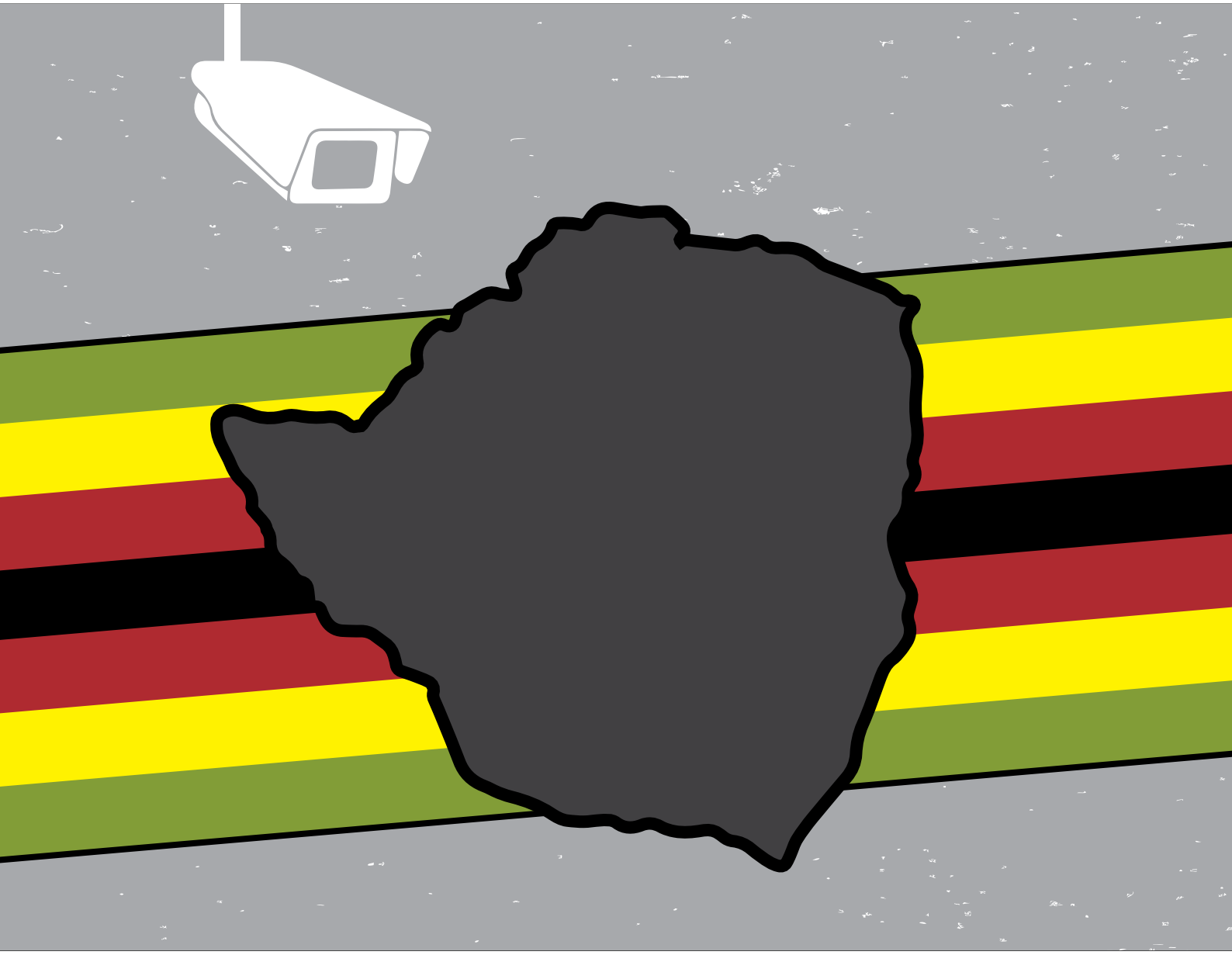
Drifting Towards Darkness: An Exploratory Study of State Surveillance in Post-2000 Zimbabwe



Media Policy and Democracy Report

Drifting Towards Darkness: An Exploratory Study of State Surveillance in Post-2000 Zimbabwe

Media Policy and Democracy Report

 We would like to thank Privacy International, who provided funding for this project through a grant they received from the Ford Foundation under the 'Security on our own terms – developing global South leaders in the field of cybersecurity' project.

November 2019

Available from the Media Policy and Democracy Project website:

https://www.mediaanddemocracy.com/

List of Acronyms

CCTV	**Closed Circuit Television**
CIO	**Central Intelligence Organisation**
CSOs	**Civil Society Organisations**
DSZ	**Digital Society of Zimbabwe**
HRL	**Human Rights Lawyers**
ICTs	**Information and Computer Technologies**
ISPs	**Internet Service Providers**
JOC	**Joint Operations Command**
MISA	**Media Institute of Southern Africa**
MNOs	**Mobile Network Operators**
NGOs	**Non-Governmental Organisations**
PISI	**Police Internal Investigations Services**
POTRAZ	**Post and Telecommunications Regulation Authorities of Zimbabwe**
RGMSI	**Robert Gabriel Mugabe School of Intelligence**
ZANU PF	**Zimbabwe African National Union- Patriotic Front.**
ZEC	**Zimbabwe Electoral Commission**
ZLHR	**Zimbabwe Lawyers for Human Rights**
ZMI	**Zimbabwe Military Intelligence**
ZRP	**Zimbabwe Republic Police**

Table of Contents

Executive Summary

Since Johannes Gutenberg's invention of the press in circa 1439, the information environment we are living in has witnessed the most profound of changes. New communication technologies now allow for the vast accumulation of data, driven by rapid computerisation and automation of life. This has given rise to nearly "privacy-less" lives – with governments, private corporations and other organisations now in possession of an ever-increasing amount of data (Naughton 2018). Corporations, both large and small, now make a profit from predicting consumer behaviour, consumption habits and spending patterns (Haggarty 2009). Yet, often times, the appropriation of these communication technologies has brought about massive surveillance of individuals, especially from states and governments. States have, on many occasions used these new communication technologies to surveil on their citizens (Lyon 2013). This has led to modern-day "surveillance societies" (Lyon 2013).

The rise of surveillance societies is a logical culmination of the digitisation of everyday life (Lyon 2013). Zuboff (2018) notes that this digitisation has recalibrated our lives and changed our conception of freedom – as we come to the realisation that we are being watched from every platform. There is, therefore, no doubt that we are in the midst of a revolution that has jeopardised our privacy by making private data ubiquitous at the click of a button, and our economic survival dependent on our data too (data-driven economies). States, both democratic and authoritarian ones, are now capable of storing huge amounts of data that used to be private. Because data is available, states can now target individuals, groups and organisations for surveillance (Lyon 2013). Communication surveillance has become the most frequently used form of surveillance (Lee 2019). A host of companies like CloudWalk, a Chinese technology company, now go beyond producing communication technologies to producing other technologies like facial recognition. As a result of the rising demand for surveillance technologies, there has been an increase in the number of companies offering surveillance technologies – a phenomenon referred to by Zuboff (2018; 1) as "surveillance capitalism". Zimbabwe has joined the bandwagon of countries scrambling to possess and utilise surveillance equipment.

There is need to highlight that despite this flagrant reported and observed abuse of surveillance powers, Zimbabwe is a signatory of international treaties that seek to safeguard human rights like privacy. These are, for example:

- Zimbabwe is a signatory of the International Covenant on Civil and Political Rights ('ICCPR'), which under Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".
- The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."

In addition to the above international obligations, section 57 of the Zimbabwe constitution guarantees right to privacy. It explicitly state that no person shall be deprived of their rights to privacy unless on the orders of a competent judicial authority. Surveillance oversight should aim at achieving both transparency and relevance (Flaherty 1989 and Bennet 2014). Relevance means it should target actual or planned criminal behaviour, not everyone (Lyon 2010). Transparency means it should be practised within a clearly defined legal framework (Lyon 2010).

Surveillance in Zimbabwe

Emmerson Mnangagwa was elected president of Zimbabwe in July 2018. The process leading to his election was disputed by the opposition, a wave of post-election violence claimed the lives of about nine opposition supporters, and injured many (see: Mail & Guardian 18 October 2018). The military and the police were heavily criticised for their brutality during the protests. International powers like the US, Britain and Germany condemned the government's handling of the protests and the assault of opposition supporters in custody (see: *Business Live*, 2019).

The Zimbabwe Military Intelligence (ZMI), the Police Internal Investigation Services (PISI) and the Central Intelligence Organisation (CIO) have been reported to have been active in the surveillance of key opposition party members, CSO leaders, lawyers, journalists and NGOs accused by the state of funding the protests (see *The Independent* 2013.) Those who have reported having been victims of these surveillance activities believe that the state ran illegitimate digital and physical surveillance on them during the month of January 2019, when the protests were spreading. Hitherto, they still insist the state has not scaled back on its surveillance of its opponents.

With an assorted mixture of surveillance technologies from China, Russia and Iran at its disposal (*Bulawayo News 24*, 2013), state surveillance agencies have been accused by CSOs, NGOs and other activists, of monitoring anti-government activists by tapping their phones, listening to their calls, monitoring their financial transactions (to ascertain whether they have been receiving foreign funding), and tracking their movements through digital technologies.

The surveillance activities that these agencies engage in are often illegal and murky. The Interception of Communication Act (ICA) provides for the granting of an Executive order for surveillance to be legally permissible, granted by the minister of State Security or anyone acting on his/her behalf, or with delegated authority to act as such. The minister is politically appointed, though, so it is difficult to see how impartial he/she can be in sensitive matters of surveillance where political (rather than criminal) interests are vested.

The covert and extrajudicial surveillance undertaken by the state's agencies have often crystallised the frequent accusation that Zimbabwe is an undemocratic country. CSOs, journalists, human rights lawyers interviewed are of the view that surveillance in the country is growing and now have a chilling effect on fundamental freedoms including the right to privacy.

