Communications & Political Intelligence Surveillance on Human Rights Defenders in Zimbabwe

A Research Report

(Year 1)

By

The Zimbabwe Human Rights Forum

In Collaboration with

Privacy International (PI) and the International, and

Research Development Center (IDRC) of Canada

Under the Surveillance and Freedom: Global Understandings and Rights Development (SAFEGUARD) project (2013-14)

Acknowledgements

The Forum would like to extend its thanks to Privacy International (PI) and the International Development Research Centre (IDRC) for their support and collaboration. In the course of carrying out the research in year 1, the Forum also received unwavering support and collaboration from various civil society organisations and individuals based in Zimbabwe. While we cannot mention all the parties' names, we would like to thank all of them for their assistance and kindness. This report could not have been completed without their participation. Last but not least, we would also like to thank the Global Community of privacy advocates especially the 'Necessary & Proportionate' Principles and the Web We Want groups, colleagues at the United Nations Human Rights Council especially Frank Larue, and colleagues who participate at the African Commission NGO Forum in particular IHRDA for creating discussion forums during the course of this research. Most importantly, we would like to particularly thank the dedicated team of research associates for their immense contribution to this project. These include Nausica Castanas, Dorothy Mudavanhu, Anna Wilton, Charlie Blagbrough, and Joseph Morgan and finally Lindani Chirambadare for coordinating advocacy efforts.

Arthur Gwagwa, Research Coordinator
The Zimbabwe Human Rights Forum (The "Forum")

Table of Contents

List of boxes

List of acronyms

ACHPR – African Commission on Human and Peoples' Rights
AIPPA – Access to Information and Protection of Privacy Act
AU – African Union
BAZ – Broadcasting Authority of Zimbabwe
BSA – Broadcasting Services Act
CAT – UN Convention Against Torture
CGS – Military Intelligence
CIO – Central Intelligence Organisation
CLCRA – Criminal Law (Codification and Reform) Act
CODE – Criminal Law (Codification and Reform) Act 2004
CP&E – Criminal Procedure and Evidence
CSU – Counselling Services Unit
ERC – Election Resource Centre
EU – European Union
FISB – Federal Intelligence and Security Bureau
GPA – Global Political Agreement
HRDs – Human Rights Defenders
ICA – Interception of Communications Act
ICCPR – International Covenant on Civil and Political Rights
IRDC – International Research Development Center
IAP – Internet Access Provider
ISPs – Internet Service Providers
JOC – Joint Operation Command
LHC – Lancaster House Constitution
MDC – Movement for Democratic Change
MDC-T – Movement for Democratic Change
MI – Military Intelligence
MIC – Media and Information Commission
MICC – Monitoring and Interception of Communications Centre
NANGO – National Association of non-governmental Organisations
NGOs – Non-Governmental Organisations
NPI – Nikuv Projects International
NSC – National Security Council
NYDT – National Youth Development Trust

PAIA – 2001 Protection of Access to Information Act
PI – Privacy International
POPI – Protection of Personal Information Bill
POSA – Public Order and Security Act
RICA – Regulation of Interception of Communications Act 2002
SADCOPAC – Southern Africa Development Community Organisation of Public Accounts Committees
SAHA – South African History Archive
SAHRC – South African Human Rights Commission
SI – Statutory Instrument 142 of 2013 on the Postal and Telecommunications (Subscriber Registration) Regulations
UCRN – University College of Rhodesia and Nyasaland
UN – United Nations
US DOS – US Department of State
YIDEZ – Youth Initiative for Democracy in Zimbabwe
ZANU-PF – Zimbabwe African National Union-Patriotic Front
ZAPU – Zimbabwe African People's Union
ZDF – Zimbabwe Defence Forces
ZESN – Zimbabwe Election Support Network
ZIM-RIGHTS – Zimbabwe Human Rights Association
ZLHR – Zimbabwe Lawyers for Human Rights
ZPP – Zimbabwe Peace Project
ZRP – Zimbabwe Republic Police

1. Introduction

Internet privacy, and, by extension, the right to privacy have recently come in focus internationally after multiple reports of mass surveillance. These surveillance practices pose a clear threat not only to the enjoyment of the rights to privacy and free expression of millions of Internet users across the globe, but also to the very existence and proper functioning of the Internet.

This trend to monitor people's Internet usage and online presence is also seen in developing countries such as Zimbabwe, where there has been an unchecked rise in state surveillance and censorship of all types of communication. In October 2013, the Zimbabwean Government extended its reach into the private lives of its citizens by promulgating a new law establishing a central database of information on all mobile telephone users in the country, thereby raising new challenges to the already embattled right to privacy and freedom of expression in the country[1]. It increases the potential of this admittedly repressive state to spy on its citizens and further clamp down on free speech.

The current rise in digital surveillance is, in many ways, simply an extension of the monitoring that political activists and Human Rights Defenders (HRDs) face in their everyday life. Extensive monitoring occurs despite the fact that, in theory, Zimbabwe enjoys an extensive set of constitutional rights.

The main challenges in protecting and promoting the right to privacy stem from the state's legal and technical surveillance capabilities, lack of domestic and regional judicial oversight as well as the fragmented international framework.

At a time when the international community is trying to take steps to ensure the Internet remains a relatively decentralized, open and free space, where human rights and in particular, the right to privacy are respected and upheld, it is imperative for the Zimbabwean Government to collaborate with IAPs, ISPs, CSOs and the private sector that are supplying surveillance technology or using communications technologies for surveillance purposes to ensure they all appreciate the human rights implications.

1.1. Research Questions

The central issue of this research is the extent to which Zimbabwe's current state of policy and practice on political intelligence and communications surveillance of particular social groups perceived to be opposed to the Zimbabwean Government interests (thereafter called Human Rights Defenders or HRDs) breach the right to privacy. What gaps, if any, are there in bringing the current policy, legislative and practice frameworks in line with international standards and norms, and other comparable national and regional regulatory standards that exhibit best practice?

A close examination of the above issue results in the following research questions, which this report seeks to answer:

The legal and constitutional landscape: What laws and constitutional provisions exist to protect privacy in theory? How are they implemented and monitored, and where are the legal and policy gaps?
Communications surveillance: What communication surveillance regimes are in place? How are they designed in theory including law and how do they operate in practice?
Adoption of surveillance technologies: Where is the Zimbabwean Government buying surveillance technologies from, and how are these used? What legal regimes are there in place to establish safeguards over the use of advanced surveillance technologies? What is the state of the art in legal protections?
Political intelligence oversight: What is the nature and operation of local intelligence services? What oversight mechanisms are in place, and how can these mechanisms be implemented or enforced?

1.2. Methodology and Structure of the Report

This part aims, firstly, to explain the inclusion of the various literatures that inform the analysis, and to describe the approach taken to the literature review chapters. Although the research focuses on the Zimbabwean context, the project calls upon some international studies.

