media 22

1. Introduction

As the use of Information and Communication Technologies (ICT) continues to grow in Zimbabwe, freedom of expression has increasingly come under attack. The government actively criminalises legitimate expression online, regularly arraigning individuals for committing often-unspecified infractions or 'abuses' online.[1] Overall, there has been what activists describe as a "disproportionate response" to national security concerns, mainly aimed at protecting political interests.[2] Exaggerated terms like "cyber-warfare", "social media terrorists" and declarations such as the one that classifies social media as a serious "national security threat"[3] have been regularly thrown around by security agents to describe digital activism and online mobilisation campaigns such as those witnessed during 2016. It is also believed that compromised regulatory agencies have compounded this problem, leading to the securitisation of the Internet in the country.[4]

Over the last decade, Zimbabwe's political and economic environment has been on a downward spiral. With a government that has presided over an economic collapse, massive formal job losses, company closures and unclear economic policies, citizens are openly critical of government oppression.[5] As the physical space for exercising freedom of expression shrinks, Zimbabweans have increasingly expressed their displeasure using avenues of expression such as the internet, the only frontier largely un-regulated by the state. Various pieces of legislation like the Public Order and Security Act (POSA) and the excesses of law enforcement agencies put stringent restrictions on public gatherings, making it hard for people to engage in traditional forms of protesting. POSA specifically has provisions that grant police the power to prevent and break up public gatherings deemed to endanger public order.

Traditional media platforms, notably television and radio, are more easily accessible and cheaper to ordinary Zimbabweans, though they are largely monopolised by the state through the Zimbabwe Broadcasting Corporation (ZBC).[6] This unrivalled access to the most powerful communication tools has often been abused for propaganda purposes. The subsequent restricted media environment in Zimbabwe therefore greatly inhibits citizens from accessing balanced, fair and independent information. To an extent, exiled and community radio stations have attempted to break this monopoly, but with limited success.[7] The Broadcasting Authority of Zimbabwe (BAZ), which is responsible for issuing broadcasting licences, has been accused of bias and issuing licences only to state-linked companies over the last decade.[8] Community radio stations are often considered a threat to the government, and in the election year of 2013, there were reports that police and youth

[1] The Herald, We had No Part in Yesterday's Whatsapp Jam, http://www.herald.co.zw/we-had-no-part-in-yesterdays-whatsapp-jam-minister

[2] Interview with Digital Security Trainer, Tawanda Mugari conducted 8th July 2016

[3] Recording of the speech of the National Army Commander General Constantino Chiwenga on radio at the occasion of the 36th Zimbabwe Defence Forces Day commemorations.

[4] Interview with Arthur Gwagwa, Strathmore University, conducted 1th July 2016

[5] See these reports: http://www.refworld.org/pdfid/54b691994.pdf and http://ccs.ukzn.ac.za/files/Bond%20ManyanyaZimbabwesPlunge2ndEdn.pdf

[6] There are at least seven radio stations in Zimbabwe, which are either state owned or privately owned by individuals closely linked to the ruling party. Because getting a radio license is next to impossible for ordinary individuals, some innovative Zimbabweans abroad are using web-based services to broadcast, like Nehanda Radio and Radio Kunakirwa among others.

[7] With the rise of satellite ownership, few radio stations have thrived, but rely heavily on unsustainable donor funding.

[8] BAZ Accused of Bias, Monopoly, Tribalism, https://www.newsday.co.zw/2016/08/04/baz-accused-bias-monopoly-tribalism

militia allied with the ruling party confiscated radio receivers that were "being used to peddle hate speech" in rural and peri-urban communities.[9]

The prospect of regulation and repression of Internet rights is expected, especially as the country heads towards the 2018 polls. Ordinary Zimbabweans are used to living in a context where their right to access information is repressed.[10] This is the same for the rights to freedom of expression,[11] privacy and related rights. Human rights defenders (HRDs), including political activists, have particularly been the main targets. Creeping authoritarianism is evident in just about every facet of social and political life in Zimbabwe. Independent media are stifled, journalists intimidated and arrested, and opposition parties and civil society groups harassed and subjected to a variety of suffocating regulations. Since independence, the successive governments led by President Robert Mugabe have wielded monopoly over the state media. Independent media have been under constant assault, and in certain circumstances been shut down.[12]

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

2. Research Methodology

The research presented in this report was conducted through a mixed methods approach. Researchers based in Zimbabwe interviewed key informants who were purposively selected. The informants were chosen on the basis of their knowledge about issues related to or affecting internet freedom in the country. They included activists and human rights defenders that are advancing free expression and association in these countries, as well as some of those who had been victims of abuses and violations. Others were internet and telecom service providers, regulators, law enforcement officials, and journalists. In total, nine key informants were interviewed for this report.

Policy analysis was conducted to generate an understanding of the existing and proposed laws that affect digital rights. The analysis took an interest both in policies and laws that have been used to curtail internet freedom and those that could potentially be employed in curtailing freedom of expression and access to digital technologies. Analysis was done of relevant Bills currently under consideration by parliament. Moreover, document review was done, including of open access sources such as media articles and secondary research reports, as well as analysis of records such as court orders and regulatory decisions, some of which are not readily available in the public domain.

[9] Police Can Confiscate Radio Sets that Spew Hate Speech: Minister, http://www.herald.co.zw/police-can-confiscate-radio-sets-that-spew-hate-speech-minister

[10] For example, the voters' roll issue, where access for public scrutiny has been denied for years.

[11] Zimbabwe Human Rights, Rule of Law and Democracy 2013 Annual Report, http://www.hrforumzim.org/publications/annual-reports/zimbabwe-human-rights-rule-of-law-and-democracy-2013-annual-report/

[12] For instance the Daily News in 2003, for failure to register in terms of the draconian AIPPA

3. Country Context

3.1 Access

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) is the entity responsible for regulating telecommunications in Zimbabwe. Established in 2000, the political independence of POTRAZ is questionable, as it falls under the president's office, who in consultation with the Minister of Transport and Communication, appoints its leaders.[13] There are more than 20 Internet Service Providers (ISPs) in Zimbabwe. Three major operators currently provide telecom services: privately owned *Econet Wireless,* state-owned NetOne and Telecel in which the government is reportedly the majority shareholder.[14] In the third quarter of 2016, the mobile penetration rate in Zimbabwe reached 97% while Internet penetration stood at 50%.[15]

Fibre optic internet is now generally widely available, after Liquid Telecom laid out fiber-optic cables in most cities and major towns. The state-owned ISP, TelOne, has on-going ambitious 'Fibre to the Home' (FTTH) project aimed at bringing internet connectivity to 100,000 homes by 2020, and by July 2016 had reportedly covered about 15,000 homes and also introduced 10 WiFi hotspots around the capital city.[16] Meanwhile, POTRAZ manages the Universal Service Fund (USF), which through a 2% levy on operators' revenue has since 2001 facilitated infrastructure roll out to extend communications services to underserved communities.[17] However, POTRAZ has been criticised for under-utilising the fund[18] and lack of transparency about its expenditures.[19]

Access to the Internet in Zimbabwe remains fairly expensive. For example, the Internet provider Zimbabwe Online (ZOL) offers 15GB capped data for USD $29 per month, with speeds of up to 5 Mbps. This is among the cheapest available data packages in the country, but is beyond what most Zimbabweans can afford. As part of mobile internet data bundles, Zimbabwean Mobile Network Operators sell packages with subsidised or "zero rated" access to social media applications such as WhatsApp and Facebook. However, in August 2016, these promotional bundles were suspended through a directive from the telecoms regulator, POTRAZ, without any official statement or explanation.[20] The directive was issued shortly after veiled threats, policy pronouncements and directives from regulatory authorities in the face of what they described as increasing 'abuse' of social media. Some critics theorise this as a desperate move by government to stifle online mobilisation and social media uproar by making internet inaccessible to the masses. One blogger identifying as *Digital Avatar* wrote on the *TechZim* website that the "government is literally,