Scope, aims and rationale of the study

This is an exploratory study that seeks to document surveillance practices in Zimbabwe. It explores the characteristics of state surveillance in Zimbabwe. It maps out the Zimbabwean context of surveillance by focusing on the following two broad areas of surveillance:

- Public space surveillance in Zimbabwe
- Communication surveillance in Zimbabwe

The revelations of mass surveillance by former National Security Agency contractor Edward Snowden confirmed peoples' fears that state surveillance is a common practice that has been going on for some time. The revelations also confirm that arbitrary state surveillance has been on-going including in countries which say they uphold the right to privacy it is argued that state surveillance may be worse in countries like Zimbabwe, traditionally perceived as authoritarian states (Makumbe 2009). State surveillance often targets critical constituencies like opposition parties, NGOs, CSOs and investigative journalists (Haggerty 2009). Readily available surveillance technologies from countries like China and Iran, and the latter's willingness to assist countries establish extra-legal surveillance strategies (Evans 2013) necessitate a need to explore the extent of surveillance in countries like Zimbabwe, that have,

for long been allies of China in Africa (Sachikonye 2012). The reports of growing surveillance capabilities (to be explained later), of the state in Zimbabwe has not, arguably, been matched by a response from CSOs, NGOs, HRL, and other players interested in fending off encroaching extra-legal surveillance.

This research therefore, seeks to first establish the extent of the Zimbabwe's state surveillance capabilities. This is very important if interested parties are to be mobilised towards a united response to counter privacy violating surveillance practices by the state.

The context of the research

Zimbabwe has had two political transitions since independence in 1980. The first transition (or the 'First Republic', as it has been referred to, see Makumbe 2009) happened in November 2017, when the country's long-time ruler, Robert Mugabe, was ousted from power by the military, after 37 years in power. His fall led to the Second Republic led by Mugabe's erstwhile ally Emmerson Mnangagwa. In both the first and second republics, a defining characteristic has been a preoccupation with surveillance of opposition supporters, CSOs and NGOs (MISA, 2018). It can be argued that Zimbabwe has experimented with almost major political system from socialism, to capitalism and now to networked authoritarianism. From even the 1980s, the ruling party, ZANU PF, had always maintained a tight grip of the state. Opposition was not tolerated, and a free press was anathema to the ruling party's political designs for total control of the state. Many politicians were charged with subversion of the state, opponents were wiretapped, physical surveillance was rife and many anti-establishment individuals had to live a life of fear (Makumbe 2009). In post- 2000 Zimbabwe, when a vibrant opposition was born and an economic meltdown began, the practices of surveillance became ubiquitous and consistently remain tools of influence and pressure on Zimbabwe's CSOs, NGOs and opposition supporters (Sachikonye 2011). Through an alliance with China and Iran, Zimbabwe has willing allies who are providing the country with the much-needed technologies of surveillance. But how did we come to this point in the first place? Mugabe, the man who dominated Zimbabwe's post-colonial politics for 37 years, has never been a democrat (Makumbe 2009), and the country has never reformed from colonial authoritarianism to embrace tenets of democracy (Sachikonye 2012). From independence in 1980, the country set itself towards an authoritarian kind of politics, backed by China and Russia (Sachikonye 2012). Slowly, the state built intelligence institutions like the CIO, Military Intelligence Agency and PISI with the help of countries like China, Russia and North Korea.

For the Chinese and Russians, Zimbabwe's mineral wealth provided an extra incentive for assisting, since access would have been guaranteed. For example, in 1995, about 70 intelligence operatives from the CIO went for training in China (Makumbe 2009). After the year 2000, China overtook Russia as the most influential power in Zimbabwe (*The Economist* 2007). China's role as an influential power was cemented by Mugabe's fallout with the West over the land reform programme. Mugabe looked east for allies (Look East policy), and China and Iran were there to help. This was a consequence of being snubbed by Western powers (Foreign Policy, 2017).

The fallout with the West, which started around 1997, was followed by a precipitous economic decline which raised dissent to the regime. Mugabe became more authoritarian and repressive. The apparatuses of surveillance were activated (Makumbe 2009) to check on dissent both within the ruling party and outside. Unemployment rose to more than 90%, and agitation against the regime increased ferociously as the economic fortunes of the country nose-dived. The youth, in particular, based in the urban areas, started agitating for change from the year 2000. The regime was threatened, and authoritarian tendencies like surveilling on opponents might have increased in this period (Harvey 2018). These tendencies have not changed in the post-Mugabe period, despite promises to.

The regime still relies on the authoritarian policies left by Mugabe (Harvey 2018).

However, the ruling party ZANU-PF has, of late been rocked by serious factionalism[1]. Even the ascendancy of Emmerson Mnangagwa does not seem to have healed these divisions. Mnangagwa is said to belong to the so-called "Lacoste faction", backed by the military and other forces of the security establishment. There was the now vanquished G40 faction which was opposed to Mnangagwa's rise to power, supported by Professor Jonathan Moyo, a former Minister of Information.

The coup did not heal the rifts in the party. The faction dominating the state and ruling party has undertaken a purge of journalists in the state-controlled media (see *The Zimbabwe Mail*, 2019), security agencies and other top government positions to weed out alleged G40 supporters. One purged state media journalist complained openly on Twitter, "I am being persecuted by I do not even know Jonathan Moyo or George Charamba…" In a faction ridden party like ZANU PF, it is dangerous to belong to, or to be suspected of belonging to the G40 faction aligned to Moyo, a renowned political scientist.

Post-2000 Zimbabwe has seen three worrying developments. Firstly, there has been a complete disregard for the rule of law as evidenced by police brutality, disregard of court rulings etc. (Sachikonye 2011). Secondly, there has been a collapse of the ruling party into state institutions, like the military, the intelligence agency, the police, etc, that are supposed to act as independent entities (Makumbe 2009). This means the ruling party is not literally propped by these institutions for its (political) survival (Makumbe 2009). Thirdly, appointments of senior members of these institutions have been politically, rather than professionally motivated (ZPP 2009). These factors have enabled the cultivation of a surveillance culture that largely operates in the dark with no judicial or institutional oversight. The politicisation of the judiciary (ZLHR 2019) has ensured that the last bastion of defence of human privacy has now been firmly captured into the service of the narrow interests of a political elite.

This worsened after the year 2000 when draconian media and security laws, like the Access to Information and Protection of Privacy Act (AIPPA) and the Public Order and Security Act (POSA) that outlawed public gatherings without police clearance amongst other issues, were introduced (Makumbe 2009). Post-2000 Zimbabwe has witnessed a progressive decline into a sustained authoritarian regime (Bond and Manyanya 2007). This has largely been because of many factors including the regime's reaction to competitive political opposition. (Makumbe 2009). AIPPA for example, outlaws public bodies from providing information to journalists. Journalists cannot, under the law, publish material deemed 'sensitive' and that 'jeopardise' the state's interests. Under POSA, journalists shall not, for example, report in ways that cause 'fear, alarm and despondency'. These are vague offences. Their interpretation is both controversial and subjective. These laws make it impossible for journalists to operate as any news story can be deemed 'sensitive' and 'likely to cause fear alarm and despondency' (MISA 2018).

The ruling regime's reaction – including draconian security and media legislations, has underlined and completed this rapid decline into an illiberal state. This has two major consequences. Firstly, draconian laws and the decimation of investigative reporting (see Munoriyarwa 2018) mean surveillance can go on without the dangers of exposure from an alert and functioning media can bring. Secondly, if journalists dare to question and expose surveillance, they themselves may risk being surveilled and their privacy exposed.

State surveillance beliefs rely heavily on panoptic beliefs (Foucault 1977) that view surveillance as instrumental in bringing order and discipline in society. The belief of the state is that surveillance will frighten citizens out of organised protests against the regime (Zuboff 2013). The developments in the Arab world (the Arab Spring) may have instilled

1 There is a lot of literature available on factionalism in ZANU PF, the intervention of the military and the fall of Mugabe as a culmination of this factionalism, see for example: https://www.up.ac.za/media/shared/85/Strategic%20Review/Vol%2039(2)/pp-3-24-masiya-and-maringira.zp136790.pdf.

fear in the state that public disenchantment ought to be anticipated before it bursts into violent confrontation with the state which may be difficult to contain. However, it should be cautioned that the "youth bulge" – the ever -increasing number of unemployed youth – may prove difficult to contain going forward, regardless of the increasing surveillance practices of the state. Scholars (Flaherty 1989; Bennet 2014 and Lyon 2010) have identified four major types of surveillance regulation that can be blended in most instances. The first, and most common type is surveillance regulation by national government (either the executive, legislature or judiciary or a mixture of them all). There is also surveillance regulation by extra-governmental organisations – watchdogs, ombudsman and/or commissions. There is also surveillance regulation by international agreements. Lastly, there is self-regulation by industry.

Methodological issues

The researcher undertook qualitative research based on in-depth interviews with practising journalists, digital activists, state surveillance agents and digital law experts, lawyers, CSOs leaders. The researcher was also able to identify respondents with detailed and intimate knowledge of surveillance practices in the country. While the research largely draws from in-depth interviews, it is also an empirical research based on observations by the researcher in the course of conducting the interviews. It also draws heavily from mainstream newspaper reports, CSO and NGO reports and related documents with regards to latest developments on surveillance in the country. Thus, this report integrates three data gathering methodologies – empirical observation by the researcher who was on the ground from January 2019 until May 2019; documents and reports – from newspaper reports to NGOs and CSOs and, finally, the in-depth interviews.

In-depth interviews allowed the researcher to understand surveillance from the perspective of the affected and of anti-surveillance activists by digging deep into the experiences of these groups. Qualitative in-depth interviews allowed the researcher to obtain "thick descriptions" (Geertz 1997) of data, and, in the process, enabling the researcher to describe and analyse the meanings of central themes in the life of subjects (Kvale 1996). Respondents were identified through snowballing – where one respondent referred the researcher to the other who shared similar experiences.

There are many ethical considerations that had to be made especially in consideration of the sensitivity of the research. The subject of surveillance in Zimbabwe is directly intertwined with the state, an entity which elicits more fear than trust in the country. Fear of who exactly the researcher is, was evidently pervasive especially amongst former senior members of the status quo. This report, therefore, adopts "partial anonymisation", where names of respondents who requested anonymity are withheld, while displaying the names of those who expressed a willingness to be named.