The report is split into two parts: *Part* I, running from Chapters *3 to 5,* makes up the literature review, which inform the key findings in *Chapter 2.* The field research is then presented in *Part II*, which is made up of *Chapter 6*.

The literature review seeks to establish how the notion of privacy is understood in international law and practice by briefly reviewing the international literature on privacy, the relevant regional and international treaties and conventions, the constitutions of nations such as South Africa, and the jurisprudence of courts across the democratic world. It is followed by a review of the existing literature on Zimbabwe's national laws, regulations, practices and safeguards relating to political intelligence oversight and communications surveillance. The literature review process made use of national and international sources, including reports by Zimbabwean civil society as well as international human rights organisations and foreign Governments that document the Zimbabwean human rights situation. The review focuses on political, surveillance and communication interception, relating to HRDs and other groups that are opposed—or perceived to be opposed—to the Government.

The latter is based on interviews and focus groups undertook in Zimbabwe over the summer of 2013 and plays a twin role: it fills in the gaps identified in the literature review and, through the course of the research, sensitises and trains interviewees on the issue of privacy. A summary of the empirical findings is presented in *Chapter 6* and an example of the questionnaire that guided the interviews is presented in *Appendix 1*.

In 2014, the third part of this project will focus on advocacy in Zimbabwe, with the intended aim of bringing about policy and practice reforms.

The scope of the topic meant that no single discipline yielded the required body of knowledge. It was therefore necessary for the literature review to be inter-disciplinary, and reflective of the many facets of this broad area.

1.3. Hypotheses

Early in the research, based on our early findings we hypothesised that we would find significant evidence of invasion of privacy in Zimbabwe at home, at work and within the community in literature. This was subsequently confirmed in the course of the research.

We believe that the production of this report and most importantly the interviews carried out all have the potential to sensitise the audience to issues of privacy as a human right and therefore promote its effective safeguard.

---

[1] Mushava, E. 2013. "Zimbabwe Govt Starts Spying On Cellphones". Retrieved December 11 from http://www.zimeye.org/zimbabwe-govt-starts-spying-on-cellphones%E2%80%8F/

PART I – LITERATURE REVIEW

2. Key findings and recommendations

2.1. Findings

Finding 1: The right to privacy is protected in numerous international covenants and declarations, as well as national constitutions, and is safeguarded by international law

Finding 2: Increasingly, online communications are included in definitions of the right to privacy, and the damaging role of modern communication technology in the protection of this right is being discussed

Finding 3: The right to privacy is interlinked to other human rights according to these same treaties, and most importantly, the freedom of expression

Finding 4: The right to privacy can be undermined because of a number of legislations, such as national security, access to information, emergency and public order—these concerns are internationally considered overriding to the right to privacy. In practice, they are often used to discriminate against HRDs and strip them of their rights. It often allows for impunity of HR violators

Finding 5: Internationally, the practice of the protection of the right to privacy in Zimbabwe is considered problematic at best, particularly vis-à-vis HRDs. While there are significant improvements, legislations that undermine the right to privacy and protect violator against legal action

Finding 6: In Zimbabwe, violations of the right to privacy include throttling of mobile service such as bulk texts, cyber attacks against government critics including subjection to distributed denial of service attacks, and use of sponsored government agents to manipulate online discussions that are critical to the government.

Finding 7: Like the GPA before it, the new constitution that came into force in May 2013 guarantees the rights to privacy, freedom of expression and the press. Nevertheless, the existence of legal instruments which directly contradict these constitutional guarantees prevent the realization of these rights in practice

Finding 8: The biggest obstacle to the effectiveness of the constitution is the lack of judicial oversight that accompanies conflicting provisions. The ruling party's tendency of taking extra-legal actions against Zimbabwean citizens is supported by the high level of executive power, which accompanies existing legal instruments

Finding 9: Powers of surveillance are most commonly used as a means of smothering freedom of expression. Journalists and HRDs are most frequently targeted with the aim of preventing the circulation of comment and information critical of the state

Finding 10: Surveillance and censorship tend to increase during periods of high political activity. As demonstrated during the July 31 elections, the impact of this is to directly undermine the democratic process in Zimbabwe

Finding 11: With technological access increasing rapidly for the population of Zimbabwe, state security officials are responding by attempting to racket up their surveillance capabilities to cover new methods of communication. For example, investigative reports have revealed the enlistment of Chinese and Iranian agencies to help boost the possibility for cyber-surveillance

Finding 12: Recent legislation passed by the newly elected ZANU-PF administration has been focused on wide scale data-gathering. Such an approach is in danger of enabling unconstitutional and arbitrary mass surveillance if not checked by appropriate legal safeguards

Finding 13: Examining the measures taken in South Africa to protect the right to privacy highlights several points that could inform Zimbabwean privacy protection in the future

Finding 14: The South African Constitution outlines not only the broad concept of “a right to privacy”, but also the specific elements of daily life that must be protected in order to guarantee this right. The definition includes the freedom to go about activities for which many HRDs in Zimbabwe are currently persecuted

Finding 15: Explicitly guaranteeing the protection of such rights is an extremely important step towards protecting against their abuse or curtailment, and as such this is one area in which South Africa can be seen to offer a positive example

Finding 16: It is also evident that a number of obstacles have hindered South Africa’s ability to protect these rights in practice. Although on the face of it attempts have been made to formally regulate violations of the right to privacy, acts such as the RICA and the Protection of State Information Bill have a tendency to place state interests above those of individuals, whilst potentially beneficial acts like PAIA are crippled by inefficient systems that hinder their implementation

Finding 17: External influences have had a positive influence in South Africa. The forthcoming implementation of the POPI, which has been produced with extensive reference to existing EU legislation, is a large step towards addressing the privacy threats created by the increasingly frequent transferal of digital personal data

2.2. Recommendations

Consequent upon the above findings, we submit the following recommendations:

Recommendation 1: There should be a clear framework—both political and legislative—protecting against violations of the right to privacy; eroding this right should not be as easy as it presently is, when other national concerns are considered more pressing

Recommendation 2: This framework should be reinforced by rigid and effective enforcement against violations, as well as accountability for violators

Recommendation 3: The Zimbabwean Government should follow recommendations by the international community to enshrine the right to privacy in its Constitution, and provide a solid basis to fight impunity

Recommendation 4: National laws that infringe upon the right to privacy, such as the POSA, the AIPPA and the BSA, as well as the general existing legal framework, which is conducive to the violations, should be thoroughly reviewed and even repealed, as recommended by Norway

Recommendation 5: Politically motivated violations of the right to privacy should be criminalised, and political opposition should be tolerated, both in theory and practice

Recommendation 6: Constitutional limitations on the right to privacy must be sufficiently clear and precise. For example this would not allow for the 'general public interest' to be included as a limitation on privacy, since it is far too broadly worded therefore risks being abused

Recommendation 7: Existing legislation needs to be a reviewed in terms of its compatibility with the new constitution of 2013. Consequently, incompatible legislations should be either reformed in line constitution or scrapped

Recommendation 8: Constitutional limitations on the right to privacy should be interpreted as narrowly as possible unless and until Zimbabwe's laws are made compatible with the constitution.