[13] MISA (Zimbabwe) position on the independence of broadcasting and telecommunications regulatory bodies, http://archive.kubatana.net/docs/media/misaz_need_for_independent_regulatory_body_0711.pdf
[14] Government Takes Over Telecel, http://www.theindependent.co.zw/2015/11/13/govt-takes-over-telecel
[15] POTRAZ, Postal and Telecommunications Sector Performance Report Second Quarter 2016, https://www.potraz.gov.zw/images/documents/QReports2016/thirdquarterreport.pdf
[16] TelOne Targets 100,000 Homes, http://www.bh24.co.zw/telone-targets-100-000-homes
[17] Overview of USF, http://www.potraz.gov.zw/index.php/usf
[18] Zimbabwe: POTRAZ has over US$20 million in unused Universal Service funds, http://www.balancingact-africa.com/news/telecoms_en/19492/zimbabwe-potraz-has-over-us20-million-in-unused-universal-service-funds and also Utilise Service Fund, Potraz Told, http://allafrica.com/stories/201012020009.html
[19] GSMA, Sub-Saharan Africa Universal Service Fund Study 2014, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/Sub-Saharan_Africa_USF-Full_Report-English.pdf
[20] Telecel Forces by Regulator to Stop Mega Bonus and Other Promotions, http://www.techzim.co.zw/2016/08/breaking-news-telecel-forced-regulator-stop-mega-bonus-promotions/#.V6yk25N946g

deliberately or accidentally, suffocating the digital revolution by cutting off the lifeblood of the revolution, which is affordable digital and social media access to give citizens an alternative voice."[21]

There is no readily available data on how many Zimbabweans use social media sites such as Facebook, Twitter and Whatsapp. However, there is an active presence of Zimbabweans on these platforms.[22] This was demonstrated, for instance, through information proliferation about the #ShutDownZimbabwe2016 stay-away which spread to the masses through Twitter and WhatsApp.[23]

3.2 Laws and Policies Affecting Internet in Zimbabwe

Section 61 of the Zimbabwe Constitution guarantees the right to freedom of expression. [24] It states that: "Every person has the right to freedom of expression, which includes - **a**. freedom to seek, receive and communicate ideas and other information." Zimbabwe currently has no specific law or policy related to internet rights or access, although the constitution provides for these rights without mentioning the online domain. However, there are several bills under consideration by parliament, including the Data Protection Bill; the Electronic Transaction and Electronic Commerce Bill; and the Computer Crime and Cybercrime Bill. [25] [26] The Law Development Commission (LDC), with support and partnership from a local legal advisory civil society group, in 2016 started undertaking consultations on these proposed laws. The Ministry of ICT is also said to be gathering stakeholder views on the proposed laws.[27] Various 'leaked' versions of the Bills are available online, making it difficult to ascertain the actual official versions, until such a time when one is officially presented in Parliament and Gazetted.

However, of the Bills that may directly impact freedom of expression, there is a version of the Computer Crime and Cybercrime Bill (2014), which if passed in its current state, would allow authorities to remotely install surveillance, spying and forensic tools onto the devices of individuals of interest. [28] Such actions would be authorised by a magistrate if satisfied, based on an application by a police officer, that there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in the Bill, but is reasonably required for the purposes of a criminal investigation.[29]

---

[21] Hiking the price of free speech. The real reasons behind government's suspension of telecoms promos: http://www.techzim.co.zw/2016/08/hiking-the-price-of-speech/#.V6wU4pN946i

[22] Veger, M.(2015).Perceptions of the risk of state harassments and state surveillance in Zimbabwe. Master Thesis. Utrecht University.

[23] Movement led by Pastor Evan Mawarire, largely organised through Twitter, Facebook and Whatsapp calling on citizens to stay-away from work in protest against government's poor management of the economy.

[24] Constitution of Zimbabwe, 2013 http://www.parlzim.gov.zw/component/k2/download/1290_da9279a81557040d47c3a2c27012f6e1

[25] Govt drafts laws to fight cyber crime, bullying, http://source.co.zw/2015/04/govt-drafts-laws-to-fight-cyber-crime/. Also see http://www.theindependent.co.zw/2015/07/24/authorities-move-to-control-cyberspace/

[26] Authorities Move to Control Cyberspace, http://www.theindependent.co.zw/2015/07/24/authorities-move-to-control-cyberspace

[27] Sharon Muguwu, Cybercrime Bill Under Scrutiny, https://www.dailynews.co.zw/articles/2016/09/19/cybercrime-bill-under-scrutiny

[28] Zimbabwe's Draft Computer Crime and Cybercrime Bill Layman's Draft, 2013, http://www.techzim.co.zw/wp-content/uploads/2016/08/Zimbabwes-Draft-Computer-Crime-and-Cybercrime-Bill-Laymans-Draft-July-2013.pdf

[29] Arthur Gwagwa, Implications of Zimbabwe's proposed cybercrime bill. http://bit.ly/1QDJ9QH

Clause 5 of the Bill as of September 2016, called for punishment of unlawful access of a person's electronic communications.[30] It reads: "Any person, who unlawfully and intentionally generates, possesses and distributes an electronic communication with the intent to coerce, intimidate, harass, threaten, bully or cause emotional distress, degrade, humiliate or demean the person of another person, using a computer system or information system shall be guilty of an offence and liable, on conviction, to a fine not exceeding level 10 or imprisonment not exceeding five years or both." This clause could be used to curtail online media activities.

The Bill raises a number of concerns. For instance, although it contains limitations on the powers to hack, it still introduces incredibly intrusive powers and provides for its use in a wide array of circumstances. There is no requirement for the court to oversee closely the implementation of the authorisation, neither are there any restrictions on the repeated renewal of the authorisations. The Bill stipulates in Section 36 (3) that the duration of authorisation in section 35(1) shall be limited to three months. Where the conditions of the authorisation are no longer met, the action taken shall be stopped immediately. However, there is no mention of mechanisms to enforce this.

Furthermore, the Bill instils in the police incredibly broad authority and responsibility that is highly prone to misuse and abuse, thus likely to make oversight and accountability very difficult. Specifically, the Bill provides in section 36 (1) that: "If a magistrate is satisfied on the basis of an application by a police officer, supported by affidavit that in an investigation concerning an offence listed in paragraph 7 herein-below or regulations made under Section 45 there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in this part but is reasonably required for the purposes of a criminal investigation, the magistrate may authorise a police officer to utilise a remote forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence."

In the absence of a cyber law, the Criminal Law and Codification Act (CODE), popularly known as the 'insult law' has been the government's weapon of choice against critics both online and offline.[31] The law was widely used during the protests in 2016 to invoke harassment and arrest of 'trouble-makers', namely those who oppose or criticise President Mugabe.[32] Indeed, in justifying the need to regulate social media, the government invokes the arguments of national security and the need to protect women and children online from cyber-bullying, paedophiles and revenge porn.[33] While these are valid grounds for social media regulation, there are also reasonable grounds for anticipating that dissenting activists will be targeted with a clampdown on internet freedoms.

The Access to Information and Protection of Privacy Act (AIPPA) of 2002 has notoriously been used to shut down several media houses on account of failure to register with the Media Information Commission (MIC). The Act purports to achieve compulsory registration of journalists but with the proliferation of the internet, the ability to register everyone including individuals identifying as 'citizen journalists' is near impossible if not futile. The Act has weak provisions for safeguarding of personal information. The Act provides for a "Personal information bank" which is a collection of personal information that is organised or retrievable by the name of an individual or by an

[30] Computer Crime and Cybercrime Bill, 2016, http://www.techzim.co.zw/wp-content/uploads/2016/09/Zimbabwes-draft-Computer-Crime-and-Cybercrime-Bill-16-September-2016-version.pdf

[31] Section 33 of CODE, which makes it a criminal offence to intentionally make public statements that undermine or insult the President in person or in his official capacity.