The interviews sought to establish, among other issues, the extent to which respondents thought state surveillance takes place in Zimbabwe; the targets of state surveillance; the extent to which it complied with domestic legislation and international standard practices on surveillance and privacy; and the capacity of the state, both on the short and long run, to undertake mass surveillance. In addition, the interviews sought to establish the various forms of state surveillance that are growing in Zimbabwe. Reports and newspaper stories enabled the researcher to keep abreast with current developments on surveillance issues in the country. The report also borrows heavily from legislative documents – i.e. constitutional chapters and clauses.

Preliminary Findings

The central actors in state surveillance

Before exploring the forms and extent of surveillance practices in Zimbabwe, the report firstly discusses the main actors aiding the state in surveillance and the central targets of their activities.

The actors: The evidence gathered from this research shows that surveillance is a pervasive practice in Zimbabwe. Respondents also highlighted that surveillance takes place outside the legal provisions of privacy laws. Surveillance is state-led, with the collusion of pliant ISPs and Mobile MNOs, according to respondents.

There are various state institutions that are involved in both physical and digital surveillance. These include the CIO, the ZMI, and the PISI. The ZMI, a specialised arm of intelligence gathering in the army, and the PISI, a specialised intelligence arm of the police force, have been deeply involved in the surveillance of private citizens inside Zimbabwe. The CIO is the central intelligence organisation of the state responsible for gathering civilian intelligence.

ISPs offer an assortment of internet-related services. But, they are begotten to the regulator, Post and Telecommunications Regulation Authorities of Zimbabwe (or POTRAZ), which can withdraw their operating licence as and when it deems necessary. Referring to ISPs, Natasha Msonza of the Digital Society of Zimbabwe (DSZ) said, "Locally, it is mostly the MNOs and ISPs. The recent internet shutdown is further proof that these companies feel as if they do not have much choice but to comply or risk losing licences". During the January 2019 mass demonstrations in Harare, the government resorted to shutting down the internet (a move later declared illegal by the High Court of Zimbabwe,). One former member of PISI said, "We have also been involved in spying on journalists and civic society leaders. But, there is very little we can do except pass on the data to the CIO. Another former member of PISI admitted: "Our job was to help know people, their political beliefs, and friends in and outside the country, their movements and communication had to be monitored, especially when they were challenging the authority of a sitting government…"

Lawyers from the Zimbabwe Lawyers for Human Rights (ZLHR) confirmed that this was beyond the statutory call of both ZMI and PISI. By statute, ZMI is created to gather intelligence on the armed forces and PISI to do the same on the police force. PISI, for example, is modelled around South Africa's Independent Police Investigations Directory (IPID), with an investigative obligation in relation to transgressions in the police services. Yet, in Zimbabwe, these two institutions get involved in matters they were not legally supposed to be involved in.

How did it come to this? A former high ranking government official interviewed proffered two reasons to explain how the military and police intelligence services now involve themselves in civilian surveillance. Firstly, the increasing factionalisation of the ruling party has been noted as a reason for increasing surveillance of ordinary Zimbabweans by the intelligent agencies: "You should understand that each of the three arms you mentioned – PISI, CIO and ZMI – serve different factions of the ruling party. Do not think factionalism in the party ended with the fall of Mugabe. It is even worse. I know for a fact that each of them report to different structures in government… always bid to outshine each other as the most lethal and effective…"

The respondent also said the formation of the JOC (Joint Operations Command) has resulted in increased surveillance in the country. The JOC is a combination of the heads of the military, police, intelligence and prison services with representatives from Finance ministries (Tendi 2013). JOC was created in around 2008 for greater operational coordination of the various intelligence and operational arms of intelligence. (*The Telegraph* 2008). Yet, from what respondents say, this has not been achieved because there is

no statutory instrument allowing for such an institution, (see High Court of Zimbabwe 2009). Its formation should be seen in the light of the growing role of the military in civilian governments.

The purpose of the involvement of the prison services in JOC cannot be ascertained in our interview with the former government official. "This is where surveillance is coordinated, especially by 'the core' ". Who constitutes the 'core'? "This was made up of the heads of ZMI, PISI and CIO and chaired by the Minister of State Security. It reports directly to the President. This is where serious issues of surveillance are discussed. This is also where procurement of needed equipment would be discussed…"

The targets: In all this, who are the targets of surveillance? From information gathered from respondents, five major targets of surveillance were identified. These were: journalists from both the state-owned media and the private media, civic activists, NGO heads, opposition leaders and senior ZANU PF (ruling party) officials. Pastor-turned civic activist Evan Mawarire admitted that for civic activists in Zimbabwe, "Surveillance is a serious threat because it is very much alive…"

According to respondents, surveillance of journalists and civic leaders is both digital and physical. Tawanda Mugari of the DSZ said, "For the physical surveillance, it is often men in suits, so-called C10". Natasha Msonza added, "In my belief, there are specific individuals who are more targeted than others. And these individuals predominantly constitute human rights defenders, activists and such-like persons of interest perceived as trouble makers". This is because often, civic leaders get charged by the state, relying on their private data, confirming that the state must have a way through which it is snooping on them.

A CSO activist gave some reasons why surveillance targeted opposition supporters, human rights defenders like human rights lawyers, civic leaders and many more related groups. "These are the people that will always be associated with the regime change agenda in our view, then. We also suspected them of working with foreign embassies and the opposition to effect regime change, these groups had to be monitored". It was also intimated that for the public-owned media journalists, loyalty to the new regime is important. "When the regime deposed Mugabe, it could not institute wholesale changes to the personnel in the public-owned media. But, they know they need people totally loyal to them, and these are residues of the Mugabe era and most of them are actually viewed as implants of the once-powerful Minister of Information Jonathan Moyo…" And for the private media, he said, "Obvious they have to be surveilled because they are far more dangerous… and we were always ordered to take a close look at them… it could also give us information to blackmail them or even expose them and shame them" (sic).

The Committee for the Protection of Journalists have on several occasions, called upon Zimbabwean authorities to stop harassing journalists and surveilling on them (CPJ 2008). MISA (2007) noted that the ICA was meant to make working conditions difficult for journalists in the country. Thus, all these reports point to a systematic use of surveillance laws for undemocratic purposes (see Human Rights Watch 2019).

Surveillance of public spaces in Zimbabwe

Surveillance of public spaces has, generally assumed two major trends. Firstly, it is the spaces where the public gathers that have been targeted. Secondly, it has been meetings, conferences and symposiums of suspected anti-government organisations, and individuals that have been targeted. In both cases, surveillance of public spaces has been a mixture of physical and digital surveillance.

From observations made during this research, surveillance has increasingly targeted public spaces like parks, stadiums, and public halls where people gather. These spaces have become frequently-used public spheres for the people of Zimbabwe where they meet and debate political, economic and social issues. In August 2018, the Chinese company, Hikvision, was awarded a contract by the government to install CCTV cameras in the

streets of the capital city, Harare to fight crime (The Herald 2018). These cameras have the capability of capturing faces, movements, actions and depending on location, even voices and utterances.

This is a serious violation of rights, as it interferes with the right to assembly as guaranteed in the country's Bill of Rights. People are intimidated from gathering and using a public space. From the evidence gathered, the project failed because of funding on the Zimbabwean side (News Day 2018), but not before some CCTV cameras had been installed at Africa Unity Square, in central Harare, opposite the parliament building. Here, Hikvision installed the cameras, plus night vision CCTV. Africa Unity Square is a space that has generally been used as a site of protest against the government. It is a space for anti-government rallies and gatherings (Makumbe 2009).

Mbare, a suburb in the west of Harare, has witnessed one of the highest urban crime rate in the country, but it has no cameras. This exposes the authorities' intentions in installing these CCTV cameras.

A vocal civil society, spontaneous civil protests, a collapsing economy and an increasingly ferocious opposition are likely to make the ruling regime more resolute in checking the growing tide of opposition to it even by means of extra-legal surveillance.

Chinese surveillance technologies companies have also entered into separate agreements with Zimbabweans state bodies and city councils, like the City Council of Harare for the supply of surveillance equipment. There is an official agreement between Hikvision and the Zimbabwe Republic Police (Pindula News 2018) in which the former will supply powerful night vision surveillance cameras across Harare. Drivers would be asked to install dashboard mounted cameras and upload videos of driving infractions to a Dropbox folder that the ZRP can access. ZRP claims this will curb driving violations and crime. But a technology journalist and anti-surveillance activist Ray Mwareya disagreed, "The Dropbox captures the names and emails addresses of people who upload any footage. It's a clever way of stealing people's data. The City of Harare has also joined the bandwagon. It recently announced officially that it will be installing US$2 million worth of surveillance cameras, supplied by Hikvision at traffic lights across the city (Pindula News 2018). The City's chief engineer, Mr. George Munyonga said, "The cameras will help identify traffic offenders, especially those who impede the smooth flow of traffic…The cameras will monitor all roads and parking spaces within the central business district… Installation of the network is 70 percent complete". But MISA activist Kuda Hove argues that the city has readily agreed to be part of the state's network of surveillance. "We know the data will end up in the state's hands… it's an elaborate ploy and the city has been hoodwinked into participating…".

While the surveillance of public spaces is a growing trend in Harare, there is need for a thorough investigation into whether this trend is also growing in other cities. This research was not able to check the situation in cities like Bulawayo and Mutare, which are increasingly becoming hotbeds of dissension and popular protests. One can speculate that this trend might be growing outside Harare, in other bigger cities and towns. For example, The Chronicle newspaper (23 August 2018), report that the city of Bulawayo is installing surveillance cameras on traffic lights.

Tellingly, it was observed during the course of this research that it is cheaper to import Chinese handsets as the duty is low, compared to importing Apple and Samsung products. This exposes the government's clear determination to "encourage" the importation of Chinese hardware through the manipulation of the tax system.