Recommendation 9: All powers of surveillance granted by legislation must be subjected to a high level of judicial oversight. This will prevent the arbitrary and unlawful abuse of these powers at risk by allowing for excessive executive discretion. It will allow for the constitution to develop as a living instrument, and thus to become more effective

Recommendation 10: Zimbabwe should follow South Africa's example and outline different aspects of the right to privacy in everyday life, instead of using a general definition which makes it harder to prosecute violations

Recommendation 11: When considering how best to protect privacy in Zimbabwe, it is important to note firstly that legislation must strike a careful balance between the security needs of the state and the need to protect the rights of citizens, and secondly that administrative and judicial systems within the country must be robust enough to support the legislation. To that end Zimbabwe could re-model its legislation based on the International Principles on the Application of Human Rights to Communications Surveillance, which embodies international human rights law

Recommendation 12: Zimbabwe should take similar steps to South Africa to combat threats to individual privacy, using the positive influence of the EU and other supranational organisations

Recommendation 13: Zimbabwe should adopt measures to increase the efficacy of supranational bodies like the ACHPR which, neither explicitly seek to protect a right to privacy nor provide the African Commission with powers to effectively deal with state violations, thus placing the onus for redress on individual states

3. Some working definitions

3.1. How are privacy and the right to privacy defined?

As with most terms in international relations and development, the right to privacy does not have a single agreed upon definition. In it simplest terms, the right to privacy is the "right to be left alone", which, in the late 19th century, future U.S. Supreme Court Justice Louis Brandeis branded the "most cherished freedom in a democracy"[1]. It is important to note that privacy extends to privacy online, as a person's online communication should enjoy the same privacy status as all other types of communication. In particular, we can distinguish between four main aspects of privacy: *information privacy*, which involves all personal and sensitive data, *bodily privacy*, that is of the physical self, *privacy of communications*, including phone, mail and email, and lastly *territorial privacy*, which concerns one's home and work environments[2].
The right to privacy has only grown more complex in the twentieth century, involving many different spheres of an individual's life such as family and home life, work life and community life, as well as a non-negligible psychological factors, which include aspects like intellectual freedom, reputation and honour, etc.[3] An umbrella definition will therefore be used for the scope of this report. Privacy can be understood as:

> […] the right to control who knows what about you, and under what conditions. The right to share different things with your family, your friends and your colleagues. The right to know that your personal emails, medical records and bank details are safe and secure. Privacy is essential to human dignity and autonomy in all societies. The right to privacy is a qualified fundamental human right[4].

Before the commencement of the project, we carried out a scoping exercise by searching through, law reports and interview clips of Zimbabwean HRDs, and we realised that, although the right to privacy is sometimes construed in its narrow sense, it is often interpreted liberally, especially in connection with the work of HRDs. This approach tends to fit into the definition of "the right to be left alone". We went through various reports and found diverse variations of this phrase, for example *operating space* and in particular in her interview with SW Radio, in the wake of the indictment of the Zimbabwe Human Rights Forum Director, Irene Petras mentioned that, "the state did not want to leave [us] alone to continue with our work". References to this are also found in subsequent numerous reports on the police clampdown on civil society organisations.

3.2. How are HRDs defined?

Here again, there exists no single definition for HRDs. In 2005, Hina Jilani, the then United Nations Special Representative of the Secretary-General on Human Rights Defenders, specified that the term needed to be broad enough that it did not limit itself to those working in organisations promoting human rights. She famously said that "anybody participating in a peaceful demonstration championing a human rights issue is a human rights defender"[5]. The official position of the UN since has been one of integration, continuously broadening the scope of the term. Margaret Sekaggya, the current Special Rapporteur on the situation of HRDs, even includes Governments and their members of staff in the definition, stating that, by upholding and promoting their human rights obligations and combatting impunity for human rights violations, they effectively act as HRDs[6]. Given the peculiarities of Zimbabwe, however, it would be imprudent to include the national Government in the definition.

In Zimbabwe, stemming from the absence of rule of law, political activists are routinely targeted by the ZANU-PF, President Mugabe's ruling party. However, intimidation is not limited to supporters of the MDC, the opposition party; all those promoting human rights in the country are perceived as opposing the status quo and thus the Government and are therefore also persecuted. It follows that numerous activities, far from limited to political dissent, are considered disruptive and attract the attention of the security forces[7]. Accepting this fact, a general categorisation of the different groups of HRDs in Zimbabwe arises. For this report, we will accept the categorization of HRDs proposed by Frontline Defenders in their 2010 report.

Protestors are at risk of persecution; participating in a public protest in Zimbabwe carries inherent risks. There are reports of protests being filmed, leading to the arrest of protestors shortly after[8].

Rural and small-town activists are also in danger. Members of civil society organisations have to deploy measures to stay safe. Nevertheless, these organisations also work on volunteer basis and many of the activists from rural areas and smaller towns are isolated from the rest of the organisation, often working alone and without Internet. As a consequence, if a problem arises or if they are attacked, there is no structure to help them cope or rescue them[9].

A group typically targeted by the Government's security forces is ***human rights lawyers***. Although the national legal framework theoretically protects them, they are often seen as an extension of their clients and there have been many reports of lawyers being "abducted, prosecuted, and threatened", even in the capital and other big cities[10]. The intimidation of lawyers is also used as a technique to coerce HRDs.

Trade unionists often organise and participate in protests and are therefore seen as opposing the Government. The fact that the opposition party grew from a trade union is an added reason to persecute trade unionists. In recent years, there has been a wave of arrests of trade unionists, many of whom reported

being tortured while in police custody[11].

Journalists have also been harassed. The Access to Information and Protection of Privacy Act (AIPPA) has allowed the Government to silence all media seen as opposing the ZANU-PF, while foreign media have been banned from reporting the situation in Zimbabwe. Access to information is very much under Government control and journalists seen as disruptive are regularly arrested[12].

Lastly, ***students*** have been prominent in recent anti-government struggles, having "organised demonstrations against school fees, forced evictions and poor social services delivery"[13]. Reports have followed of frequent arrests and different forms of intimidation and torture, including being "forced to drink the contaminated water [of a sewer outlet]" and having their belongings confiscated[14].