[32] Interview with TZ, Political Analysts conducted 22 June 2016.

identifying number, symbol or other particulars assigned to an individual and includes personal images. The bank has not yet been set up.

The Interception of Communications Act (ICA) of 2007 sets out the legal basis for authorities to conduct communications surveillance. The Act "provides for the lawful interception and monitoring of certain communications in the course of their transmission through a telecommunications, postal or any other related service system."[34] Section 2(2) of the Act defines "interception" as "to listen to, record, or copy, whether in whole or in part" communications sent through telecommunications or radio systems and "to read or copy the contents" of communications sent by post. The Act criminalises interception without a warrant or the consent of at least one of the parties to the communication, an offence punishable by a fine, or imprisonment of up to five years.

There is very little publicly available information about how the Act is applied and interpreted by the authorities. A number of aspects are of particular concern. For instance, the Act authorises four senior officials (or their nominees), representing police, intelligence, national security, and tax interests, to individually make applications for warrants of interception. Those authorised include the Chief of Defence Intelligence, Director General of National Security, Commissioner of the Zimbabwe Republic Police, and the Commissioner General of the Zimbabwe Revenue Authority can apply to the Minister in charge of communication. Authorities may obtain warrants to intercept private communications through a process that is controlled by members of the Executive and not subject to independent judicial scrutiny or public oversight. Further, the supervision of this Act falls within Office of the President and Cabinet.[35] It also fails to prescribe a test of necessity and proportionality, [36] but instead grants wide discretion to the minister.[37] Additionally, Section 11 of the Act provides that the Minister may issue a warrant where there are 'reasonable grounds' for the Minister to believe that it is necessary to gather information "concerning an actual threat to national security or any compelling national economic interest" or "concerning a potential threat to public safety or national security." Such a wide provision, without a proper detailed guideline, can be subject to abuse.

There is no provision for independent and impartial judicial scrutiny. The only oversight of the warrant regime comes from the Prosecutor-General, who is required to receive an annual summary from the Minister detailing, "the particulars of every warrant which, during that calendar year, was issued by him or her but not renewed." This information is not made public in any form, therefore does not meet the test of transparency, which is especially a challenge given that there is no mechanism for independent oversight.[38] There is also no requirement for this information to be made public. Moreover, while the Act allows a person or group to appeal a decision to the Administrative Court once they have been 'notified' or somehow 'become aware' of a warrant, there are insufficient avenues for targets of unlawful surveillance to seek redress.

There is broad, vague and sometimes obscure language used in the Act, i.e. 'monitoring' and 'intercept' which are not well distinguished, allowing for permissive interpretations that potentially create confusing overlaps in their application, therefore making it difficult to distinguish between

[34]Interception of Communications Act, long title. Accessed here: http://archive.kubatana.net/html/archive/legisl/070803ica.asp?sector=legisl

[35] Statutory Instrument 19/2014

[36] International Principles on the Application of Human Rights to Communications Surveillance; Necessary and Proportionate Principles.

[37] The Minister for Presidential Affairs in the President's Office, who is tasked with administration of the Act. Statutory Instrument 162/2012 assigned administration of the Act to the Office of the President and Cabinet headed by this Minister.

[38] Interception of Communications Act section 6(1)(a), (b), (c)

'monitoring' and 'intercepting'. Monitoring sounds less intrusive than interceptions, hence if there is no clarity, the two will then be used interchangeably.[39]

Government authorities have used the 2007 Act on interceptions to restrict access to encrypted services that allow people to communicate anonymously and privately. Although the Act does not specifically and wholly ban the use of encryption technology, POTRAZ tends to interpret the broadly worded language in the Act as some form of authorisation for the agency to ban encrypted services. Bans on the use of encryption technology violate the right to privacy and the right to freedom of expression. As the Special Rapporteur on Freedom of Expression noted in 2015, "encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attack."[40]

The ICA requires telecom service providers to have "the capability of interception"[41] and ensure that their services are "capable of rendering real time and full time monitoring facilities for the interception of communications."[42] This provision opens doors for ISPs to collect and store large amounts of data and meta-data, a thing that contravenes international human rights standards, but is locally considered strictly necessary to respond to legitimate law enforcement needs.[43] Failure by the service provider to comply with the provisions of ICA constitutes an offence punishable with a fine not exceeding USD 2,000 or imprisonment not exceeding three years or both. At the time of passing of the Act, the Zimbabwe Internet Service Providers Association (ZISPA) attempted to object to these provisions due to concerns over the cost of procuring the requisite equipment for surveillance as well as intrusion into customer privacy.[44] However, there is no evidence to-date whether individual ISPs have refused to cooperate with any of the provisions. After the passing of ICA in Parliament, ZISPA chairperson and *TeleContract*[45] Group Executive, Shadreck Nkala, reportedly stated that measures were being "put in place to comply."[46]

The **Postal and Telecommunications Regulations Statutory Instrument 95 of 2014 (Subscriber Registration)** requires all telecommunications companies to create a centralised subscriber database of all their users.[47] The database is supposed to be accessible to the government and stay regularly updated with new user information. The regulations further provide that the centralised database would be managed by POTRAZ, who would use it among other things, to assist law enforcement agencies for safeguarding national security (upon production of a court order or warrant, and as long as the request complies with the constitution[48]) as well as authorising access for the purposes of research in the sector. The Regulations stipulate the penalty of imprisonment of up to six months for

[39] Interview with Otto Saki, Zimbabwean Lawyer, conducted on 12 June 2016.
[40] Report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 2015, Para 16.
[41] Interception of Communications Act section 12(1)(a)
[42] Interception of Communications Act section 9(1) (c)
[43] The right to privacy in the digital age, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, A/HRC/27/37, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; see also Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.
[44] VOA, Zimbabwe Internet Service Providers Comply With Snooping Law, http://www.voazimbabwe.com/a/a-13-56-74-2007-08-30-voa63-69000422/1464872.html
[45] TeleContract owns Telconet, an Internet service provider.
[46] Interview with Shadreck Nkala, ZISPA chairman and group executive for Telecontract, 23 July 2008 as published in Public Broadcasting Africa Series: Zimbabwe, available at http://archive.kubatana.net/docs/media/osn_public_broadcasting_zimbabwe_091124.pdf
[47] Replaced Statutory Instrument 142 of 2013 "Postal and Telecommunications (Subscriber Registration) Regulations, 2013"
[48] Section 9 (1) – (3)

failure to register a SIM card or providing incorrect information. Although the 2014 regulations introduced the requirement that a warrant or court order is required for POTRAZ to release information to law enforcement agents, the warrant regime contains a concerning loophole.[49] While a judge or magistrate may issue a court order, police officers designated as justices of the peace, can also issue warrants.

Compulsory SIM card registration and retention of data about mobile phone users in a centralised database threatens the right to privacy in Zimbabwe, especially in the absence of data protection legislation. In measures meant to improve access and connectivity through inter-connections and inter-operability, government proposed laws on infrastructure sharing, backbone nationalisation and the establishment of a National Data Centre in the draft National ICT Policy. [50] The policy stipulates the establishment of the National Data Centre as a "critical common infrastructure" to support both public and high security services and information.[51] The implementation of such a system may result in the potential monitoring of all local Internet traffic. Without adequate technical and legislative safeguards, this poses a threat to the privacy and security of data, whether in transit, at rest or in storage.[52] There is also concern that one entity will end up controlling all Internet gateways and infrastructure, making it technically easier to monitor, filter, or even block internet traffic. With the mandatory registration of all internet access points and telephone accounts, mass surveillance and interception will become an easily achievable task.[53]

4. Findings

4.1 Using and Abusing Courts of Law to Stifle Internet Freedom

Sections 31 and 33 of the **Criminal Law Codification and Reform Act (CODE)** of 2004 criminalises "publishing or communicating false statements prejudicial to the state" and "undermining authority of or insulting [the] President." The police have charged several individuals under these provisions for statements made publicly or privately. For example, in 2013, a professor at Great Zimbabwe University was sentenced to three month's imprisonment for calling the President a "dirty old rotten donkey"[54] in a supermarket under Section 33.

