GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

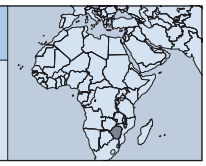
ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Creative Commons Attribution 3.0 Licence <creativecommons.org/licenses/byncnd/3.0>

ZIMBABWE

Surveillance under the garb of rule of law



MISA-Zimbabwe
Nhlanhla Ngwenya
www.misazim.com

Introduction

Zimbabwe is a multi-party democracy with a population of 13 million, located in southern Africa. As the country's political crisis worsened between 2000 and 2008, with swelling opposition against the ruling ZANU-PF party which has governed Zimbabwe since its independence in 1980, the government reacted by enacting a raft of laws meant to control and restrict free and active citizenry. These included the Interception of Communications Act. The law provides for the "lawful interceptions and monitoring of certain communications during their transmission through a telecommunication, postal or any other related system or service in Zimbabwe."[1] While it was always suspected that the government conducted communications surveillance of its opponents and human rights activists, the enactment of the law simply provided a legal basis for the practice. In October 2013 the government sought to entrench the surveillance law through Statutory Instrument (SI) 142 on Postal and Telecommunications (Subscriber Registration) Regulations. The SI provides for the establishment of a central database of information about all mobile phone users in order to assist emergency services and law enforcement agencies and to protect national security. This was despite the fact that five months prior, in May 2013, Zimbabwe had adopted a new constitution with better safeguards for the enjoyment of freedom of expression. And as things stand there is discord in the legislative framework caused by disharmony between the statutes and the constitution, providing fertile ground for violation of citizens' basic liberties including their right to privacy.

Policy and political background

After 33 years of debate and failed attempts at constitutional reform, Zimbabwe finally adopted a new constitution in May 2013 to replace the Lancaster House Constitution, which ushered in the country's independence. Key among the content of the new charter is an expansive Bill of Rights, which among other liberties, grants for the first time in Zimbabwe's history explicit guarantees for freedom of expression, media freedom and access to information.

Despite this, the country is still to align its laws to the new constitution, thereby ensuring that a gamut of laws remain in place to curtail freedom of expression. These include the Access to Information and Protection of Privacy Act, the Criminal Law (Codification and Reform) Act, the Interception of Communications Act, and the Official Secrets Act, among other laws. These acts separately and/or collectively severely erode Zimbabweans' right to freedom of expression. Although the Interception of Communications Act is the one that is more relevant to online communication, the authorities can still use the other laws to press charges against those deemed to have crossed the line when expressing themselves through online platforms. The recent arrest of a teenager, Gumisai Manduwa,[2] over a Facebook post on President Robert Mugabe, and threats of the arrest of those who may have provided information to an online Facebook character called *Baba Jukwa*,[3] demonstrate the extent to which the state can go in trying to sniff out those expressing themselves online.

1 The Interception of Communications Act (Chapter 11:20), enacted in Zimbabwe in August 2007.

2 Gumisai Manduwa appeared in court in January 2014 facing charges of contravening Section 33 of the Criminal Law (Codification and Reform) Act for allegedly insulting President Robert Mugabe. Manduwa had posted on Facebook claims that Mugabe had died and his body was being preserved in a freezer. Manduwa's arrest was the second such case following the arrest in 2011 of Vikas Mavhudzi, who had also posted a Facebook comment that suggested the opposition should emulate pro-democracy protests in Egypt. He was charged with subversion and spent close to a month in prison. He was subsequently acquitted in 2013 for lack of evidence.

3 Baba Jukwa is a faceless online blogger with a Facebook account that has gained popularity in Zimbabwe for exposing alleged unpleasant secrets of the government and the ruling party, ZANU-PF. On 11 May 2014, a state-run newspaper, *The Sunday Mail*, alleged that individuals behind the Facebook account had been unmasked by unnamed hackers in New Zealand, who had hacked into Baba Jukwa's private Google account. The hackers reportedly then passed the information to Zimbabwean state authorities. Since then the state-controlled newspapers have been feasting on the story, serialising private correspondence between Baba Jukwa and his associates as well as informants calling on the authorities to arrest them and charge them under the country's security laws.

Legislative paralysis provides room for surveillance

Although the new Zimbabwean constitution has received its fair share of criticism, especially as it relates to executive authority,[4] there is general consensus that it is far more democratic than its predecessor, as it seeks to promote and protect wholesale civil liberties. Further, it obligates the "[s]tate and every person, including juristic persons, and every institution and agency of the government at every level" to "respect, protect, promote and fulfil the rights and freedom set out" in the Declaration of Rights provided for in Chapter 4 of the constitution. One of the key elements of the constitution is its protection of citizens' right to privacy.

Article 57 states:

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 condition disclosed.

This provision is anchored on international human rights law and instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which Zimbabwe ratified in 1991.