---

[1] Privacy International. "Privacy and Human Rights: An International Survey of Privacy Laws and Practice". Retrieved on May 2 from http://gilc.org/privacy/survey/intro.html#defining
[2] Ibid
[3] Parker, R. B. 1974. "A Definition of Privacy". Rutgers Law Review, Vol. 27, No. 2, pp. 275-296
[4] Privacy International. 2012. Retrieved on April 19 from https://www.privacyinternational.org
[5] Human Rights House Foundation. 2005. "Kenya: Govt. on the Spot over Treatment of Human Rights Defenders". Retrieved on April 19 from http://humanrightshouse.org/Articles/498.html
[6] Sekaggya, M. 2013. "Report of the Special Rapporteur on the situation of human rights defenders, Margaret Sekaggya"
[7] Easton, M. 2010. *Strategies for Survival: Protection of Human Rights Defenders in Colombia, Indonesia and Zimbabwe*. Dublin: Front Line
[8] Ibid
[9] Ibid
[10] Ibid
[11] Ibid
[12] Ibid
[13] Ibid
[14] Ibid

4. International Framework on Human Rights Defenders and the Right to Privacy

This section explores the international provisions for the protection of the right to privacy, as well as the perception of the international community of the situation for HRDs in Zimbabwe, analysing the following questions:

- Is the right to privacy protected internationally?
- Is Zimbabwe perceived to be in line with international standards and best practice?

Answering these questions will allow to investigate what the best practice is, allowing for a comparison with the existing situation in Zimbabwe.

4.1. The International Framework on the Right to Privacy

The right to privacy is recognised and protected as an indelible human right in most international conventions dealing with human rights. Article 12 of the 1945 Universal Declaration of Human Rights and Article 17 of the 1966 International Covenant on Civil and Political Rights and state 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"[1].
The European Convention for Human Rights—and therefore the European Court of Human Rights—also acknowledges the right to privacy. Article 8 on the Right to respect for private and family life also presupposes that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others[2].

The 1993 Vienna Declarations and Programme of Action, the most important human rights covenant of the past 20 years, reaffirmed the rights outlined in the previous treaties, clarified the hierarchy of rights and strengthened the human rights protection mechanisms, particularly by setting up of the Office of the High Commissioner for Human Rights. It also stressed that the violation of a right is interconnected to the violation of other human rights[3]. It then follows that the violation of the right to privacy also violates the right of expression or speech and vice versa.

Internationally, the constitutions of different countries as well as the international charters on human rights are translated into laws that safeguard against impunity. Knowing that if the right to privacy is violated, the guilty parties will be judged provides an enabling environment for HRDs. However,

these laws and legislations do not suffice in protecting the right to privacy. In the absence of accountability of those violating this right, or in the absence of effective enforcement, human rights violators too often go unpunished[4]. In fact, active enforcement of legislations protecting the right to privacy is a prime concerns for those working on safeguarding it.

It is clear that, even within an international framework where the right to privacy is recognised and theoretically protected, this is frequently not the case. In particular, looking at the use of intercept communications offers an insight into what remains problematic in much of the democratic world.
The right to privacy is often violated because of overriding legislations on national security and emergency as well as public order, morality, etc.[5] These laws are often used to target HRDs and strip them of their rights, both in democratic and non-democratic countries. The most common tool used in this regard is communications intercept, "intelligence activities aimed at defenders leading to obstruction of their work, violation of their privacy and placing them and the people they work with at greater risk of violence"[6]. Sometimes, these violations are ingrained in the way the country functions, allowing for the sanction of HRDs who undertake to improve the country's human rights record. In her 2002 speech, Jilani offered insight in the way this is done:

> Reporting human rights violations have led to charges of spreading false information and defamation of authorities. Expression of views on human rights issues has been termed as incitement. Civic education programmes have led to charges of sedition. Criticism of discriminatory practices has been prosecuted as an offence against religion. Concerns expressed on the independence and impartiality of the judiciary have invited proceedings for contempt of court. Environment in academic institutions has been brought under strain by restrictions on academic freedom[7].

This framework allows for impunity for human rights violators and severely impedes the work of HRDs and constraints the environment for civil society. In Russia, for example, NGOs accepting funding from other states are categorised as "foreign agents" after a new package of restrictive laws was passed in 2012[8]. UN experts insist that the new law is inciting an "obstructive, intimidating and stigmatizing effect" on the correct functioning of civil society[9]. The new categorisation of foreign-funded NGOs leads to closer inspection by the Government and stricter penalties.

An interesting aspect of the right to privacy is the use of secret information gathered by infringing upon this human right. A 2011 report for the Joint Committee on Human Rights[10] noted that concerns or perceived threats to national security and in particular relating to terrorism allow for the use of secret information. Yet most democratic states have safeguards against the violation of the right to privacy even in these extreme cases.

This is also the case in the United Kingdom. The Government's Communications Data Bill proposed in 2012 would allow for a record of electronic communications—including email, Twitter and Skype—to be kept on file by the police for a year aiming at combatting terrorism. While the Bill stipulates that the content of the communications would remain private, significant information such as "the time, duration, originator and recipient of a

communication and the location of a communication device from which a communication is made" would be available to the authorities[11]. It is also interesting that communications data—aka the form but not the content of the acquired information—are admissible to court. While the Communications Data Bill was not passed as is, an amended version will be proposed to Parliament at a later date.

Following alarming reports on US Internet Surveillance on foreign officials, as well as civilians, which caused an outcry by the international community, on 18 December 2013 the UN adopted a resolution stating that Internet surveillance is a violation of the right to privacy[12]. The objective of this resolution is to expound that violations of this right are not acceptable, irrespective of the means used to carry them out. As Brazil's Ambassador Antonio de Aguiar Patriota noted, the resolution "establishes for the first time that human rights should prevail irrespective of the medium, and therefore need to be protected online and offline"[13]. This is the first time that Internet surveillance has come to be the focus of a UN resolution and marks the tightening of the framework protecting the right to privacy. On the same day the U.S. White House unveiled recommendations that shield U.S citizens and foreign leaders from the National Security Agency surveillance[14].

The UN resolution is the latest development concerning the relation between the right to privacy and the use of technology and the Internet. In her speech from September 2013, Navi Pillay stressed that, despite the democratic potential of modern communications technology "by vastly increasing individuals' access to information and facilitating their active participation in society", these have "also contributed to a blurring of lines between the public and private sphere, and made possible unprecedented levels of interference with the right to privacy"[15]. She noted that modern communications technology increased the potential scope of surveillance regimes to infringe upon individuals' and groups' right to privacy. She added that what is distressing about this development is that it is now "easier and cheaper than before to monitor, filter, censor and block communications. It is quite simple to monitor personal traffic data and calls in real time"[16].

4.2. Perceptions of the Situation of Human Rights Defenders and the Right to Privacy in Zimbabwe by Supranational Organisations and Democratic Countries

The international community sees the violation of the right to privacy as an important concern in Zimbabwe. In its 2012 report, the US Department of State noted that "the most important human rights problems remained the Government's targeting for torture, abuse, arrest, and harassment members of non-ZANU-PF parties and civil society activists, partisan application of the rule of law among security forces and the judiciary, the Government's compulsory acquisition of private property, and restrictions on civil liberties"[17].