In what was seen as a move to censor as well as silence dissenting voices online, head of the Zimbabwe Media Centre, Ernest Mudzengi, and blogger Mlondozi Ndlovu were in April 2016 interrogated for over eight hours over a story published on the Zimbabwe Sentinel website.[55] The story had been deemed too critical of the president, and therefore the two were charged under Section 33 of this law. This was widely seen by critics as a move meant to intimidate the journalists. The main strategy was to harass media practitioners under the pretext of investigating a story yet achieving the chilling effect on journalists intending to pursue sensitive stories.[56]

[49] Postal and Telecommunications (Subscriber registration) Regulations, 2014, Section 9(2)
[50] Section 21.3 of the ICT policy; 21.3 The National Backbone Company
[51] Section 21.5 of the ICT policy
[52] Digital Society of Zimbabwe statement made in a presentation at the MISA-Zimbabwe multi-stakeholder cyber-indaba on Online Ethics and Privacy in December 2015: http://www.techzim.co.zw/2015/12/takeaways-zimbabwes-cyber-indaba/#.V6pxqY6zDaY
[53] Interview with IT Expert, Christopher Musodza conducted on 1 August 2016
[54] Zim lecturer jailed for labelling Mugabe 'rotten old donkey', http://mg.co.za/article/2013-05-18-zim-lecturer-jailed-to-labelling-mugabe-rotten-old-donkey
[55] http://www.zimsentinel.com
[56] Interview with MISA-Zimbabwe official, 12 June 2016

Sections of civil society have been challenging the legality of some parts of this law and some legal critics have declared Section 33 in particular to be unconstitutional,[57] a "serious hazard to democracy"[58], out-dated and too vague in a way that any critic of the president knows only after the fact, that their statement was actually deemed offensive.

In February 2016, the Constitutional Court outlawed and struck down Section 96 of CODE on 'criminal defamation'. This section had long been used to criminalise freedom of expression and terrorise media practitioners in their journalistic enterprise. MISA-Zimbabwe had made an application challenging the legality of the section and seeking confirmation that criminal defamation was no longer part of the law. This followed the judgment in the case of *Madanhire and Others* in 2013, in which the court ruled that Section 96 of the CODE was inconsistent with the provisions of Sections 61 and 62 of the constitution, which protect the right to freedom of expression, and was therefore void. [59] Specifically, the courts said that Section 96 of CODE was void *ab initio* (from the beginning), and recognised that it was not only unnecessary to criminalise defamatory statements, but "There can be no doubt that the freedom of expression, coupled with the corollary right to receive and impart information, is a core value of any democratic society deserving the utmost legal protection." [60]

In September 2011, POTRAZ banned Blackberry Messenger– then an encrypted messaging service provided on Blackberry phones. Their argument was that under the Interception of communications Act, telecommunications services should have hardware and software with the ability to carry out surveillance for the government.[61] As of July 2016, the ban on Blackberry Messenger remained in place.[62]

4.1.1 Prosecutions and Detentions Related to Online Activities

Since 2015, over 120 people have been arrested for posts made on social media sites such as Facebook and Twitter, according to the Zimbabwe Lawyers for Human Rights (ZLHR).[63] The majority of arrests are of ordinary citizens under spurious charges, especially under insult laws in the CODE. In the majority of cases, the courts have ruled in favour of protecting privacy rights, but have also cited some cases as being in breach of freedom of expression online.[64]

Below are some of the cases of Zimbabweans arraigned before the courts over their online activities:

***State vs. Kudzayi* (Baba Jukwa Case)**
In June 2014, Edmund Kudzayi and his brother Philip Kudzayi were arrested and slapped with sedition charges under the Criminal Law and Codification Reform Act (CODE) for allegedly being

[57] Legal expert and blogger Alex Magaisa makes a very detailed critique of the unconstitutionality of Section 33 of CODE here: http://alexmagaisa.com/2016/07/31/why-zimbabwes-presidential-insult-law-is-unconstitutional-a-critical-analysis-of-section-33-of-the-criminal-code
[58] Alex Magaisa, Why Zimbabwe's Presidential Insult Law is Unconstitutional: A critical Analysis of Section 33 of the Criminal Code, accessed on 31 July 2016 here: http://alexmagaisa.com/2016/07/31/why-zimbabwes-presidential-insult-law-is-unconstitutional-a-critical-analysis-of-section-33-of-the-criminal-code
[59] Madanhire and Another v Attorney General, CCZ 2/2015
[60] http://www.southernafricalitigationcentre.org/1/wp-content/uploads/2016/09/Chapter-2.pdf
[61] Challenges in promoting privacy and freedom of expression in Zimbabwe, http://nehandaradio.com/2013/06/11/challenges-in-promoting-privacy-and-freedom-of-expression-in-zimbabwe/.
[62] Alfonce Mbizwo, Zim BlackBerry services still banned, http://www.biztechafrica.com/article/blackberry-services-remain-banned-zim/1213/#.V6nlao6zDaY
[63] Interview with ZLHR lawyer TM conducted on 11 June 2016
[64] Interview with legal practitioner Otto Saki, conducted on 12 June 2016.

behind the pseudonymous Facebook character "Baba Jukwa." They were accused of urging citizens to overthrow the government. In his defense, one of the accused indicated that he was working with several government officials who were aware of his activities, including Ministers of Defence, and Information and Youth and Empowerment. The duo was arrested following indications that a SIM card registered in their names had been used to log into and register the Baba Jukwa Facebook account, using a fake Gmail address. Two weeks after their arrest, all charges were withdrawn. Posts on the *Baba Jukwa* page continued while the suspects were in prison.[65]

State vs. Mavhudzi

Vikas Mavhudzi was arrested in March 2011 following posts that he allegedly made on Facebook, using his mobile phone.[66] The police who arrested him apparently acted on the tip-off from an anonymous informant. The problematic Facebook message had been directed at then Zimbabwean Prime Minister Morgan Tsvangirai and stated: "*I am overwhelmed (don't) know what to say Mr. PM (Prime Minister), what happened in Egypt is sending shockwaves to all dictators around the world. No weapon but unity of purpose, worth emulating hey."* Mavhudzi was charged with subverting a constitutionally elected government under Section 22 (2) of the CODE. The court dismissed the case, stipulating that no permissible evidence was available to prove that a crime had been committed.

State vs. Machingauta

On June 15, 2015, Benjamin Machingauta, was charged with sending insulting, offensive and annoying messages as defined in Section 88 (c) of the Postal and Telecommunications Act, to Member of Parliament Joseph Chinotimba in a Whatsapp group chat called Com Fighter.[67] He was convicted on his own guilty plea and handed a US$100 fine or one month in prison. He paid the fine. His arrest reportedly followed assistance from the mobile service provider ECONET in providing the user's details to the police during the investigations.