Digital Communication surveillance

On top of public space surveillance, digital communication surveillance has been rising fast in Zimbabwe. What forms of digital communication surveillance are on the rise, and why has digital communication surveillance increased? It is first important to assess the existing communication surveillance practices.

Prevalent digital communication surveillance techniques include email snooping using individuals who also work as journalists. There is a case that clearly demonstrates the penetrative impact of the state's digital surveillance. On 27 March 2008, the then Head of the intelligence agency CIO, Happyton Bonyongwe and his deputy Menard Muzariri, sought a High Court interdict seeking to stop The Zimbabwe Independent (27 March 2008), from publishing a story about the CIO itself, as it threatened national interests and was likely to ignite public distrust in the agency. The surprising aspect of the CIO's case was that the story had not been published. This means it had been leaked to them right from the newsroom. Zimbabwe High Court judge Lavender Makoni dismissed the case. The Independent later suspended and fired its senior reporter, Augustine Mukaro after computer experts it hired traced the leak to his email. Mukaro insisted it was a mistake he made to forward the story. His employers insisted it was deliberate. Available information says the story had not been shared in the newsroom. It was on the editor's computer, which means there was most plausibly, an orchestrated plan to snoop on the editor's desktop and get the story.

A more recent case involves a senior journalist in a state-owned newspaper who was fired after his conversations were tapped by a passenger he had picked along on his way[2]. The passenger turned out to be a member of the CIO. Another senior reporter at the public-owned broadcaster, Zimbabwe Broadcasting Corporation (ZBC) was demoted from her position and subsequently passed on when her private WhatsApp chats criticising the new government of Emmerson Mnangagwa were leaked to the public (Zimbabwe News 2018).

These incidences serve to illustrate the pervasiveness and interaction of both physical and digital surveillance in Zimbabwe. With regards to physical surveillance Natasha Msonza noted, "Physical surveillance, which is often an intimidatory (sic) tactic. For a lot of human rights defenders, their meetings are sometimes infiltrated by unidentified individuals in the proverbial suits and dark glasses. Human rights activists said they often observe unknown individuals parked outside their offices. The second prevalent is phone tapping and general interception of communications". Thus, when an individual is considered to be an anti-government activist, through frequent attendance of meetings and conferences by such groups, surveillance moves to tapping their phones – it migrates from physical to digital.

The exploitation of metadata

Some of the interviewees noted that the state has one huge advantage – its ability to access metadata without legal hindrances. The UN Office of the higher Commissioner (OHCHR) says, "The aggregation of information commonly referred to as metadata may give an insight into an individual's behaviour, social relationship, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication" (OHCHR 2017). But Zimbabwe has no metadata protection laws. This means there is no legal protection for aggrieved citizens whose data has been accessed by any organisation, be it an agent of the state or a private organisation.

State's access to metadata is not regulated by law, and therefore access to it does not require obtaining approval from any authority. As metadata can reveal a sizeable amount of private information about individuals and/or allow further information to be derived and/or inferred from it, if it is not given a sufficient level of protection, its abuse by state agencies or any other organisations can jeopardise the right to privacy.

In Zimbabwe, a SIM card is supposed to be registered using a valid National identity document and a valid proof of residence letter. Worse still, the state can push mobile network operators and Internet Service Providers to release people's metadata, especially phone numbers and residential addresses by simply requesting the data in terms of ICA Chapter 12. The 2018 incident, in which ZANU

2 The journalist confirmed the incident to the researcher. The passenger turned out to be a member of the CIO

PF send a personalised campaign message to every voter with a registered SIM in their name, raises questions about how metadata has been exploited in Zimbabwe (ZLHR 2018).

The exploitation of data and metadata for financial surveillance in Zimbabwe

There has been a growing number of incidents of financial surveillance that exploit people's financial metadata, data like addresses, phone numbers, national ID numbers, place of transaction, "biller code" of the transaction, the point from which the transaction has taken place, details of the recipient of the transaction, time, date of the transaction. Activists, pointed to the growing powers of the state in surveilling financial transactions of both individuals and organisations that challenge the state. Zimbabwe has been running a "cashless" economy since the disappearance of the US$ in about April 2016 from the formal banking system.

The most common mode of financial transactions has been through mobile network operators (MNOs), taking place on individual cellphones. The three major mobile phone providers provide such transactions are: *Econet*, with the largest subscriber base runs a facility called Ecocash; *NetOne*, the second largest MNO with a feature called OneMoney, and *Telecel*, the smallest provider, which runs Telecash. These services have grown rapidly due to the shortage of hard cash in the country. Simultaneously, these platforms have offered a huge cache of data that the state can readily tapped into to surveil organisations and individuals.

The state in Zimbabwe justifies mobile money transactions surveillance on two grounds. Firstly, the state argues that surveillance is important for ensuring regulation and tax compliance, in the process, maximising tax revenue for the state (The Financial Services Act provides for this). Secondly, the state argues that surveillance of these platforms protects citizens from fraudulent transactions, ensure that mobile money platforms are not exploited for money laundering which might promote or fund illegal activities like terrorism. Activists in Zimbabwe say these platforms have been exploited by the state for sinister surveillance. One activist from the Zimbabwe Peace Project (ZPP) noted, "We know for certain that the state monitors our financial transactions at organisational level and at individual level. They want to see who is sponsoring us".

There is no legal provision for such surveillance (of CSOs and other organisations by secret agencies as alleged by activists) under the Financial Services Act. Another respondent said transactions between ruling party supporters an opposition can be flagged too by ruling party-aligned agencies. Yet, according to the Financial Services Act, this is illegal. In August 2016, the state-owned daily newspaper, The Herald, ran a story where it revealed that prominent activist and pastor, Evans Mawarire had received huge amounts of money through his Ecocash mobile account, "to mobilise youth and destabilize the country, by hiring youth for violence and mayhem…" (The Herald 2016). How did the paper find this out? These two incidences confirm that the platform has been used to surveil individuals. This violated the Zimbabwe's Banking Act (Chapter 24; 20, Section 76 & 77). These sections in fact restrict disclosure of collected financial information. Section 13 of the Act creates an offence for unlawful use and disclosure of any financial data. Another respondent from a mobile money transfer business said, "We hand over data upon request… we have to comply…"

Two aspects have enabled financial surveillance by the state. Firstly, there is the identification mandate for mobile money customers. Secondly there is the requirement for a registered SIM. This makes it easy to track and monitor individual's transactions. This highlights a potentially dangerous function creep in mobile money transaction services – where the state extends these services for illegal surveillance on activists. The Financial Services Act, however does provide for privacy in financial transactions except in cases where suspicions of money laundering, fraud and other crimes are raised. Under those circumstances, the Reserve

Bank of Zimbabwe flags down the suspicious account(s) and report the matter to investigating authorities. That does not seem to be the case in Zimbabwe, though: intelligence agencies, working in a partisan fashion for the ruling party seem to snoop on financial transactions for political reasons. In particular, it was reported that they monitor financial transactions of NGOs, CSOs and other "marked" individual (*The Patriot* 2019).

The legal architecture of communication surveillance in Zimbabwe

Surveillance is regulated by the Interception of Communications Act (ICA) (2007), chapter 11:20 of the Zimbabwe constitution and the Postal and Telecommunication Act (PTA) (2001) Chapter 12:05.

Examples of explicit clauses on surveillance in these two acts are:

- Section 3 of ICA: IPSs to put in place the hardware and software required for the state to carry out surveillance.
- ICA Section 14: Interception would be authorised by the Minister as appointed by the President.
- Section 12:1 of PTA: Prosecutor General (a presidential appointee) can grant authority to a postal or telecommunication licensee to hand over any communication of an individual on the request of a police officer.
- Section 2 of PTA: Discretionary power of surveillance lie with the Director General of telecommunication or anyone acting in his/her place.

These are not the only problematic clauses of surveillance in Zimbabwe, but they clearly spell out how even the legal interception of communication fall far below international best practices. International best practices of surveillance require oversight by the judiciary to separate this function from the Executive, which is the entity which undertakes the surveillance activities. In the Zimbabwean case, there is too much discretion for political appointees. There is also no legal provision of an Inspector General for Intelligence, as in the case of South Africa, who can provide oversight. Zimbabwe's legislation, especially the ICA, acts contrary to internationally accepted surveillance standards which state that surveillance should achieve a legitimate aim and pursue this proportionally. It should not discriminate on language, political beliefs and other values.

Internationally accepted standards of surveillance also provide for proportionality, stating thus: Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests. This requires a state, at a minimum, to establish the following to a competent judicial authority, prior to conducting communications surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

1. there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out; and
2. there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought; and
3. other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option; and
4. information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and
5. any excess information collected will not be retained, but instead will be promptly destroyed or returned; and
6. information will be accessed only by the specified authority and used only for the

purpose and duration for which authorisation was given; and

7. that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms. (see: OHCHR 2013,17)

The state in Zimbabwe has not attempted to construct legal and institutional arrangements that balance security concerns and simultaneously buttress individual rights to privacy. The conflict between state surveillance versus civil liberties has been an enduring one. In Zimbabwe, this conflict is more manifest as there is no institution specifically created to regulate and oversee state surveillance and to take measures when it encroaches into individuals' privacy.

This has been worsened by a timid judiciary that has, over the years, progressively failed to fence off rights from the state's reach. For example, in the trial of Edmund Kudzayi, a journalist charged of espionage, the High Court allowed the matter to proceed when the accused was challenging the illegal snooping of his private data on Facebook (News Day 2014). The matter collapsed when the state failed to make available printouts of the defendant's private facebook conversations. (News Day 2014). Efforts to engage Facebook by the state failed as the organisation flatly refused to cooperate (News Day).State surveillance in Zimbabwe seems to occur without a clear legal or institutional oversight framework. The judiciary seems to defer most of the case to the Executive, without articulating clearly enough the limits of state powers when they interact with sacred rights like privacy. A good example is the recently reported Zimbabwe army intelligence-led operation "Savannah Revolution" (The Zimbabwe Situation 2019). According to CSO activists, this operation targets civilians who have been fighting for democratic space in the country. Civil society organisations allege that "Operation Savannah" is targeting them for harassment and prosecution by snooping into their communication and conversations. This surveillance operation is being led by military intelligence, which in the first place should not under be involved in civilian issues.