Following her visit to Zimbabwe in 2012, Navi Pillay, the UN High Commissioner for Human Rights, the first ever visit to Zimbabwe from someone in this position, addressed a number of issues that are impeding the protection of human rights in the country[18]. She stressed the importance of a New Constitution with an entrenched Bill of Rights to promote the punishment of impunity in Zimbabwe, hoping that human rights violations will eventually be settled in court. However, her visit ended on a positive note, focussing on the improvements that have already been achieved in the country.

Zimbabwe went on to improve its existing framework for the protection of human rights by enacting two important documents: the Human Rights Commission Bill and the Electoral Amendment Bill. Zimbabwe also accepted 115 of the 177 recommendations made by member and observer states during the Universal Periodical Review of 2011, which included criminalisation of torture and the adoption of international human rights mechanisms, including the UN Convention Against Torture (CAT), its optional protocol (OP CAT) and the Optional Protocols to the International Covenant on Civil and Political Rights[19]. However, Zimbabwe rejected recommendations from countries such as Norway to amend or repeal laws that undermine human rights such as the Public Order and Security Act (POSA), the Access to Information and Protection of Privacy Act (AIPPA) and the Broadcasting Services Act (BSA), which infringe on the freedom of expression[20]. In her meetings with Government officials, Navi Pillay also called attention to these acts, noting that the way they restrict the freedom of expression of journalists and the media is particularly worrisome[21]. What is also troubling is the fact that reports of "state-led low-level politically motivated harassment of human rights activists and political figures remains prevalent and appears to be increasing as we enter 2013" due to the upcoming elections[22]. The UK Foreign & Commonwealth Office stressed the importance of fully implementing the Global Political Agreement (GPA) ahead of the October 2013 elections in order for human rights violations—and particularly violations of the right to privacy—to remain in check during this politically charged period[23]. This is particularly significant if Zimbabwe is to avoid the escalation of violence that occurred during the 2008 elections. In particular, in February 2013, three United Nations Special Rapporteurs issued a joint statement claiming to "have received increasing numbers of reports about acts of intimidation and harassment, physical violence and arrests against civil society actors, mostly working on human rights issues" leading to the referendum on the new Constitution in March 2013[24]. Frank La Rue, the Special Rapporteur on the right to freedom of opinion and expression, stated that Zimbabwe should try to adhere to international norms, ensuring that "everyone is guaranteed the right to speak freely without fear of persecution, arrest and intimidation", particularly in the electoral year[25].

---

[1] Office of the High Commissioner for Human Rights (OHCHR). 2013a. "International Covenant on Civil and Political Rights". Retrieved on May 8 from http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx; United Nations (UN). 2013a. "The

Universal Declaration of Human Rights". Retrieved on May 8 from https://www.un.org/en/documents/udhr/

[2] European Court of Human Rights (ECtHR). 2010. "European Convention on Human Rights". Retrieved on May 8 from http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf

[3] Office of the High Commissioner for Human Rights (OHCHR). 2013b. "Vienna Declaration and Programme of Action". Retrieved May 24 from http://www.ohchr.org/EN/ProfessionalInterest/Pages/Vienna.aspx

[4] Pillay, N. 2013a. "Opening Remarks by Ms. Nivi Pillay, United Nations High Commissioner for Human Rights". Retrieved November 20 from http://www.norway-geneva.org/unitednations/humanrights/Statements/Side-event-on-Privacy-in-the-Digital-Age/Opening-Remarks-by-Ms-Nivi-Pillay-United-Nations-High-Commissioner-for-Human-Rights/#.UpdujsRdXMc

[5] Jilani, H. 2002. "Protecting Human Rights Defenders at Risk: a priority of the new Special Representative of the Secretary General on Human Rights Defenders". Speech delivered at Steps to Protection: The First Dublin Platform for Human Rights Defenders, retrieved on April 19 from http://www.frontlinedefenders.org/node/120

[6] Ibid

[7] Ibid

[8] Foreign & Commonwealth Office. 2013. Human Rights and Democracy: The 2012 Foreign & Commonwealth Office Report. United Kingdom: The Stationery Office Limited

[9] United Nations (UN). 2013b. "Civil society in Russia facing increasingly hostile environment – UN experts". Retrieved on May 18 from http://www.un.org/apps/news/story.asp?NewsID=44899&Cr=Russia&Cr1=#.UZ9be5VASfQ

[10] Alati, D., R. Dennis, R. Gross, A. Johns, E. Kuforiji, P. Troop and K. Hardy. 2011. "The Use of Secret Evidence in Judicial Proceedings: A Comparative Survey". Retrieved May 7 from http://denning.law.ox.ac.uk/news/events_files/Secret_Evidence_JCHR_27_October_2011_final.pdf

[11] Secretary of State for the Home Department. 2012. Draft Communications Data Bill. London: The Stationery Office Limited

[12] Miami Herald. 2013. "UN Advances Internet Privacy Resolution". Retrieved November 15 from http://www.miamiherald.com/2013/11/26/3780690/un-advances-internet-privacy-rights.html

[13] Ibid

[14] Liberty & Security in a changing world, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, 12 December 2013

[15] Pillay, N. 2013a. "Opening Remarks by Ms. Nivi Pillay, United Nations High Commissioner for Human Rights". Retrieved November 20 from http://www.norway-geneva.org/unitednations/humanrights/Statements/Side-event-on-Privacy-in-the-Digital-Age/Opening-Remarks-by-Ms-Nivi-Pillay-United-Nations-High-Commissioner-for-Human-Rights/#.UpdujsRdXMc

[16] Pillay, N. 2013b. "Opening statement: How to safeguard the right to privacy in the digital age". Retrieved November 20 from http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=E

[17] US Department of State. 2012. "2012 Human Rights Reports: Zimbabwe". Retrieved April 20 from http://www.state.gov/j/drl/rls/hrrpt/2012/af/204183.htm

[18] Office of the High Commissioner for Human Rights (OHCHR). 2012. "UN Human Rights Chief Ends First Ever Mission to Zimbabwe". Retrieved May 15 from http://www.ohchr.org/EN/NewsEvents/Pages/HRChiefendsfirstevermissiontoZimbabwebyaUNHCforHR.aspx

[19] Foreign & Commonwealth Office. 2013. *Human Rights and Democracy: The 2012 Foreign & Commonwealth Office Report*. United Kingdom: The Stationery Office Limited

[20] For more information on the aforementioned laws and Acts, please refer to chapter 4

[21] Pillay, N. 2012. "Opening remarks by UN High Commissioner for Human Rights Navi Pillay at a press conference during her mission to Zimbabwe". Retrieved May 15 from http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=12192&LangID=E

[22] Foreign & Commonwealth Office. 2013. *Human Rights and Democracy: The 2012 Foreign & Commonwealth Office Report*. United Kingdom: The Stationery Office Limited

[23] Ibid

[24] Office of the High Commissioner for Human Rights (OHCHR). 2013c. ""Zimbabwe must respect fundamental freedoms in run-up to constitutional referendum," warn UN rights experts". Retrieved May 24 from http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=13055&LangID=E

[25] Ibid

5. Legal and Constitutional Landscape

The aim of this section is to analyse the legal and constitutional framework regarding the right to privacy in Zimbabwe. In particular it will seek to address the following questions:

- What laws and constitutional provisions exist to protect privacy?
- How are they implemented and monitored, and where are the legal and policy gaps?