State vs. Matshazi

An opposition party Councillor, Nduna Matshazi, was arrested in October 2015 for offending the president in a message he posted in a WhatsApp group whose administrator reported him to the police.[68] The message was a parody of the Lord's Prayer in the Bible, which according to the administrator of the WhatsApp group was "twisted to demean and attack the President."[69] Nduna was suspended from his position, and he subsequently appeared in court on charges of sending an offensive message about President Mugabe.[70]

State vs. Matsapa

In April 2016, an agriculture ministry staffer from Nyanga district, Ernest Matsapa, was charged with "criminal nuisance" after "unlawfully and intentionally" sending an audio-visual message to a

[65] Baba Jukwa mystery arrest fails silent phantom character, http://www.southerneye.co.zw/2014/06/23/baba-jukwa-mystery-arrest-fails-silence-phantom-character

[66] Zimbabwe makes arrest over Facebook comment, http://www.zdnet.com/article/zimbabwe-makes-arrest-over-facebook-comment

[67] Paidamoyo Muzulu, Man fined for insulting Chinotimba on WhatsApp, News Day, June 25, 2015, https://www.newsday.co.zw/2015/06/25/man-fined-for-insulting-chinotimba-on-whatsapp/

[68] Whatsapp slur against Mugabe gets Zim man arrested, http://www.news24.com/Africa/Zimbabwe/WhatsApp-slur-against-Mugabe-gets-Zim-man-arrested-report-20151004

[69] MDC official nabbed for Whatsapp President slur, http://www.chronicle.co.zw/mdc-t-official-nabbed-for-whatsapp-president-slur/

[70] Silas Nkala, MDC-T councillor up for Mugabe insult, https://www.newsday.co.zw/2016/07/26/mdc-t-councillor-mugabe-insult/

WhatsApp group.[71] The clip is said to have depicted an incapacitated Mugabe as having become a burden on citizens, including his family.[72] Matsapa was charged under Section 46 (2) (v) of the Criminal Law (Codification and Reform) Act but was later released on bail.[73]

State vs. Chuwe and two others

In March 2016, when school teacher Edson Chuwe, Edna Garwe, and Lenman Panyiwa, were arrested for posting pictures and messages mocking President Mugabe on Facebook and Whatsapp, thereby 'insulting and undermining the president's authority'. [74] The messages read: "Mr. President, isn't it time to bid farewell to the people of Zimbabwe?" The trio was charged for insulting the president and contravening Section 33 (2) of the Criminal Law and Codification Reform Act. They were each granted USD 50 bail.[75] The case is yet to be concluded in court.

State vs. Evan Mawarire

After successfully starting a cyber movement calling for Zimbabweans to stay away from work on July 6, 2016 to protest against corruption, poor governance and state of the economy, Pastor Evan Mawarire was arrested the day before the second stay away that was scheduled to take place on July 13 and 14. His arrest on what appeared to be trumped up charges of "inciting violence and disturbing the peace" was part of the government's attempts to dissuade Zimbabweans from taking part in the stay away.[76] During court proceedings, state prosecutors attempted to change the charges against Mawarire to a more serious one of subversion. After over eight hours in court, the charges against Mawarire were dropped after the Magistrate's Court found that his arrest had been unconstitutional.

State vs. Mahiya

On July 2016, Douglas Mahiya, spokesperson of the Zimbabwe National War Veterans Association, was arrested following issuance of a "treasonous" communiqué[77] criticising Mugabe's leadership. [78] Among other things, the communiqué described the President as a 'genocidal dictator' whom the association would no longer support in elections. Mahiya was charged under the CODE law for insulting and undermining the president. The actual author of the communiqué in question is still unknown, as the document shared with the media was not signed. The case was still pending at the time of writing this report.

4.2 Blockages of Access to Social Media and Mobile Phone Networks

In controlling online information, government has blocked access to communication channels and social media sites, issued directives to remove certain content deemed to be critical of its actions and of the president. In the past, the state has generally been suspected of interfering with mobile

[71] Zimbabwe Arrests Soar Mugabe Regime Cracks Down Social Media, http://www.ibtimes.co.uk/zimbabwe-arrests-soar-mugabe-regime-cracks-down-social-media-1553230
[72] Ibid
[73] Govt staffer says Bob a burden, arrested, http://www.thezimbabwean.co/2016/04/govt-staffer-says-bob-a-burden-arrested/
[74] School head charged for doctored Mugabe images, http://www.radiovop.com/index.php/national-news/13335-school-head-staffers-charged-for-doctored-mugabe-images.html
[75] ZLHR, Human Rights Defenders Alert, 02 March 2016, http://www.newzimbabwe.com/news-28024 Sch+head+Photoshops+Mugabe,+arrested/news.aspx,
[76] 'ThisFlag' opposition leader, Pastor Evan Mawarire, arrested in Zimbabwe, http://www.dw.com/en/thisflag-opposition-leader-pastor-evan-mawarire-arrested-in-zimbabwe/a-19396073
[77] War Vet Mahiya Arrested, The Herald, July 28, 2016, http://www.herald.co.zw/war-vet-mahiya-arrested
[78] Full text of communiqué accessed on 10 August 2016 here: http://nehandaradio.com/2016/07/21/full-text-war-veterans-statement-dumping-mugabe

telephone networks in periods of significant political activity. For instance, during the 2013 presidential elections and the 2016 'Million Man March[79], mobile networks "seemed to be a little jammed and mobile money transfers noticeably slower than usual."[80] Some critics allege that throttling the internet is something that the government has always done, but because there was no deliberate monitoring, these incidents went unnoticed.[81]

Prior to the 2013 elections, in an unconstitutional move, the telecoms regulator POTRAZ issued a directive to telecoms companies to block the delivery of bulk SMS from international gateways until after the July 31 polls.[82] Non-profit organisations such as Kubatana were using bulk messages as a way of disseminating critical voter information to ordinary Zimbabweans.[83] Zimbabwe currently has no regulations regarding the distribution of bulk SMS in relation to dissemination of political information. However, the proposed cyber crime bill contains clauses pertaining to 'spam' that may in the future be used to regulate bulk SMS services.

In April 2016, upon his return from a recent official visit to Japan, President Robert Mugabe made a public pronouncement that he would introduce "Chinese-style" internet restrictions on social media, ostensibly "to control 'abuse' of the digital platforms and cyberspace."[84] The communications regulator also issued public threats that those who "misused" social media would be nabbed. Many Zimbabweans on Twitter took this to mean a possible ban of social media. The government is generally not trusted to fairly regulate the platforms it considers offensive or threatening, hence any regulation would be perceived as tantamount to a ban. This is why it was easy for the citizenry to believe that there was a shutdown of some parts of the internet, especially of WhatsApp, on the day of the first #ShutDownZimbabwe2016 in July 2016.[85]

This was especially believable because a previous protest in the peri-urban areas of Epworth and Ruwa had been allegedly initiated and mobilised through social media[86]. (Read more about the #ShoutDownZimbabwe2016 in the digital activism section). Interruptions to internet access during the #ShutDownZimbabwe2016 lasted approximately four hours, with telcos and ISPs issuing apologies for the 'disruption' without giving an explanation. Nevertheless, ICT Minister Supa Mandiwanzira issued a public statement[87] distancing his ministry and the government from the

[79] An initiative organised by the ruling party Zanu PF's youth league early this year on 25th May 2016, as a way to 'celebrate the visionary and iconic leadership of President Mugabe': http://www.herald.co.zw/live-one-million-man-march-25-may-2016-in-solidarity-with-the-iconic-leadership-of-president-mugabe

[80] Interview with political analyst, TZ held 22 June 2016.