POTRAZ, which is tasked with oversight in telecommunications, does not seem to be actively interested in protecting individuals from illegal surveillance by state intelligence agencies. Based on the researcher's observation, POTRAZ is more focused on four main aspects of telecommunications regulation: (1) regulating the price of all forms of data provided by MNOs and ISPs, (2) monitoring the quality of voice to voice calls, (3) Ensuring compliance to the law with regards to operating licence payments and infrastructure distribution and (4) ensuring international best practices in mobile network provision. The PTA tasks POTRAZ with safeguarding individual data from misuse and abuse. But it is silent on what the organisation can do when the state or any of its organisation is involved.

Thus, the existing constitutional creature proved inadequate to the task of providing oversight on citizens' data access and its use by the state or any other players. In fact, it has proved to be Zimbabwe's state surveillance enabler rather than protector of citizens from surveillance abuse by the state.

Three incidents that happened in Zimbabwe that serves to illustrate this point.

Case 1

The first one is the arrest of five human rights activists at Robert Mugabe International Airport on charges of attempting to subvert a constitutional government. Those arrested were: George Makoni of the Centre for Community Development Trust; Nyasha Frank Mpahlo of Transparency International Zimbabwe; Tatenda Mombeyarara of the Citizens Manifesto; and Gamuchirai Mukura of Community Tolerance Reconciliation and Development Trust. The following day the authorities arrested Farirai Gumbonzvanda, a girls' rights activist and community volunteer with the Rozaria Memorial Trust. On May 27, they arrested Stabile Dewa of Women's Academy for Leadership and Political Excellence and Rita Nyampinga of the Female Prisoners Support Trust. POTRAZ agreed to assist in this regard despite having no legal standing in the matter: The police appealed to POTRAZ to assist with accessing data on the laptops and cellphones of the accused (*The Standard* 2019). In fact there is no clause providing for the provision of such a service under the PTA of 2002.

Case 2

The second one is the ZANU PF SMS scandal that happened on 27 July 2018. On this day, the ruling party ZANU PF sent an unsolicited SMS to 3 million registered voters, thanking them for voting for the party ahead of the July 30 national elections. Section 4 of the Postal and Telecommunications Act, POTRAZ requires operators to respect the constitutional right of customers to personal privacy and should not provide their subscriber databases to third parties without the consent of customers. Data protection laws should ensure that the state and companies process personal data according to certain principles and standards in order to ensure the protection of the individual and their data.

One of the standards is that this data cannot be used for marketing purposes and by other third parties without the express permission of the owners. Persons affected by the sending out of these bulk SMSs may seek legal redress as stipulated in the Postal and Telecommunication Regulatory Authority of Zimbabwe (Regulatory Circular on Unsolicited Bulk SMS) Regulatory Circular[3] No. 2 of 2013 issued in terms of the Postal and Telecommunications Act. This regulatory circular prevents MNOs from sharing consumer data with third parties without the consumer's consent. Furthermore, it prohibits sending marketing SMSs that do not give the consumer an option to opt out of receiving such messages in the future. An applicant has approached the courts for relief arguing that the ZANU-PF bulk SMS incident violated his privacy rights.

But the sending of these bulk messages raised very serious questions. Firstly, how did the party obtain this data in the first place? Mobile Network Operators (MNOs) professed ignorance, saying they did not collude to give ZANU PF people's data (Techzim 2018). POTRAZ issued a statement saying it did not. Hitherto, no explanation has been given about where the party got the database. When asked for an account, the ZANU PF secretary for legal affairs, Paul Mangwana said it was none of anyone's business. The major lesson learnt is that the ruling party can arm-twist MNOs or POTRAZ to access to people's personal data.

3 The circular can be found here: (http://www.potraz.gov.zw/wpcontent/uploads/2018/07/REGULATORY_CIRCULAR_NUMBER_ON_UNSOLICITED_BULK_SMS.pdf.

Case 3

The third incident involved a website that published the current version of the Zimbabwean voters roll in its entirety. The voters' roll on the website contained most of the personal data voters gave when they registered to vote – phone numbers and residential addresses, next-of-kin addresses and phone numbers (Techzim 2018). The website creators who identified themselves as a website, http://www.myzimvote.com/, stated that they were not sharing the voters' roll out of malice, but as a means of making information on the voters' roll accessible, and to allow voters to audit the voters' roll on their own to identify any discrepancies which would negatively affect the voting process.

There are two legal issues here, according to lawyers at the Zimbabwe Lawyers for Human Rights (ZLHR). Firstly, Section 20 of the Electoral Act states that only the Zimbabwe Electoral Commission (ZEC) is responsible for the keeping of physical and electronic formats of the voters roll. Secondly, this website is hosted outside of Zimbabwe. The-then Minister of ICT and Cybersecurity, Supa Mandiwanzira issued a statement[4] condemning the uploading of an "unprotected" version of the voters' roll. In the same statement, the Minister called for the website and its (hosting) internet service provider to "cease" the illegal publishing of the voters roll.

The minister's remarks about taking down the website or going after its host internet service provider are made in the absence of any statutory backing. A take-down request refers to the process used to compel an Internet service provider or website host to take down content from their website (MISA 2018).

4 https://www.techzim.co.zw/2018/07/supa-mandiwanzira-speaks-about-the-voters-roll-being-online-he-however-ignores-the-unsolicited-texts-from-zanu-pf-candidates/

The silence of POTRAZ in this matter is surprising for an institution created to protect individual rights. It never sought to engage the international partners to have the website taken down as it was violating the private rights of Zimbabwean individuals. For a start, it never issued a statement to condemn the violation of privacy. It should also have engaged with regulatory agencies where the website was hosted to request a take-down of the website. Take-down requests are common globally, and are resorted to when a website share content that is offensive, plagiarized, or violates privacy (see https://ispa.org.za/tdn/). Take-down requests are commonly used to remove content that is shared without proper consent or infringes on copyright. However, there has to be a law or set of laws in terms of which such takedown requests are made (MISA 2018). The failure of POTRAZ to request take-down would possibly mean it is not actively involving itself in data protection. It might also mean that as a regulatory agency, it has not developed effective relations with other international organisations to make such request. If these relations have been developed, it would have been easier for POTRAZ to request a take-down. It is commonsensical that when people's data is illegally exposed, responsible organisations should act by all means possible, act to protect citizens.

Zimbabwe's data protection laws, furthermore, give room to wanton surveillance and possession of data by any organisation with citizens having no recourse to the law. The Access to Information and Protection of Privacy Act (AIPPA) promulgated in 2002 is anachronistic for protecting citizens in the new digital age. For example, the Act protects data held by public bodies and penalises its leakage. Affected citizens, whose data is leaked by a body not considered private, cannot rely on AIPPA for redress. Section 57 of the Zimbabwe Constitution guarantees the right to privacy, but it does not articulate clearly how this guarantee is affected in the event of violation by organisations, public

bodies, and as it turns out, by the state. In this case of the bulk SMS send by ZANU PF, there is a possibility that the party may escape legal sanction because it is not considered a public body. MNOs are also not public bodies. This is a legal vacuum because it means no-public bodies cannot be sanctioned. Secondly, the law does not specify what sensitive data, which ought to be protected is.

The Cyber Crime and Cyber Security Bill[5] (2017) (see currently being discussed is not adequate because it falls short of protecting individuals from state surveillance. Instead, it criminalises the dissemination of falsehoods online, likely to cause, "fear, alarm and despondency…"

One respondent said, "The bill under discussion does not wrestle away the power of surveillance from the state, which is misusing it. Rather, it creates an unnecessarily punitive environment… It does not answer the pertinent question; how are we protected from wanton surveillance by the state... it is legal nonsense…" The Zimbabwe Democracy Centre (2019) has condemned the bill as authoritarian. There is also the weakness of the regulatory board, POTRAZ. According to lawyers, POTRAZ is weak in one major aspect – "the legal vacuum under which it operates…" (ZLHR member).

Several lawyers interviewed for this research noted that the Telecommunications Act that POTRAZ should administer is silent about what it can do when the state illegally surveils individuals. In other words, it has no legal teeth to "bite back" at illegal surveillance. "Look, when ZANU PF sent those mass messages in clear violation of telecommunication rule number 4, POTRAZ issued a tame press statement condemning MNOs and not even ZANU PF…" (ZLHR member). Another lawyer added, "Either POTRAZ is colluding with the state or it is simply weak when faced by ZANU PF which dominates the state…"

But, this is just but one of the weaknesses of POTRAZ. POTRAZ as an organisation is weak in two other respects. Firstly, it is partisan in its composition. First of all, it is important to highlight that for about a year and a half, Zimbabwe did not have this statutory board after the previous one was dissolved. No urgency was made to institute another one. This seems to indicate that the state is able to proceed with its surveillance activities without POTRAZ actually being operational.

Then, when in October 2018, the Minister of Information and Communication Technologies finally came up with the board, it was difficult to convince people that it is a non-partisan agency. The POTRAZ board is made up of 6 members: Nobert Mugwagwa, Mathews Kunaka, Charity Kadungure, Tinashe Robin Tanyanyiwa, Fradson Shavi and Doreen Sibanda.

Civic organisations like MISA had reservations. A member of the parliamentary committee on ICTs that was interviewed for this research, argued that the board is but a partisan appointment to enable surveillance because it lacks independence. For a start, most of the members of the board are related to other state institutions or had such a relationship prior to the appointment. For example, the chairperson, Nobert Mugwagwa has worked for many years in the Office of the President in various capacities. Fradson Shavi, another board member, is an appointee directly from the President's Office. Charity Kadungure works for another state entity – the Reserve Bank of Zimbabwe. Mathews Kunaka is also chairperson of another state-owned entity, the Women's Bank of Zimbabwe. This board's composition raises serious questions about its independence from the state. With almost all the members related directly or indirectly to the Executive, the ability of the board to independently oversee surveillance activities by the State and to challenge extra-legal surveillance by the state is put into question.