In asking these questions it is hoped that some insight will surface as to how the current policy, legislative and practice frameworks in Zimbabwe can be brought into line with international standards and best practice.

The section will begin with an overview of the main constitutional documents, which have formed the basis of Zimbabwe's legal system since independence. Particular attention will be drawn to provisions protecting the right to privacy. This will be followed with an analysis of existing laws in Zimbabwe, which are used by the security forces to infringe the constitutional rights of HRDs.

5.1. Who are the Security forces in Zimbabwe?

According to the US Department of State (US DOS) report[1], the main security forces are the Zimbabwe Republic Police (ZRP), the Central Intelligence Organisation (CIO) and the Zimbabwe Defence Forces (ZDF), which are sometimes used domestically.

In 2009 the National Security Council (NSC), comprising of the three main political parties, was created in order to oversee the country's security services. However, the NSC rarely met and, reportedly, this function continued to be exerted by the Joint Operation Command (JOC), consisting of the security forces themselves under the control of President Mugabe.

Other organisations, which prevent free expression, include the Broadcasting Authority of Zimbabwe (BAZ), responsible for licensing broadcasters, the Media and Information Commission (MIC), which refuses to licence journalists, and the Monitoring and Interception of Communications Centre (MICC), which operates the country's programme of communications surveillance.

5.2. Lancaster House Constitution

Zimbabwe achieved independence in 1980. The negotiations which took place between the British colonial powers, the outgoing Smith Government and nationalist politicians, including the current ZANU-PF President, Robert Mugabe, and Joshua Nkomo of ZAPU, produced an agreement known as the Lancaster House Constitution (LHC)[2].

Throughout its time as the main constitutional document in Zimbabwe, the LHC was amended numerous times. There were calls from all quarters for it to be replaced with a constitution emanating from civil society, which would be reflective of national values. This recognised that the LHC had been the product of political wrangling rather than a real democratic process. An attempt in 2000 to install a similarly partisan document, led by President Mugabe, was therefore met with little surprise when it was defeated in a referendum.

The Colonial Government

There were many examples in Rhodesia of the colonial powers ruthlessly suppressing political activism. Under the Smith Government, the rule of law was often not observed. Fundamental human rights were often violated with impunity. Though a number of constitutional enactments contained a declaration of rights, these were often not justiciable in court.

At the University College of Rhodesia and Nyasaland (UCRN), many expatriate lecturers who were seen as a threat to the Government were put under surveillance or deported by the Federal Intelligence and Security Bureau (FISB). These security measures violated a key component of the UCRN's academic freedom and the civil liberties of these lecturers. Often, reports of their support for communism or African nationalism were based on FISB's distorted and sometimes false secret intelligence about their political opinions and activities.

Despite being conceived at a time of great political turbulence, the LHC contains a surprisingly liberal declaration of rights, more akin to that of a democracy than the totalitarian society, which Zimbabwe has latterly become. Without specifically mentioning privacy, there are parts of the LHC, which, on paper, protect our four constituent parts of information privacy, bodily privacy, privacy of communications and territorial privacy.

Under Article 17 of the Lancaster House Constitution, individuals were protected from arbitrary searches of their person and entry onto their property. It recognised the rights to bodily and territorial privacy. Other rights, such as the freedom of expression, association and assembly, which have a fluid relationship with privacy, were also protected. For any of these rights to be properly enjoyed, they require a private operating space; in the nascent stages of formulating an argument, creating a political party, or organising a mass demonstration. In turn, the strengthening of these rights expands the ‘operating space’ of privacy, which the individual is free to occupy without interference from the state.

In this sense the right to privacy is partly covered by the right to free expression in section 20 of the LHC, which includes "the freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with [a person's] correspondence". An example can be seen in the last part, insofar as the freedom to correspond without interference means that a person's private communications cannot be lawfully monitored, intercepted or infringed. The freedom to hold opinions is also a crucial element of a person's private life, which they should be free to discuss at home and at work with friends and colleagues.

Moreover, in section 21, the rights to freedom of assembly and association protect interactions "with other persons" whether it is in public or private life. Although the freedom "to form or belong to political parties or trade unions or other associations for the protection of his interests" would essentially tend towards a person's public endeavours, there is also a sense in which a liberal definition of a private life would simply cast these a person's right to join a political party of their choosing without state interference. Or, as the UK Court of Appeal has stated in a case regarding Zimbabwe, the choice to be apolitical should also be a private one.[3]

However, these sections of the LHC, like the civil rights espoused in many constitutions, are subject to exceptions. In particular, the right to free expression can be limited by section 20 (2) in the interests of "national defence, public safety, public order [and] public security". Even the Governments of liberal democracies worldwide exhibit the tendency to exploit national security exceptions in order to limit free expression and to quell political criticism. However, in Zimbabwe, the propensity for these exceptions to be used in ways, which are politically motivated, is even greater. Given that ZANU-PF has been the only party constantly in Government ever since independence, there is a cultural tendency for any criticism of ZANU-PF to be classified as a criticism of the nation, and is therefore likely to be criminalised on one of these grounds.

The most notorious illustration of this attitude is seen in the Criminal Law (Codification and Reform) Act (CLCRA) 2004. Although the CLCRA will be described in detail below, it is worth noting here that, as the US DOS describes, under the Act:

> making a false statement prejudicial to the government carries a maximum prison sentence of 20 years. Security authorities continued to restrict freedom of speech and arrest individuals, particularly those who made or publicized comments critical of President Mugabe or made political statements opposing the government's agenda[4].

Thus, even though the LHC, the main constitutional document operating at the time, purports to protect free expression, in practice the Government has been able to enact laws running completely counter to those rights. This suggests that the problem in Zimbabwe has not been one of constitutional deficiencies on paper, but one of enforcement.

5.3. Global Political Agreement

There was a protracted period of political violence in Zimbabwe following the 2008 elections. The end to this violence only came with the introduction of a new constitutional document called the Global Political Agreement (GPA)[5]. With this document, and for the first time since independence, the ruling ZANU-PF party committed itself to sharing power with others.

MDC Leader Arrested

In 2002, Morgan Tsvangirai was arrested on charges of treason. He was videotaped during a visit to Canada engaging in a conversation with people he believed to be political consultants. The police alleged that Mr Tsvangirai was filmed discussing plans with them to assassinate President Mugabe. However, the charges were later dropped. It also emerged that the man responsible for the video was a former Israeli agent with business and personal links to President Mugabe. It is likely that he was working under the orders of the Zimbabwean state with the objective of entrapping Mr Tsvangirai prior to the 2002 elections. State surveillance has occasionally, therefore, extended beyond Zimbabwe's borders.