[81] Interview with IT Expert, Chris Musodza conducted on 1 August 2016

[82] Potraz bans bulk SMSs, https://www.newsday.co.zw/2013/07/26/potraz-bans-bulk-smss

[83] At the time, SMS was a more popular means of reaching citizens, and Kubatana was looking at a database of about 95 000 subscribers: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/02/Case_Study_-Kubatana.pdf

[84] Lincoln Towindo (2016), President cracks whip, The Sunday Mail, April 3, 2016 http://www.sundaymail.co.zw/president-cracks-whip/

[85] Facebook, Whatsapp users face glitches in Zimbabwe as civil servants strike - See more at: http://nehandaradio.com/2016/07/06/facebook-whatsapp-users-face-glitches-zimbabwe-civil-servants-strike/#sthash.wgCD8ycf.dpuf http://nehandaradio.com/2016/07/06/facebook-whatsapp-users-face-glitches-zimbabwe-civil-servants-strike/

[86] Updated: 30 nabbed in Epworth, Ruwa as police rein in rowdy touts, http://www.newsjs.com/url.php?p=http://www.herald.co.zw/30-nabbed-in-epworth-ruwa-as-police-rein-in-rowdy-touts/

[87] Outrage on Whatsapp Blackout, https://www.newsday.co.zw/2016/07/07/outrage-whatsapp-blackout/

blackout, reminding people that in fact, his ministry had been fighting for the rights of citizens to keep accessing Whatsapp in the face of sustained efforts by local telcos to have it banned.[88]

On the day of the stay away, POTRAZ, issued a veiled threat in a public warning that "any person who would be caught in possession of, generating, sharing or passing on abusive, threatening, subversive or offensive telecommunication messages, including WhatsApp or any other social media messages that may be deemed to cause despondency, incite violence, threaten citizens and cause unrest, will be arrested and dealt with accordingly in the national interest."[89] The notice went on to further warn that "All SIM cards in Zimbabwe are registered in the name of the user. Perpetrators can easily be identified." Following this notice, some social media users believed that the government had the capability to intercept and decrypt even Whatsapp messages. Also, what is worrying about this notice is the vagueness of what constitutes 'abuse' of social media.

Following the internet disruptions, Zimbabweans on Twitter and non-Zimbabwean supporters online quickly updated local netizens about circumvention tools such Virtual Private Networks (VPNs) to install on devices and use in order to get around the shutdown and stay connected. [90]

Other senior government officials have joined President Mugabe in speaking out in favour of curtailing internet freedom. For instance, in April 2016the ICT Minister, Supa Mandiwanzira, mentioned government's intentions to penalise those who abused social media platforms. And on August 9, 2016, army commander General Constantino Chiwenga declared in a press conference that social media criticism and mobilising against the government had "serious potential to disturb the peace" and therefore the full wrath of the law would be applied.[91] On the same day, reports of three men allegedly exposed in the government's latest 'cyber-terrorism probe' surfaced.[92] A close look at the social media activities of the said "social media terrorists" showed that one of them - @rimbe_t - had not posted a tweet in over a year. Besides, the article also did not stipulate which laws these 'terrorists' broke. Critics see these utterances as government's tactics "to instil fear and self-censorship on the exercise of constitutionally guaranteed rights of freedom of expression, access to information and freedom of conscience."[93]

4.3 Website Blockages and Content Removals

While blockages of specific content are significant, the state also dabbles with content removal. Between 2013 and 2014, Zimbabwean government authorities and opposition leaders frequently pressured users and content producers to delete content from social media platforms during the election period, reflecting a rise in this trend compared to previous years.

[88] Gov't rejects WhatsApp Proposal Ban – Minister, The Herald, March 15, 2016 http://www.herald.co.zw/govt-rejects-whatsapp-proposal-ban-minister/

[89] Here's the Zimbabwean government's warning against social media abuse, http://www.techzim.co.zw/2016/07/heres-zimbabwean-governments-warning-social-media-abuse/#.V4jc5o6zDaY

[90] Survive Social Media Blackout, http://kalabashmedia.com/2016/07/05/survive-social-media-blackout-zimbabwe/

[91] ZDF Stand by President Says General Chiwenga, http://www.herald.co.zw/zdf-stand-by-president-says-general-chiwenga

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

[93] MISA-ZIMBABWE Statement on Disconnection of Whatsapp July 2016, http://www.misazim.com/misa-zimbabwe-statement-on-government-threats-to-regulate-abuse-of-social-media

Most notably, the Facebook page of the anonymous whistle-blower Baba Jukwa was deleted in July 2014, though the manner in which it was removed remains mysterious.[94] Baba Jukwa, believed to be a mole within or connected to the ruling party Zanu PF, was pseudonymously posting to a Facebook page allegations of scandals and corruption, mainly involving politicians and state officials. Baba Jukwa also made predictions of what was going to happen within the political landscape and within the ruling party, many of which turned out to be true. In late 2014, the government reportedly went out of its way to identify the person(s) behind Baba Jukwa, including reportedly sending some officials to the United States to try and liaise directly with Facebook and convince the company to delete the page, which at the time, had close to half a million users.[95]

In previous years, the government had reportedly sought Chinese technical assistance in censoring the page and identifying its owner.[96] Some believe that the authorities eventually just managed to hack into and take control of the Baba Jukwa page to delete the profile. Whatever the case, the page was ultimately taken down in July 2014, after an editor at the state-owned *Sunday Mail* newspaper, Edmund Kudzayi, was arrested in June on accusations of running the Baba Jukwa account with the intention of subverting the government through waging what was termed as "cyber-terrorism".[97] Kudzayi was released on a USD 5,200 bail about two weeks later, sparking speculation that he had just been used as a scapegoat.[98] However, he lost his job at the *Sunday Mail*. There is wide belief that 'Baba Jukwa' was not one person but a small network of disgruntled individuals collectively providing intel on the page.[99]

Whereas many citizens are increasingly using pseudonyms online to discuss political topics,[100] and following the arrest of the suspected owner of the anonymous Baba Jukwa account in mid-2014, users have increasingly opted to self-censor out of concern over the state's perceived capacity to seek out the identities of pseudonymous individuals.[101] Around the time the purported Baba Jukwa was arrested, the pages of a few other anonymous bloggers and operators of controversial social media pages, including the popular *Mugrade Seven,* mysteriously went down.[102] Some followers of the pages claimed that the page admins had de-activated their own accounts amidst fears that local law enforcement agents had perhaps acquired sophisticated hacking skills and would soon catch up with them. The *Mugrade Seven* page has long since been revived, and carried a message on the front highlighting that this was a new page as the old one had been hacked.

---

[94] Facebook Politics in Zimbabwe, Who is Baba Jukwa, http://africasacountry.com/2014/07/facebook-politics-in-zimbabwe-who-is-baba-jukwa

[95] Tendai Rupapa, "Baba Jukwa investigators in US," Chronicle, September 2, 2014, http://bit.ly/1QBh73O

[96] Jane Flanagan, "Mugabe hunts for internet mole 'Baba Jukwa' revealing his secrets," The Telegraph, July 4, 2013, http://bit.ly/1QBhb3L. Cited in Freedom House, Zimbabwe Freedom on the Net 2015.

[97] Adam Taylor, "Has Baba Jukwa, Zimbabwe's infamous anonymous whistleblower, really been caught?" Washington Post, June 25, 2014, http://wapo.st/1KetzRG; Charles Laiton, "Sunday Mail Editor 'is Baba Jukwa," The Standard, June 22, 2014, http://bit.ly/1Lyv02G.

[98] Interview with journalist working in the private media held on 23 June 2016. http://nehandaradio.com/2014/08/01/baba-jukwa-speaks-to-nehanda-radio

[99] Baba Jukwa Speaks to Nehanda Radio, http://nehandaradio.com/2014/08/01/baba-jukwa-speaks-to-nehanda-radio

[100] Tendai Chari, "Consumption and Networking," in Online Journalism in Africa, ed. Hayes Mawindi Mabweazara, et al., (New York: Routledge, 2014) 192; Cited in the Freedom House, Freedom on the Net Report, 2015.

[101] John Mokwetsi, Cyber freedom: Have we started to censor ourselves? http://bit.ly/1jIMmPE.