5 http://www.itwebafrica.com/security/887-zimbabwe/245414-zimbabwe-fast-trackscybercrimelegislation,orhttp://kubatana.net/wpcontent/uploads/2018/03/zdi_mc_cybercrime_bill_analysis.pdf

The conspicuous silence of the board in the face of civic organisations' complaints about growing state surveillance, and the lack of any input from the organisation on the Cyber Crime Bill, being debated at the time of writing, does not speak well for its independence, nor is it a positive sign of its future conduct with regards to surveillance issues.

MISA (2019) activists interviewed asserted that if the board's appointment process is not changed, there is no hope that an independent board can come into being. It is made up of bankers, economists and the only notable lawyer in the board is a notary and property attorney. There is a visible absence of data experts, surveillance experts and human rights and privacy lawyers. This raises the question: how can the board deliver its mandate with this dearth of expertise amongst members? This should worry civic organisations and privacy lawyers.

Currently, it is the minister's prerogative to appoint the board in consultation with the President. In addition to all these weaknesses, lawyers from the ZLHR said Zimbabwe needs to evolve oversight mechanisms (e.g. judicial oversight or the appointment of an Inspector General, like in the case of South Africa)to avoid unwarranted surveillance. "There is no role of the judiciary, even any other institution to referee the process, and say, "stop" (sic) that has nothing to do with crime…" Another Lawyer said, "Who will raise red flags on the state? The state is now massively loaded with surveillance technologies provided by China, Russia and Iran (see Foreign Policy 2018). People are not talking about it? … if those legal mechanisms are not evolved, then there is every likelihood that we are game (sic)…" (ZLHR member, interview in Harare, 7 May 2019).

Accounting for the ever-increasing state surveillance practices

There is evidence from numerous reports pointing to the fact that digital surveillance is increasing in post -2000 Zimbabwe (see research by Feldstein (2019 and Mwareya 2019).

Journalists, CSOs and human rights lawyers interviewed for this research presented five main factors that account for this increasing rate of surveillance. The five factors are: the availability of surveillance technology providers whose services are fairly affordable; the construction and equipping of the Robert Gabriel Mugabe School of Intelligence (RGMSI), which has institutionalised surveillance; lax and non-transparent surveillance laws and pliant judiciary and MNOs and lastly, "a sleeping and corrupt parliament" (Interview with journalist Ray Mwareya).

On 24 November 2018, the Minister of Finance, Mthuli Ncube announced that the government would use DNA and other biometric forms of identification to obtain data from civil servants, a move illustrative of the government stepping up surveillance of locals. While the drive to eliminate "ghost workers" is positive, using DNA to keep a register of workers presents a minefield of its own, and there is need to take a step back before implementing what could be a populist move, but quite detrimental to rights such as the right to privacy. The fact that the authorities want to proceed this way illustrates that they have some form of capabilities to implement that. This is, however, being done in a clandestine manner.

Zimbabwe has established access to suppliers of digital surveillance technologies. The major supplier since 2000, has been China (Quartz 2014). But, it was reported that Iran and Japan have also supplied Zimbabwe with digital surveillance equipment and grants (Quartz 2017), for the purchase of such, respectively. Yet, of all these suppliers, China has been at the forefront through its Belt and Road Initiative, a global development strategy adopted by the Chinese government involving infrastructure development and investments in 152 countries and international organizations in Asia, Europe, Africa, the Middle East, and the Americas. Hawkins (2018) notes that in all practical terms, "Zimbabwe is signing for China's surveillance state, but its citizens will have to pay the price…"

In 2016, China's surveillance technology giant CloudWalk signed a deal with the Zimbabwe government to supply mass facial recognition software and devices. This would give the Chinese company two major advantages. The first advantage is financial. Surveillance technologies come at a price. One respondent said, "We could not roll out the CloudWalk deal as fast and as widely as we wanted because of financial issues. What we did with facial recognition was more of experimental… our focus was limited… CloudWalk was demanding that we pay a lot of money and that we fulfill certain conditions first…like rolling out a nationwide, authentic registration system…" CloudWalk is assured that in Zimbabwe, they have a ready customer other than China itself.

Secondly, technology experts like Hawkins (2018) state that despite this ready market for their technologies, the Chinese now have an "experimental field". Hawkins (2018) states thus, "By gaining access to a population with a racial mix far different from China's, CloudWalk will be better able to train racial biases out of its facial recognition system – a problem that has beleaguered facial recognition companies around the World and which could give China a vital edge…" Chinese telecommunication giant, ZTE, is now the biggest supplier of telecommunication infrastructure in the country. Its mobile handsets dominate the Zimbabwean market. ZTE mobile gadgets and Huawei gadgets have for long, been suspected of leaving backdoor spyware that allows for authorities to steal private (Baig 2018). With the state-owned telecommunication company, NetOne, one of the former workers admitted that it was the state that dictated where they could source for their hardware. "And you know with our Look-East policy, it will always be China". The CloudWalk deal makes Zimbabwe one of the first countries to use this technology in Africa.

China has also been fingered as the supplier of much of the surveillance equipment at RGMSI (see: *Mail & Guardian* 2013). The RGMSI is one of the few schools of intelligence known in the region and, perhaps in Africa. It was built in 2007 by the Chinese and equipped by the Chinese. The School is situated some 40km North-West of the capital city, Harare. One respondent disclosed that the School was equipped by the Chinese using different spying technologies. The government itself has openly admitted that the country's security personnel are receiving training in digital surveillance and spying at the school, by the Chinese and acknowledged that it is preparing for cyber warfare. While officiating at the graduation of some of the security personnel trained there, the-then Commander of the Zimbabwe National Army, Valerio Sibanda said, "As an army, at our institutions of training, we are training our officers to be able to deal with this new threat we call cyber warfare where weapons [are] not necessarily guns but basically information and communication technology". (Quoted in *The Herald*, 26 August 2009). The government has acknowledged in public, and officially, that Zimbabwe and China have struck a deal under which the latter would provide surveillance training to the country's security arms, and any organisation in need of it (Former Minister of State Security, Didymus Mutasa, Question and Answer Session; Parliament of Zimbabwe 12 August 2007).

While China has been fingered as the main supplier of surveillance technologies and human resources training in the use of these technologies, some other significant players have largely been under discussed in conversations of surveillance in Zimbabwe. Iran, for example, has been reported as a major player in providing surveillance technology and equipment to the state of Zimbabwe. In 2015, Iran provided cyber-surveillance technologies to Zimbabwe (*The Herald* 2015). These included IMSI catchers for eavesdropping on telephone conversations (*The Herald* 2016). Earlier, in 2014, it was reported/evidence was published indicating that Iran had supplied to Zimbabwe spy-phone software and other programmes to monitor personal computers that was meant to be tested at RGMSI. Former President, Robert Mugabe officially thanked the Iranians, saying, "As we face regime change threats, we need an intelligence arm that is well-equipped to deal with cyber-threats

to our sovereignty…" (Quoted in an interview with The Sunday Mail, 20 September 2014). Thus, technologies of digital surveillance in Zimbabwe now rest with foreign suppliers- with China and Iran leading the pack.

However, Japan has become the latest benefactor of the surveillance state in Zimbabwe. In February 2019, it donated US$3,6 million grant to the state of Zimbabwe (*The Sunday Mail* 12 February 2019). The grant is clearly named as "Grant Aid Project for Cybercrime Equipment Supply". The Chairperson of the House of Assembly Committee on Security and ICTs, Charlton Hwende said, "Japan has not been traditionally, a country that helps in the suppression of Zimbabweans. But we now know the grant can be used for exactly such despite Japan's good intentions…"

The Zimbabwe state's blanket cyber-surveillance capabilities: Ambition versus ability

That cyber-surveillance is growing in Zimbabwe is now beyond doubt. The state is evidently determined to achieve mass surveillance/blanket on the Chinese level, (*The New York Times* 2019). Currently, there is no law providing for mass surveillance in Zimbabwe. However, such a law would not be difficult to pass. This is because the dominant player in the state, ZANU PF has a majority in parliament. It will, hence, be easy to railroad the law. Of course, there will be protests by activists and CSOs. But, ZANU PF has no history of compromising on its interests, consultation or even logrolling practices in parliament. Add to this, the absence of powerful lobbying groups in Zimbabwe's parliamentary practices, and it is easy to see how such law would be easy to pass.

Achieving blanket mass surveillance in the whole country is still further off the horizon, according to respondents. Nevertheless, the current understanding of the Zimbabwe state's surveillance practices are already wide enough and lethal enough to be a serious course of concern. Current practices are also murky, and extra-judicial, to be a serious cause of violation of privacy concerns. But, achieving blanket surveillance is not going to be an easy task for the Zimbabwean state. One respondent said, "It requires mass registration of individuals. You know our registration of individuals of IDs, and other related documents is far from perfect. Yet, this is the starting point if we were to achieve mass surveillance…" This means, surveillance may have to continue on a case-by-case basis – as it is happening currently – where journalists, political opponents, CSOs activists and other "malcontents" are targeted. The official continued, "For the technology, (mass surveillance technologies like facial recognition etc), we were quoted US$3 billion, but not to cover the whole country either, but much of it (sic)… remember this was in 2009 when we went to China… And this amount was twice or thrice bigger than our national budget".

There are also attendant problems of human labour. Surveillance still needs trained human labour, and this is also what the Zimbabwe state lacks to achieve blanket surveillance. The same respondent said, "We do not have enough trained personnel to help with digital surveillance at a national level. The few we have in the CIO I think could not do this job at national level".

Zimbabwe's state is also dogged by numerous bureaucratic inefficiencies, some of them historical ones, which greatly hinder the creation of a national registration database, a prerequisite for wide scale digital surveillance. Yet, even if the government has no financial capability (for now) to roll out a national project of digital surveillance blanketing all (*The Hustle* 2019), what already exists is highly concerning and as reported by the different primary and secondary sources presented in this study, it has been employed to devastating ends amongst opposition supporters, NGOs leaders, CSOs leaders, journalists and other outspoken citizens of the country. But, as the ruling regime totters under economic collapse, and a rising tide of political resistance it may consider a blanket surveillance system to sustain and maintain its power. Political experience has shown that when the regime's political power is challenged, its authoritarian tendencies increase.