Besides constitutionally outlawing infringement of citizens' right to privacy, the constitution also guarantees citizens' freedom to express themselves and their right of access to information. It does this under Articles 60 and 61.

For example, Article 60 stipulates as follows:

(1) Every person has the right to freedom of conscience, which includes—

(a) freedom of thought, opinion, religion or belief; and

(b) freedom to practise and propagate and give expression to their thought, opinion, religion or belief, whether in public or in private and whether alone or together with others.

Article 61 states:

(1) 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.

Cognisant of the fact that freedom of expression is not absolute, the constitution then provides precise and narrow scope within which the right could be limited under Article 61 (5). These limitations are in line with international instruments on freedom of expression and in particular satisfy the three-part test for measuring restrictions on freedom of expression; this test has been elaborated on in judgments delivered by international courts on matters related to human rights treaties.[5]

However, despite this development, Zimbabwe has continued to retain interception of communication laws – disguised as upholding the rule of law – specifically the ICA and SI 142, which contain provisions that are in conflict with the new constitutional dispensation. For example, while the new constitution provides for the right to privacy and free expression, the ICA legalises the interception of one's communication and actually establishes an interception of communications unit named the Monitoring of Interception of Communications Centre. The Centre is staffed, controlled and operated by designated experts of the state.[6] The process of establishing the Centre, its composition and work is opaque, and as a result there is no accountability around its activities.

Although the ICA provides for procedure for interception, the requirements to obtain a warrant of interception remain vague and subject to abuse. According to the law, an application for interception may be made to the ministry responsible for transport and communications by the Chief of the Defence Intelligence, the Director General of the President's Department of National Security, the Commissioner General of the Police and the Commissioner General of the Zimbabwe Revenue Authority. A warrant for interception can be issued where there is "reasonable suspicion" that a serious offence has been, is being, or will probably be committed, or to prevent

4 New Zimbabwe. (2013, February 5). NCA slams Constitution, urges 'No' vote. New Zimbabwe.com. www.newzimbabwe.com/news-10197-NCA+urges+rejection+of+new+constitution/news.aspx

5 Center for Law and Democracy. (2010). Restricting Freedom of Expression: Standards and Principles. Background paper for meetings hosted by the UN Special Rapporteur on freedom of opinion and expression. www.law-democracy.org/wp-content/uploads/2010/07/10.03.Paper-on-Restrictions-on-FOE.pdf

6 MISA-Zimbabwe. (2010). *An Analysis of Amendments to Media Laws in Zimbabwe Since the Year 2005*. Harare: MISA-Zimbabwe.

a threat to national security, the economic interests of the state or public safety.[7] There is no clarity on what constitutes reasonable suspicion and how it is determined. Neither is there an explanation on what constitutes sufficient grounds to prove that an offence is likely to be committed. Further, the Act defines "serious offence" as conduct constituting an offence punishable by a maximum jail sentence of up to four years. There are a number of offences that fall under this category, which include abortion, assault perjury, reckless driving and violating a corpse. Lack of clearly listed offences considered serious under the interception law leaves the Act vague and open to abuse by those in authority.

To make matters worse, the minister's decisions are not subject to court review. Instead, it is only the Attorney General, who is a political appointee, who has authority to review the conduct of the minister and the exercise of their power. And this is only done within three months of the end of each year, thereby allowing potential abuse of the law to go unchecked and giving state agents latitude to intercept citizens' communications without restraint.

Besides giving wide discretionary powers in the administration of the Act to the relevant minister while circumventing effective judicial oversight, the Act also places harsh duties on service providers to undertake interception and monitoring, and gives authorities any assistance they may require to snoop into private communication. Refusal to provide assistance is punishable by up to three years imprisonment.

There are no provisions in the Act guaranteeing the safe keeping or storage of information or data collected through interception. Neither is an individual whose information has been intercepted informed after the completion of investigations, nor does the law provide specific timeframes within which the information should be destroyed when no longer needed. Instead, the Act simply enjoins the responsible state officer to destroy it "as soon as possible after it is used for the purposes of (the) Act."[8]

Instead of addressing the law's patently intrusive nature and aligning it with the new constitution, the state seemingly entrenched the harmful effects of the Act through SI 142. The Instrument calls for the establishment of a database of information about all mobile phone users in the country; compulsory SIM card registration; and the release of private information to the police in the absence of a search warrant, supposedly with the objective of assisting emergency services, assisting law enforcement agencies and safeguarding national security.[9] While it is acknowledged that concerns around e-crimes and state security would require legislative intervention, SI 142 generally fails the democratic test as it simply legalises intrusion of citizens' privacy guaranteed in the constitution.

As Gwagwa[10] argues, for example, mandatory registration provides the government with the means to track citizens' whereabouts – and by extension the people with whom they associate – and creates a situation in which personal data could theoretically be shared between government departments, allowing for the creation of individual profiles based on data stored elsewhere.