Surveillance of MDC Leader's wife [5]

In August 2013, it was reported in the state weekly newspaper The Zimbabwe Guardian that the wife of Morgan Tsvangirai had rekindled an inappropriate relationship with her ex-husband. The piece featured several emails that had been sent between Tsvangirai's wife and her ex, and went on to suggest there had been monitoring of her telephone and emails. This scandal seems to add weight to fears that spy agencies have been routinely intercepting cellphone text messages and hacking into computers in search for scoops. Lawyer Kudazyi Kadzere said that the phone hacking was "totally unconstitutional".

Both incidents serve to demonstrate the extent of state sponsored monitoring activity both at home and abroad.

As Human Rights Watch noted in their 2013 World Report on Zimbabwe, this momentous occasion meant that:

> Human rights developments in Zimbabwe in 2012 were dominated by the drafting of a new constitution and the implementation of the Global Political Agreement (GPA), signed in 2008, which created the power-sharing coalition between the former ruling party, the Zimbabwe African National Union-Patriotic Front (ZANU-PF), and the opposition party Movement for Democratic Change (MDC) following the 2008 elections[6].

The GPA, like the Lancaster House Constitution, expresses the Government's commitment to the rule of law and to the protection of individual rights. Article XIX underlines "the importance of the right of freedom of expression". This Article therefore emphasises what was already enshrined and should have been enforced in article 20 of the LHC. Further, article 21 of the LHC is built

upon by Article XII of the GPA, which states that "the Parties have agreed to work together in a manner which guarantees the full implementation and realisation of the right to freedom of association and assembly". Combined, these provisions express the Government's inclusive commitment to protecting the private lives of its citizens in some important ways.

However, despite these seemingly good intentions espoused in the GPA, HRDs in Zimbabwe have often encountered difficulties with other discontinuous parts. Whilst the GPA espouses these rights in theory, it also contains a number of practical measures for their restriction. These are unfortunately much wider than the national security exceptions included in the LHC, and it seems that their aim is to consolidate the place of repressive pieces of legislation and assert their compatibility with constitutional rights.

The right to free expression, for example, in the first paragraph of article XIX is tempered by the commitment in the last paragraph to keeping and enforcing the Broadcasting Services Act (BSA) and the Access to Information and Protection of Privacy Act (AIPPA). Much more will be said about these Acts below, but given the nature of these pieces of legislation it is unlikely that, without their repeal or amendment, the GPA could possibly turn the tide from an environment of political violence in 2008 to one of respect for constitutional rights.

The sentiment from Sokwanele is that the "GPA demands a genuine commitment towards achieving freedom of expression in Zimbabwe". One of the issues facing media companies had been that the regulator set up by the Broadcasting Services Act had failed to grant licences to any media providers other than those run by the Government. The proposed solution to this problem in the GPA is for media companies simply to re-submit applications for registration to the "appropriate authorities". However, with the BSA still in place after the GPA, it is highly unlikely that the "appropriate authorities" would in any way change this practice of denying licenses to private sources[7].

Similarly, in Article XII of the Constitution, the whole remit of the right is made subject to the pre-existing "security legislation". The US DOS[8] report highlights this weakness, insofar as "Government efforts to reform the security forces were minimal…[and] authorities [in 2012] rarely provided training on nonpartisan implementation of the rule of law". It is therefore doubtful whether the Government's commitment to training the police and security forces would achieve respect for the rights, given that enforcement of legislation such as the Public Order and Security Act (POSA) and the Criminal Law (Codification and Reform) Act give the police legal powers to infringe the very rights for which the GPA feigns respect. According to Human Rights Watch:

> The power-sharing government has either failed to amend or come to agreement on amending repressive laws such as the Access to Information and Protection of Privacy Act (AIPPA), the Public Order and Security Act (POSA), and the Criminal Law (Codification and Reform) Act, which severely curtail basic rights through vague defamation clauses and draconian penalties.

Although the doctrine of implied repeal would suggest that these laws, which all preceded the GPA, would have to be made compatible with it, there has been little action from the Government aimed at achieving this result. The UN High Commissioner for Human Rights, Navi Pillay[9], recently warned that a failure to implement the GPA reforms in practice could mean a return to political violence before the next election. Such warnings were echoed by the UK Foreign and Commonwealth Office, who stressed the importance of having a fully implemented GPA in order for human rights violations to remain in check during this politically charged period[10]. Given the escalation of violence that occurred during 2008, these warnings must hold some weight. In addition, now that Zimbabwe has a new Constitution, the same must be said to equally apply. In February 2013, three United Nations Special Rapporteurs issued a joint statement claiming to "have received increasing numbers of reports about acts of intimidation and harassment, physical violence and arrests against civil society actors, mostly working on human rights issues" leading to the referendum on the new Constitution in March 2013[11]. From the perspective of this project it is vital that the new specific right to privacy in the Constitution be enforced in Zimbabwe's laws.

5.4. New Constitution

Zimbabwe's new Constitution[12] was signed into law on 22nd May 2013. This replaces the LHC, which had in any case been amended so many times as to be almost unworkable. In 2000, the previous attempt to introduce a new constitution was rejected at referendum. Marred by partisanship and dictated by the political class, it failed because of a lack of consultation with the people. This time around, therefore, the Government was careful to give civil society a greater role[13].

Thus, it could be assumed that the new Constitution better reflects the rights which normal Zimbabweans find important. This might explain why the new Constitution finally contains a specific right to privacy. The language of privacy has finally entered into Zimbabwean constitutional discourse. This brings it into line with international best practice on constitutional rights, as evidenced by article 12 of the UN Declaration of Human Rights[14]. In terms of best practice in the African region, however, the new Constitution actually goes further than the African Charter on Human and People's Rights, which has been criticised for not containing a specific right to privacy[15].

It is worth quoting Zimbabwe's right to privacy in article 57 in full:

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

This article clearly integrates a number of the old provisions from the LHC and the GPA. Article 17 of the LHC, protecting Zimbabweans from body searches and entry into their homes, is reflected in parts a and b. On the other hand, the right to private communications has been removed from under the heading of free expression and now stands on its own as an essential part of right to privacy in part c. The new Constitution also places extra emphasis on the right to keep property and possessions private. Repressive laws like the Interception of Communications Act, which allows the seizure of possessions such as letters should now be rendered unconstitutional.

The rights to expression, assembly and association are reaffirmed in articles 58 to 60 of the new Constitution. Their substance remains largely unchanged from the LHC. However, it is significant that the many qualifications which existed in the GPA, making the Constitution subject to the repressive statutes set out below, have been removed. This suggests that these repressive laws might now be repealed or amended in order to remove the unconstitutional portions.