Concluding Remarks: Towards a Rule of Law Approach to State Surveillance

It is too early to rule out the possibility of blanket surveillance and dismiss it as ambition outstripping ability. What Zimbabwe needs is a rule of law approach to surveillance. Information from collected from primary and secondary sources indicates that the current scenario has given room to wanton prying on citizens' rights in a way which is contrary to international best practices on legitimate, necessary and proportionate surveillance.

A rule of law approach to surveillance in Zimbabwe requires an "institutional metamorphosis" – the creation of strong, robust and independent institutions able to challenge the state when it transgresses legally set boundaries. It also requires the promulgation of rules and laws that fence off the state from intruding arbitrarily into individuals' privacy. But, judging by the proven intentions of the state in Zimbabwe, the creation of both institutions and legal frameworks that police surveillance does seem to be on the horizon. Contrary to this, the state is quickly embracing the Chinese model of surveillance (see: Human rights Watch 2019 comments on Zimbabwe).

Burdened by a reluctant state, what, then, should CSOs and activists do to push for surveillance law reforms? This question cannot be answered by certain prescriptions that can be adopted by activists, CSOs and interested parties. This is because Zimbabwe's post-colonial politics lacks prediction and, therefore, the reaction of the ruling elites cannot be judged with near certainty. Three approaches can be adopted by players in order to ensure Zimbabwe's surveillant state is monitored.

First of all, CSO, NGOs, political activists who have been the targets of the state extra-legal surveillance can adopt what can be termed the "litigation approach". Under this approach, they sue the state in the Constitutional Court for its illegal surveillance activities. For example, a ZLHR member, Owen Mafa[6], has sued the state, ZANU PF and the MNO, Econet for the unsolicited election message sent on his mobile device. Such acts may not guarantee legal victory for activists and concerned individuals, especially considering that the Courts in Zimbabwe have always been viewed as partisan (see Makumbe 2009; Bratton 2011 and Alexander 2013). But, constant and vigilant litigation can achieve three possible consequences. Firstly, active judicial involvement may, despite the partisan accusations of the Zimbabwe courts, be a line of defence. Secondly, if such cases are always before the Courts, the matter will not slip away from the public agenda. Keeping the surveillance debate alive is a very important step of raising awareness to the public about its real consequences. Thirdly, litigation can go a long way in exposing the porosity of Zimbabwe's surveillance legislation. This exposure is an important step in itself in speaking back against unwarranted, intrusive and illegitimate surveillance.

There is also need for concerned parties to include citizen education on the issue if they are to garner widespread support and keep surveillance debate as an important aspect in the country. A major problem is that the debate about surveillance seems, generally, to be too elitist. The "ordinary men and women" are largely divorced from this debate. Surveillance activism can gain traction if activism spreads to involve educating the public about it. Thus, organisations like DSZ, ZLHR can be centres of this dialogue. On the other hand, journalists should keep writing about it. Zimbabwean journalists operating in the country are afraid of surveillance and know its consequences. Yet are not interested in using the might of their pens to write about this

6 Case number HC305/18) filed at the High Court. The respondents contravene the provisions of the Postal and Telecommunication Regulatory Authority of Zimbabwe (Regulatory Circular on Unsolicited Bulk SMS) Regulatory Circular No. 2 of 2013 as read together with Section 4 of the Postal and Telecommunications Act Chapter 12.05 of 2000. The conduct of the respondents was therefore unlawful and should be declared as such.

and make the public aware of it. It is rather ironic considering that most of them, whether in the state-owned or private media, testified that surveillance is a lived reality among them. Perhaps, not writing about it is a culmination of this fear?

Finally, there is need to undertake further research in Zimbabwe to establish how CSOs, NGOs, and independent activists can be empowered to be useful lines of defence against the ever-growing surveillance powers of the state. Building capacity for resistance is an important aspect of fighting illegitimate surveillance prevalent in the country. For now, it should be known that the state keeps expanding its surveillance capabilities, and the Chinese have proved central in the provision of the technology that the Zimbabwe state desperately wants. Consequently, Zimbabwe keeps drifting towards darkness.

Recommendations

In this section, we make recommendations based on the findings outlined in this report.

The Parliament of Zimbabwe

- It is recommended that the parliament of Zimbabwe take a more active role in matters of surveillance. It can do this by scrutinizing further legislative processes of laws which interfere with the right to privacy and other fundamental rights, and refusing to ratify laws that violate human rights like privacy. Secondly, parliament is empowered by the constitution to hold hearings with organisations and individuals if cases of surveillance and violation come up, like they frequently do in Zimbabwe. The failure of parliament to act in this regard is a failure of its constitutional duties.
- Moreover, it is recommended that parliament pass a motion to codify surveillance laws in Zimbabwe. Currently, there is not specific code of law- a consolidated act that covers all forms of surveillance. The state relies on a variety of clauses scattered across the whole constitution. This has made it difficult for anyone to challenge surveillance laws as this might mean challenging the whole constitution or, at least, many of its provisions. This is a daunting task in a legal environment where the courts are viewed as biased and pro-regime.
- Parliament is recommended to quickly reign in on POTRAZ so that it play its statutory duties, and not aid the state in criminal investigations. There is no such provision in its enabling act.
- Parties in parliament should move ahead and table a Private Member's Bill that regulates surveillance and keep the state and its agencies in check. The Bill has been mooted recently, but no progress has been made so far.

The Zimbabwean Executive

- It is recommended that the state should reform its surveillance laws to meet internationally accepted standards of proportionality, transparency etc.
- The state should also move fast to ensure a legal provision providing for an oversight mechanism that would curb illegal surveillance by state institutions. Zimbabwe needs, therefore, to strengthen its surveillance legislation and oversight mechanisms so that they comply with international best practices of surveillance and individual privacy.
- The authorities in Zimbabwe needs to create strong and independent oversight institutions to ensure that state surveillance is subjected to independent oversight, and that it adheres to the Section 57 of the Zimbabwe Constitution which guarantees the right to privacy.

- The state is urged to engage in meaningful dialogue with CSOs and other interested parties in order to reform the laws governing surveillance.
- It is recommended that those agents who had served the Mugabe regime, and had acquired a notoriety for brutality should be retired from active service. In neighbouring South Africa, a Presidential Commission has recommended a massive reorganization of the State Security Agency. Zimbabwe needs one too.
- The state is recommended to retrain 'new men and women' oriented to the right to privacy and other fundamental rights.

The Zimbabwe media

- It is recommended that the media in Zimbabwe report more frequently on matters of state surveillance, in order to contribute to the agenda -setting and to educating the public.
- Reporting frequently on surveillance exposes the state, and exposure is a way of resisting the surveillance state. More so, it keeps the matter alive amongst policy makers. There are, disappointingly, few cases of such reportage in the media in Zimbabwe. This comes at a time when digital surveillance of opposition, journalists, CSOs, and NGOs is increasing[7]. At the time of writing this report, The Independent (14 June 2019) was reporting that military intelligence agencies had launched a targeted surveillance operation that targets journalists and civic organisation leaders[8]).

7 (follow: http://zimbabwe.misa.org/2018/09/15/zimbabwe-government-steps-up-surveillance-efforts/ and http://zimbabwe.misa.org/privacy-and-surveillance/).

8 (see: https://www.theindependent.co.zw/2019/06/14/civil-society-activists-on-military-watch-list/

Civil Society Organisations (CSOs)

- It is recommended that CSOs should evolve clear responses to counter the growing practice of state surveillance. They should, in addition, continue to mobilise and challenge the state and its institutions of surveillance.
- There is also need for CSOs to keep challenging through increasing litigation, the laws governing surveillance. In Zimbabwe, debates on surveillance are deemed politically sensitive and dangerous. Such narratives are often followed by a spiral of silence if raised in the public. CSOs should, in light of this, concientise the public, such that discussions on surveillance are entrenched in everyday public narratives. CSOs should continue advocating for, (1) changes in the state's surveillance practices in ways that make surveillance abide by international practices of transparency. (2) A legal framework that creates protective clauses buttressing and maintaining individual rights of privacy.
- They should also expose organisations, state agencies and any other institutions that collude with the state in its extra-legal surveillance activities.

The Regulatory agency – POTRAZ

- Members of the POTRAZ board are urged to maintain their independence from the state and not be willing instruments in the violation of individual privacy rights, having the constitution (which originated the agency itself) as a guide.

References

Adey, P. (2012). "Borders, identification and surveillance". In; Ball, L., Haggerty. K.D., and Lyon, D. (Ed), *Routledge handbook of surveillance studies*. London: Routledge; pp.193–208.

Agar, J. (2003). *The Government Machine: A Revolutionary History of the Computer.* Cambridge: MIT Press.

Baig, C.E. (2018). "Spy games: Is buying a Chinese smartphone risky?" In; *USA Today*, March 12, 2018. Accessed`at;https://www.usatoday.com/story/tech/columnist/baig/2018/02/27/chinese-espionage-huawei-zte-congress/356095002/ Accessed on 28 February 2019.

Ball, K., Lyon, D. and Haggerty, K.D. (eds). (2012). *Routledge handbook of surveillance studies*. London: Routledge.

Bennett, C.J. (2012). Privacy advocates, privacy advocacy and the surveillance society. In; Ball, L., Haggerty. K.D., and Lyon, D. (Ed), *Routledge handbook of surveillance studies*. London: Routledge; pp.412–419.

Bentham, J. (1791). *Panopticon*. Dublin: T. Payne.

Bond, P., & Manyanya, P. (2007). Competing explanations of Zimbabwe's long economic crisis. *Safundi: The Journal of South African and American Studies*, 8(2), pp.149–181.

Bulawayo News 24 (2013). 'Identity card surveillance coming'. Accessed at; https://bulawayo24.com/index-id-technology-sc-internet-byo-131135.html. (Accessed on 4 May 2019).