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

However, not only the Zanu PF government seemed fazed by activities happening on social media. Popular Movement for Democratic Change (MDC) opposition party leader, Morgan Tsvangirai in May 2015 ordered that all Whatsapp and Facebook groups administered by any members of his party be shut down or the members would be suspended.[103] It is alleged that Tsvangirai had started to feel irked by the amount of critical public debate being held on social media platforms among the party's senior officials. Following the ban, the MDC party reportedly suspended five of its officials based in Zimbabwe's second largest city Bulawayo on May 10, 2015 for allegedly "abusing social media platforms to attack the party's top leadership."[104]

Earlier in 2013, a website called 'My Zim Vote' was anonymously created to enable Zimbabweans to check if they were registered on the voters' roll by simply entering their national registration identity number. The people behind the website were not known, nor how they had managed to get a hold of the voters' register. Many Zimbabweans found the website extremely useful as it allowed them to access information that they were entitled to but was generally mystified by the Zimbabwe Electoral Commission (ZEC) and the Registrar General's office.[105] ZEC has since launched an investigation and there is speculation that it ordered the subsequent shutdown of the website. The website (www.myzimvote.com) remains down as at the time of writing this report.

4.4 Pushing Government's Propaganda Online

The Zimbabwe government is embracing the use of social media platforms such as Twitter and Facebook to engage with citizens in discussing socio-political and economic issues affecting the country. However, the use of technology in the government is still limited as several institutions do not have an online presence and officials lack digital skills for meaningful engagement with citizens. Nonetheless, some government officials, and state media, are also pushing government's propaganda into the online sphere.

Only a handful of government officials like former Minister of Information (now Higher and Tertiary Education Minister) Professor Jonathan Moyo, Zanu-PF Member of Parliament for Highfield Psychology Maziwisa, and a pseudonymous Twitter account operating as @ZANUPF_Official, among others, are actively using platforms such as Twitter to endorse government operations. For instance, the @ZANUPF_Official Twitter account often echoes what Professor Moyo tweets, dishes out veiled and sometimes direct threats, and following the arrest of Evan Mawarire, tweeted that it was time to "unleash operation #occupytwitter by transforming the narrative." Professor Moyo, who with over 70,000 followers as of July 2016, tweets from the handle @ProfJNMoyo famously known for fuelling Twitter wars[106] through his outbursts and sometimes "very crude and undignified language of hate speech"[107] and staunch defense of unpopular government positions. Whether he actually represents the government position or not, Moyo is vicious in his attacks of the government's perceived and real enemies.

To some, the professor's rants and "illogical defense of the indefensible is an indicator of a regime that is running scared and out of ideas in the face of a 'third force' they can neither fully comprehend nor control."[108] The professor has been one to play the role of downplaying the impact

[103] Gift Chirauro, Is banning social media good for MDC, Techno Mag, http://bit.ly/1NNa6PT
[104] Luyanduhlobo Makwati, MDC-T suspends officials for abusing social media, Southern Eye, May 10, 2015, http://bit.ly/1LSORfd.
[105] ZEC has historically refused to release the voter's roll for public inspection, citing logistical reasons.
[106] Jonathan Moyo fuels Twitter wars, http://www.thezimbabwedaily.com/zimbabwe/31468-jonathan-moyo-fuels-twitter-wars.html
[107] Interview with blogger and twitter user, Daphne T. Jena conducted on 9 July 2016
[108] Interview with human rights activist and anonymous blogger conducted on 9 July 2016

of the #ThisFlag campaign and social media movement, which in its initial stages he quickly dismissed as a "passing fad" when it started gaining popularity online, as well as attempted to disparage its founder Pastor Evan Mawarire by labelling him a regime change agent sponsored by the West. Further, Professor Moyo has actively accused Pastor Mawarire of working with the "'succession elements" within ZANU PF perceived to be led by Vice President Emmerson Mnangagwa.

Moyo and Maziwisa were also central in the creation of the counter movement #OurFlag believed to have been started especially with the hope to confuse some Zimbabweans while diluting what #ThisFlag was trying to achieve by urging citizens to demonstrate their 'patriotism' and support for the President. The #OurFlag movement momentarily caused some confusion on Twitter. The #OurFlag campaign naturally got the backing of the state broadcaster, ZBC, whuch run dozens of adverts on national television, with the movement culminating in the #OneMillionMan 'tribute' match on May 25, 2016, which according to Home Affairs Minister Dr Ignatius Chombo was mainly intended to demonstrate "Zanu PF's force and might."[109]

Professor Moyo also initiated the hashtag #ZimbabweOpenforBusiness as a counter to the #ShutDownZimbabwe2016 campaign. Known for his quick wit and smart talk, Professor Moyo quipped recently on Twitter, that "the notion that anyone can build #Zimbabwe by shutting it down is an oxymoron!" According to a human rights blogger, Moyo is "single-handedly doing an excellent job of holding the fort for the Zanu-PF machinery online."

On the surface, Zimbabweans online engage directly with these officials, some take part in protracted diatribes especially with Professor Moyo, because the effect that these platforms have is to make everyone equal. It appears that since some of these officials are open to engagements, people will still try that route of knocking sense into them, no matter how futile it might seem.[110]

4.5 Digital Activism

The year 2016 saw Zimbabweans took a stand and stage an almost unprecedented act of civil disobedience.[111] Citizens heeded a call to 'stay-away' from work in protest against the government's failure to address citizens' concerns over the declining economy the campaign utilised social media through the Twitter hashtag #ShutDownZimbabwe2016 to mobilise protesters while groups such as teachers' unions and public transport drivers organised their members via WhatsApp groups.

The #ShutDownZimbabwe2016 movement was initiated by the #ThisFlag cyber-movement that was started by a frustrated Pastor, Evan Mawarire, who through posting videos lamenting the country's collapse, quickly garnered the support of online activists and other citizens. Observers cite #ShutDownZimbabwe2016 as the first campaign in Zimbabwe where online mobilisation led to offline action.[112]

Independent news websites and other digital media outlets based outside Zimbabwe are providing critical sources of information for Zimbabwean citizens, especially on taboo or sensitive subjects that

[109] Quoted in the Sunday Mail newspaper: http://www.sundaymail.co.zw/million-man-march-just-the-beginning

[110] Blogger Daphne T.Jena in an interview conducted on 9 July 2016.

[111] Tension as 'Zim shutdown' begins, https://www.newsday.co.zw/2016/07/06/tension-zim-shutdown-begins/

[112] Paraphrasing Alex Magaisa in: The Big Saturday Read: Citizens' movement and the resurgence of the repressive state in Zimbabwe - http://alexmagaisa.com/big-saturday-read-citizens-movement-resurgence-repressive-state-zimbabwe

some local media groups might be too afraid to cover due to fears of government reprisal.[113] These diaspora-based outlets, such as *NewZimbabwe.com* and *Nehanda-radio.com*, post reports on sensitive issues sent to them by local journalists and citizens who write under pseudonyms, a practice employed by many journalists. Few independent news outlets are based in the country. When the *#ThisFlag* movement started to take shape in the middle of 2016 a new website named shutdownzim.net emerged online among other things, to aggregate, document and 'storify' the "revolution that is clearly starting to happen in Zimbabwe for posterity."[114]

In 2014 a Facebook group called 'Occupy Africa Unity Square' was born, with the intention to campaign for the president's stepping down. The movement organised a series of peaceful protests largely characterised by calling supporters to meet offline and sit in the Africa Unity Square gardens, which face the Parliament building. The police always reacted in a heavy handed manner to disperse the protestors, and eventually, the movement's leader, Itai Dzamara, was abducted in March 2015 and remains missing to-date.[115] There have been previous reports of abduction of vocal activists.[116] In 2016, Pastor Evan Mawarire, founder of the #ThisFlag movement, reported that he had on several occasions, been followed by unknown individuals who tried to abduct him. [117]