Gwagwa further argues that while the regulations stipulate that no information shall be released if doing so would violate the constitution, by empowering the police to request information without informing the individual concerned and without judicial oversight, citizens are not provided time to object to the release of their data based on the constitutional rights granted to them.

It is against these constitutional deficiencies that in March 2014 the Parliamentary Legal Committee, whose mandate is to assess the constitutionality or legality of laws made by parliament, found the regulations to be unconstitutional. This was due to their potential infringement of Article 57 providing for the right to privacy and Article 61 guaranteeing freedom of expression.[11] The Committee recommended that the regulations should be amended to bring them into line with the constitution and guarantee judicial oversight over access to subscriber databases.

While government subsequently repealed SI 142 in June 2014 and replaced it with Statutory Instrument 95 in response to the Parliamentary Legal Committee's report, the import of the new regulations largely remain similar to the old instrument.

It is the failure and/or reluctance to amend the law that continue to provide the legal basis to erode citizens' freedoms in complete disregard for the constitution and international protocols on the right to privacy.

Conclusion

While it is not uncommon for countries to promulgate laws that seek to safeguard their national

7 Ibid.

8 Section 17 of the Interception of Communications Act.

9 Gwagwa, A. (2014). State Security and Personal Liberty in the Digital Age. Paper presented at a discussion on surveillance in Harare, 8 May 2014.

10 Ibid.

11 Veritas. (2014) Bill Watch Report 15/2014. Zimbabwe Situation. www.zimbabwesituation.com/news/bill-watch-152014-19th-march

security and prevent e-crimes through interception of communications, this should not be to the detriment of citizens' fundamental freedoms. Aside from threatening the very freedoms guaranteed in the constitution, the interception of communications laws that the state can use to conduct surveillance of its citizens fails the democratic test in a number of ways when juxtaposed against international human rights law and standards on communications surveillance. For instance, there is no transparency in the establishment and operations of the monitoring and interception body, which fosters arbitrary actions that infringe on citizens' right to privacy. In other jurisdictions such as Australia, New Zealand and the UK, independent commissions that report to parliament conduct interception and undertake public reporting processes. Such a commission is imperative, especially in Zimbabwe, where there is mistrust of those in power.[12] Also, one of the key principles in ensuring democratic legislations on surveillance is judicial oversight in the implementation of the law. This is not the case with the Zimbabwean laws. As a result, the instruments do not contain the requisite checks and balances that will guarantee the balance between the need for interception and protection of citizens' rights, which is key in preventing the arbitrary abuse of the law. In essence, the interception laws in Zimbabwe do not meet the minimum standards as prescribed in the 13 International Principles on the Application of Human Rights to Communications Surveillance.[13] The Principles call for:

- Clear laws governing how state authorities may access communications data
- Communications data to be given the same protection as the content of communications
- Access to communications data to be authorised by a competent judicial authority
- Prior or post user notification that a request for communications data has been authorised
- Transparency about the use and scope of communications surveillance powers
- Effective public oversight of the implementation of surveillance laws
- Better protection for the integrity of communications and systems
- Strong privacy safeguards in mutual legal assistance treaties
- The introduction of criminal offences against illegitimate access to communications data
- The protection of whistleblowers.[14]

Action steps

While Zimbabwe is still to publicly record incidents where the interception law has been used against citizens, there is general fear that the state is snooping. This fear is grounded on the publication of information and correspondence as well as unflattering details of government opponents and civil society activists. This has resulted in either self-censorship when it comes to electronic correspondence or the exercise of extreme caution in how people express themselves through online platforms. In this regard it is therefore critical that the Zimbabwean government:

- Repeals its interception of communications and surveillance laws in line with the new constitution to protect citizens' right to privacy and freedom of expression.
- In its review of the laws, the government should ensure that the new acts are in line with regional and international instruments on the right to privacy and expression, as well as in sync with international principles in formulating democratic legislation on surveillance.

Civil society and media freedom groups should:

- Provide policy alternatives that will inform their lobbying of state actors on policy and legislative reforms.
- Build public support for legislative reforms by raising awareness on the right to privacy and its relevance to Zimbabweans' livelihoods and their democratic well- being.
- Seek judicial intervention through test litigation around provisions of the law so as to create legal precedents that will prompt the review of the law as well as inform its content.
- Forge alliances with like-minded regional organisations to lobby states to comply with their own international agreements.

12 MISA-Zimbabwe. (2010). Op. cit.

13 The Principles were developed by a coalition of civil society organisations and have been endorsed by more than 250 organisations across the world. See: en.necessaryandproportionate.org/text

14 Article 19. (2013, September 20). Principles on Surveillance and Human Rights: UNHRC must take action on surveillance. *Article 19*. www.article19.org/resources.php/resource/37251/en/principles-on-surveillance-and-human-rights:-unhrc-must-take-action-on-surveillance