Ceyhan, A. (2008). "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics". *Surveillance & Society*, 5(2): 102–23

CPJ., (2008). 'Zimbabwe authorities should stop harassing journalists'. Accessed at; https://cpj.org/reports/2008/06/zim08.php. (Accessed at 5 May 2019).

Detrixhe, J. (2018). "The US is worried about China spying via Huawei because it did the same in the past". In; *The Quartz*, 10 December 2018. Accessed at; https://qz.com/1489707/the-us-is-worried-about-china-spying-via-huawei-because-it-did-the-same/. Accessed on 12 May 2019.

Digital Society of Zimbabwe. (2016). "Computer crime and Cybercrime in Zimbabwe Report". Accessed;http://crm.misa.org/upload/web/Computer%20Crimes%20&%20Cyber%20Crimes_Framework_Zimbabwe.pdf. Accessed on 10 March 2019.

Dubrofsky, R.E. and Magnet, S.A. (eds). (2015). *Feminist surveillance studies*. London: Duke University Press.

Duncan, J. (2014). *Communications surveillance in South Africa: the case of the Sunday Times newspaper*. Global Information Society Watch: Communications surveillance in the digital age.

Duncan, J. (2016). Is South Africa reverting to a repressive state? *Under Pressure, Shrinking Space for Civil Society in Africa*, p.18.

Duncan, J. (2018). "Taking the Spy Machine South: Communications Surveillance in Sub-Saharan Africa". In: *The Palgrave Handbook of Media and Communication Research in Africa* (pp. 153–176). Cham: Palgrave Macmillan.

Elmer, G. (2003). "A diagram of panoptic surveillance". *New Media & Society*, 5(2), pp.231–247.

Fernandez, L.A. and Huey, L. (2009). "Editorial. Is resistance futile? Thoughts on resisting surveillance". *Surveillance & Society*, 6(3), pp. 198–202.

Flaherty, D. H. (1989). *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press.

Foucault, Michel. (1977). Discipline and Punish: The Birth of the Prison, translated by A. Sheridan, New York: Vintage

Giddens, A. (1990). *The Consequences of Modernity*. Cambridge: Polity

Haggerty, K. (2006). "Tear down the walls: On demolishing the panopticon". In D. Lyon, D. (Ed.), *Theorising surveillance: The panopticon and beyond*. Uffculme, Devon: Willan Publishing.

Haggerty, K.D. and Ericson, R.V. (2000). "The surveillant assemblage". *British Journal of Sociology*, 51(4), pp. 605–622.

Hawkins, A. (2018). "Beijing's Big Brother Tech Needs African Faces: Zimbabwe is signing up for China's surveillance state, but its citizens will pay the price". In: *Foreign Policy*, 24 July 2018. Accessed at; https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/. Accessed on 12 January 2019.

Higgs, E. (2004). *The Information State in England: The Central Collection of Information on Citizens Since 1500*. Basingstoke: Palgrave Macmillan.

High Court of Zimbabwe (2009) 'Mudzuri versus the state'. Accessed at: http://www.veritaszim.net/sites/veritas_d/files/Mudzuru%20%26%20Another%20v%20Minister%20of%20Justice%20%26%202%20Ors%20%20Applicants%27%20Heads%20of%20Argument.pdf. (Accessed on 4 February 2019).

Human Rights Watch., (2019). 'Ramaphosa cannot stay silent on Zimbabwe'. Accessed at; https://www.hrw.org/news/2019/01/23/ramaphosa-cannot-stay-silent-zimbabwe.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. UK: McGraw-Hill Education.

Mail & Guardian., (2018). 'Zimbabwe army blamed for post-election fatalities'. Accessed at; https://mg.co.za/article/2018-12-18-security-forces-to-blame-for-zim-post-election-fatalities.

Makumbe, J. (2009). *The impact of democracy in Zimbabwe: assessing political, social and economic developments since the dawn of democracy*. Harare: UZ Publication office.

Mare, A. (2016). "A qualitative analysis of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa". South Africa: *Media Policy and Democracy Project*.

Marx, G.T. (2002). "What's New About the 'New Surveillance'? Classifying for Change and Continuity". *Surveillance & Society*, 1(1), pp.9–29.

Mitchell, A and Diamond, L. (2018). "China's Surveillance State Should Scare Everyone. The country is perfecting a vast network of digital espionage as a means of social control—with implications for democracies worldwide." In; *The Atlantic*, 2 February 2018. Accessed at; https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/. Accessed on 23 March 2019.

News Day. (2018). 'Harare residents up in arms against traffic cameras'. Accessed at; https://www.zimeye.net/2018/10/25/harare-residents-up-in-arms-against-traffic-control-cameras/ (Accessed on 10 February 2019).

'Baba Jukwa bid for freedom hits snag'. Accessed at; https://www.newsday.co.zw/2014/09/baba-jukwa-case-editors-discharge-bid-fails/) (Accessed on 12 December 2019 News Day.,(2014).).

Norris, C. (2012). The success of failure. In Ball, L., Haggerty. K.D., and Lyon, D. (Ed), *Routledge handbook of surveillance studies*. London: Routledge; pp.387–410.

Pindula News., (2018). 'City of Harare to install 2 million traffic cameras'. Accessed on: (https://news.pindula.co.zw/2018/10/25/the-city-of-harare-to-install-2-million-traffic-cameras-at-all-intersections/. (Accessed on 12 December 2018).

Quartz Africa., (2014). 'Beijing exporting facial recognition to Africa'. Accessible at: https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/. (Accessed 4 March 2019).

Report of the High Commissioner for Human Rights on the right to privacy in the digital age A/HRC/27/37 (2016. Accessible at; https://necessaryandproportionate.org/principles (Accessed on 13 February 2019).

Schulhofer, S. J. (2002). *The enemy within: Intelligence gathering, law enforcement, and civil liberties in wake of September 11*: New York: twentieth Century Fund

Swart, H. (2011). "Secret State: How the Government Spies on You". *Mail and Guardian*, 14 October 2011. Accessed at: mg.co.za/article/2011-10-14-secret-state. Accessed on 12 February 2019.

Techzim (2019). 'Econet denies selling people's private data. Accessed at; https://www.techzim.co.zw/2018/07/econet-denies-selling-customers-data-to-3rd-parties-refutes-zecs-allegations-so-who-sold-data-to-zanu-pf/) (Accessed on 12 September 2019).

The Business Live., (2019). 'EU recommends more sanctions on Zimbabwe'. https://www.businesslive.co.za/bd/world/africa/2019-02-15-eu-recommends-more-sanctions-against-zimbabwe/. (Accessed at; accessed on 2 May 2019).

The Economist., (2007). 'Africa is attracting interest from powers elsewhere'. Accessed at; https://www.economist.com/briefing/2019/03/07/africa-is-attracting-ever-more-interest-from-powers-elsewhere. (Accessed on 14 August 2018).

The Herald., (2018). 'Surveillance cameras for Harare'. Accessed at; https://www.herald.co.zw/2m-surveillance-cameras-for-harare/. (Accessed on 16 March 2019).

The Hustle (2019). 'China's surveillance loan'. Accessed at; https://thehustle.co/china-surveillance-business-loan/ (Accessed on 12 February 2019).

The Independent., (2008). 'High court dismisses CIO application'. Accessed at: https://www.theindependent.co.zw/2008/03. /27/high-court-dismisses-cio-application-on-zimind-story/. (Accessed on 2 February 2019).

The Independent., (2013). 'CIO steps up mass citizen surveillance'. Accessed at; https://www.theindependent.co.zw/2013/08/30/cio-steps-up-mass-citizen-surveillance/ (Accessed 3 March 2019).

The New York Times (2019). 'China's racial profiling technology'. Accessed at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (Accessed on 23 May 2019).

The Patriot., (2019). 'Regime change agenda exposed'. Accessed at; https://www.thepatriot.co.zw/old_posts/civil-society-and-regime-change-in-2019. (Accessed on 13 March 2019).

The Telegraph (2008). 'Zimbabwe generals have taken over Mugabe's powers'. Accessed at; https://www.telegraph.co.uk/news/worldnews/africaandindianocean/zimbabwe/2080992/Zimbabwean-generals-have-taken-Robert-Mugabes-power.html. (Accessed on 5 March 2019).

The UN Office of the higher Commissioner (2013). 'Privacy in the digital age report'. Accessed at;(https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx) (Accessed on 2 March 2019).

The Zimbabwe Mail (2019). 'Charamba loyalist targeted in fresh round of purges'. Accessed at: https://www.thezimbabwemail.com/editors-memo-pad/charamba-loyalists-targeted-in-fresh-round-of-purges-at-the-herald/. (Accessed on 12 March 2019).

The Zimbabwe News., (2018). 'Leaked WhatsApp messages blamed for Judith Makwanya's death". Accessed at; https://zwnews.com/leaked-zbc-whatsapp-chats-insulting-ed-blamed-for-judith-makwanya-death/. (Accessed on 3 March 2019).

Weller, T. (2010). *Information History in the Modern World: Histories of the Information Age*. Basingstoke: Macmillan Palgrave

Zimbabwe Lawyers for Human Rights. (2016). "Enforced disappearances – An information guide for human rights defenders and CSOs." Accessed at https://www.zlhr.org.zw/wp-content/uploads/2016/10/Enforced-Disappearances-An-Information-Guide-for-Human-Rights-Defenders-and-CSOs.pdf. Accessed on 12 March 2019.

Zimbabwe Peace Project. (2009). *Peace Monthly Report*: November 2009. Harare. Zimbabwe Peace Project Printers

Zimbabwe News, (11 May 2019). Charamba loyalists demoted, http://zimbabwe.shafaqna.com/EN/AL/483271

Zimbabwe Situation., (2019). 'Civil society leaders under military watch list'. Accessed at; Accessed on 23 May 2019) https://www.zimbabwesituation.com/news/civil-society-activists-on-military-watch-list/ (Accessed on 2 May 2019).

Zuboff, S. (2018). *The age of surveillance capitalism: the fight for the future at the new frontier of power*. London: Profile Books.