Emboldened by the general discontent and uprisings gripping the country, another Facebook group called *Tajamuka/Sesjikile*[118] (we have had enough) rebranded its mission as that to "give Zimbabweans a voice in running the country with the primary aim of forcing President Robert Mugabe to step down before the general elections to be held in 2018." Initially created to address youth problems in Zimbabwe,[119] the movement ignited the violent protests that saw the torching of the Zimbabwe Revenue Authority (ZIMRA) warehouse at the Beitbridge border post in protest against the Statutory Instrument (SI 64 of 2016)[120] introduced in June 2016 by the government, banning the importation of selected basic commodities. *Tajamuka* in partnership with the National Vendors Union also led the protest in June 2016, against Vice President Phelekezela Mphoko's continued stay in the five-star *Rainbow Towers* hotel in the capital at the taxpayers' expense. [121] The movement's leadership was arrested in July 2016 on allegations of "inciting public violence" and later released on bail with conditions to report to the police once a week.[122]

Overall, not a lot of civil society is directly engaging with issues of internet governance and online freedom in Zimbabwe partly due to insufficient understanding of the issues. A fear of reprisals from state authorities also hinders some civil society actors from working on promoting internet freedom.

[113] Commentators based abroad do not feel that they are under the same danger of arrest as those based domestically, and therefore express themselves freely.
[114] Interview with political analyst TZ conducted on 22 June, 2016
[115] Itai Dzamara Case History, https://www.frontlinedefenders.org/en/case/case-history-itai-dzamara
[116] Jestina Mukoko Abduction and detention, Wikipedia, https://en.wikipedia.org/wiki/Jestina_Mukoko,
[117] Zimbabwe - Reports Emerge - Pastor Evan Mawarire escaped an abduction!, https://www.youtube.com/watch?v=r4GwTSSeE8Q
[118] Tajamuka Sesjikile Campaign Fcaebook page, https://www.facebook.com/TajamukaSesjikile-Campaign-1207194655958782/about/?entry_point=page_nav_about_item&tab=page_info
[119] Tajamuka Campaign, http://www.pindula.co.zw/Tajamuka/Sesjikile_Campaign
[120]Control of Goods (Open General Import Licence) (No.2) Amendment Notive, 2016 (No.8), http://www.czi.co.zw/images/downloads/statutory.pdf
[121] VP Mphoko hotel stay protest, https://www.youtube.com/watch?v=TLEp6WypRT0
[122] https://www.newsday.co.zw/2016/07/12/tajamuka-leader-granted-bail

5. Conclusion

From the findings of this research, some notable patterns emerge that indicate the different strategies and tactics employed by the Zimbabwean government to stifle the digital rights of citizens:

- Resorting to the growing trend of effectuating internet shutdowns while evoking state security justifications especially through the throttling of social networks. Because so many other governments seem to be getting away with this disproportionate method of quelling political unrest, the Zimbabwean government also jumped onto the bandwagon, and this will likely get worse in the run-up to the 2018 election year.[123]

- Hiking the cost of free speech both monetarily and through elevating personal risk for committing minor infractions, for example through veiled threats and subsequent imposition of impossible jail terms or fines.

- Stringent laws and policy directives are on the increase. The Zimbabwean government is adopting a broad array of draconian, vaguely worded and overly broad laws to govern the digital space, in attempts to silence legitimate criticism of public officials. While in the majority of cases charges have been dropped or dismissed, implicated individuals would have necessarily been subjected to harassment, arrest, held in pre-trial detention and subjected to costly criminal trials. This achieves the overall effect of self-censorship.

- Meanwhile, the government invokes various pieces of existing but deficient legislation in attempts to quell criticism and dissent online and punish individuals perceived to be troublemakers. [124] Consequently, there have been far too many cases of individuals being arrested for online posts that criticise, 'insult' or undermine state security or the person and office of the President.

- Making real-life examples of perceived 'trouble makers' through criminalising peaceful expression. Vocal activists are often profiled, occasionally singled out, isolated or neutralised in some way as a means of containing trouble and disheartening other activists, resulting in self-censorship.

- The government of Zimbabwe is currently working on a raft of laws to regulate ICT use with the touted objective of protecting online users and curbing cybercrimes. However, the measures are likely to strengthen the government's arsenal for violating citizens' internet freedoms. [125]

[123] Interview with Political Analyst TZ conducted on 22 June 2016

[124] For example the Criminal Law and Codification Act (CODE) which was used to arrest the alleged Facebook pseudonymous character, Baba Jukwa believed to be former Sunday Mail Editor Edmund Kudzayi. Charges were later dropped due to failure by the state to gather sufficient evidence.

[125] Presentation by POTRAZ on what the cyber regulatory framework in Zimbabwe might look like, including aspects of the proposed Computer Crime and Cyber Crime Bill: http://apps.fpb.org.za/101/presentation/day3/Online_Regulatory_Framework_in_Zimbabwe.pdf

6. Recommendations

Based on the findings and conclusions above, several recommendations can be drawn for government, civil society, private sector and media to improve the overall state of internet freedom in Zimbabwe.

6.1 Government

The government must amend regressive and draconian laws, including clauses in the CODE that must be abolished. In the same spirit, reference should be made to the need to protect human rights online and offline as embodied in international human rights instruments, including the recent UN Human Rights Council resolution.[126] Commitment to this should be unequivocal. 'Necessary and Proportionate Principles'[127] should also be applied to the crafting of cyber laws, so that there is observance and application of human right principles to proposed communication surveillance.

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

In the case of intent to regulate social media, there are risks of penalising a mere tool (social media platforms) rather than the conduct of individuals using the tool. There is value in undertaking a "robust and wide-ranging consultative process to gather the views of the most invested stakeholders who live and thrive online.[128] This has the distinct advantage of ensuring that those who fully understand how such platforms work suggest workable and practical solutions for their regulation.

6.2 Civil Society

There is need for more meaningful engagement by civil society through finding ways of participating in the limited consultative processes by government. This includes taking part in spaces such as the Zimbabwe Internet Governance Forum (ZIGF) and submitting policy briefs through relevant parliamentary portfolio committees. Over the past few years, Zimbabwe civil society seems to have understandably felt powerless to shape the cyber bills currently under discussion. This is mainly because of lack of capacity and inability to comprehend Internet governance processes and their accompanying legalese.[129] However, civil society should work actively with human rights defenders, technologists, lawyers and academics in making inputs to policy processes.

6.3 Media

The media being the fourth estate should focus on the undue and abusive practices of government in regard to internet governance issues. Responsible journalism includes the ability to be the voice that simplifies the issues for its audiences. There is a capacity gap within the media that needs to be addressed through training to empower the press and to shed light on problematic legislations and processes relating to Internet use and policy gaps.[130]

---

[126] See: UN Human Rights Council resolution, https://www.accessnow.org/un-passes-resolution-condemning-internet-shutdowns

[127] Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/principles

[128] Social media: Penalise the conduct, not the tool, http://www.herald.co.zw/social-media-penalise-the-conduct-not-the-tool

[129] Interview with IT Expert, Chris Musodza conducted on 1 August 2016.

[130] Comment from Koliwe Nyoni, MISA-Zimbabwe Programme Officer on 15 July 2016

This report was produced by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) under the OpenNet Africa initiative (www.opennetafrica.org) which monitors and promotes internet freedoms in a number of African countries including Ethiopia, Kenya, Rwanda, Burundi, Tanzania, Uganda and South Africa. As part of the project, we are documenting internet rights violations, reviewing cyber security policies and how they affect internet freedoms, promoting information availability and conducting awareness-raising.

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