However, article 86, entitled "limitation of rights and freedoms", allows privacy to be limited by a law of general application which is held to be "fair, reasonable, necessary and justifiable in an open, just and democratic society" in the interests of "defence public safety, public order, public morality, public health, regional or town planning or the general public interest". Although international best practice shows that the right to privacy is often considered to be a qualified right[16], there is no precedent for allowing a limitation to be as broad as "the general public interest". There is no indication what this could mean, which fosters worries that the Government could again seek to make Zimbabwean constitutional rights non-justiciable.

As Zimbabwe Lawyers for Human Rights have stated, "It remains to be seen whether limitations will be narrow or wide-ranging as the State in the past has abused this provision without adequate justification, and the safeguard here is still not specific enough"[17]. It is recommended that these limitations should be interpreted as narrowly as possible whilst all of the necessary reforms to Zimbabwe's laws are carried out.

Under section 70(3) of the new Constitution, evidence obtained in violation of the Declaration of Rights and in violation of section 57, for example evidence acquired through illegal searches or monitoring of communications, must be excluded in criminal trials. Allowing the evidence to be submitted would render the trials unfair or would be detrimental to the administration of justice or the public interest.
The traditional common-law position is directly inversed: illegally obtained evidence is generally allowed in court, although evidence obtained through torture is excluded, and statements made by the accused are not admitted in evidence unless the statements are proved to have been made voluntarily[18].

According to Veritas[19], provisions of the Criminal Procedure and Evidence (CP&E) Act, which reflect the common-law position, will have to be amended. For example, section 258(2) of the CP&E Act allows the police to give evidence that an accused person pointed out something, for example a murder weapon or where stolen property was hidden, even though the statement was illegally induced by threats, etc.

5.5. Legislation

In the recent history of Zimbabwe, the Government has increasingly used national security and criminal legislation as a means to gain powers to keep citizens under surveillance and infringe upon their privacy rights. Since the turn of the millennium, laws which have been passed with the aim of limiting communications privacy include the Interception of Communications Act (ICA) 2007, Access to Information and Protection of Privacy Act (AIPPA) 2002, and the Broadcasting Services Act (BSA) 2001[20].

The Herald Interferes with Lawyer-Client Confidentiality

On 12 June 2013, state newspaper The Herald published a front-page article entitled "MDC-T launches litigation crusade", which reported of an alleged meeting of Zimbabwe Lawyers for Human Rights (ZLHR). While this has been seen by critics as a cynical attempt to cause friction between the MDC, ZLHR and the judiciary, it is also contended by ZLHR to be a breach of the client-lawyer privilege as protected by the Constitution. Section 69(4) of the new Constitution provides the right of every person to legal representation. When individuals seek to exercise this right, access to such information may be restricted on the grounds of professional confidentiality in accordance with section 62(4).

Territorial privacy has increasingly come under threat from the passage of the Public Order and Security Act (POSA) in 2002 and the Criminal Law (Codification and Reform Act) (CLCRA) in 2004. Such laws have given the police and security forces power to storm the offices of HRDs when they are empty in order to collect intelligence. Similarly, the US DOS report[21] states that there has been an increase in instances where "CIO agents and informers routinely monitored political and other meetings" as a means of creating a "chilling effect" on free expression and political activism[22].

A Crisis in Zimbabwe Coalition report from February 2013 states that civil organisations who have reported break-ins to their offices include the Zimbabwe Election Support Network (ZESN), the Counselling Services Unit (CSU), the Zimbabwe Human Rights Association (ZIM-RIGHTS), the Zimbabwe Peace Project (ZPP), the National Youth Development Trust (NYDT), the Youth Initiative for Democracy in Zimbabwe (YIDEZ), the Election Resource Centre (ERC), and even the National Association of Non-Governmental Organisations (NANGO). Whilst not all of these break-ins are presumed to have been carried out under the relevant legislation, there is little

doubt that the environment, which has been created by Government policy, has encouraged break-ins by non-state actors.

State Surveillance in 2005

In 2002, the National Association of non-governmental Organisations (NANGO) stated that, "that there have been reports of increased surveillance of NGOs by people believed to be state agents, at the back of an announcement by Public Service, Labour and Social Welfare Minister, Paul Mangwana, that a Committee has been set up to probe NGOs. This includes people being followed, unidentified vehicles being parked around the vicinity of offices of NGOs, and NGOs being approached by strangers and asked intrusive questions about their personal lives and institutional issues." This demonstrates some of the human-based surveillance tactics used by the state.

Nevertheless, these Acts did not pass without significant resistance from civil society. According to Amnesty[23], the Chair of Zimbabwe's Parliamentary Legal Committee was compelled to describe the AIPPA as "the most calculated and determined assault on our liberties guaranteed by the Constitution" when it passed through the House. Then, in 2003, Zimbabwe Lawyers for Human Rights, jointly with the Associated Newspapers of Zimbabwe, filed a petition for the AIPPA to be declared unconstitutional. The African Commission on Human and Peoples' Rights (ACHPR) eventually heard that case[24]. Its ruling states that the AIPPA contravenes Article 9 of the African Charter on Human and People's Rights, to which Zimbabwe is a party. In particular, it was held that sections 79 and 80—discussed below—should be repealed[25].

There was similar opposition to the passing of ICA. According to submissions made by the Crisis Coalition to the Legal and Parliamentary Affairs Committee, "the act is aimed at stripping off the citizenry's rights of freedom of expression…we therefore deplore the motivation by the Government of criminalising the fundamental freedoms". A report[26] by Margaret Zunguze notes that to some extent Parliament agreed. Allegations of unconstitutionality were raised in the debate for the Act, before eventually being dropped prior to the ICA entering the statute books in 2007.

The Supreme Court of Zimbabwe in fact declared the precursor to the BSA unconstitutional. The basis for this ruling was that the state monopoly over broadcasting services breached the right to freedom of expression. However, there has still not been one licence issued to an independent broadcaster since the duty to licence new providers was passed to a state regulator. This means that the state monopoly is still in place and that the BSA must be therefore subject to the same charges of unconstitutionality.

One precursor to POSA[27] had a number of clauses removed over the years by the Supreme Court for failing to meet constitutional requirements whereas another met with criticism from the Special Representative of the UN Secretary General on HRDs for unduly restricting the rights to free expression, association and assembly[28]. In 2011, the Government made

several commitments to improve the human rights situation[29] as left by these laws. However on-going human rights abuses still remain, including the selective application of the Constitution, the arbitrary application of the powers outlined below, and tight control of the electronic media.

5.6. Interception of Communications Act 2007

The Interception of Communications Act (ICA) 2007[30] gives the Zimbabwean Government significant powers of surveillance over the communications of its citizens. According to the long title of the Act, the aim of this legislation is to allow both the "interception" and "monitoring" of communications. Of course, both "interception" and "monitoring" are acts of surveillance, which infringe on the rights of an individual to communicate with others without interference from the state.

The ICA does, however, treat "monitoring" and "interception" differently, insofar as it only provides a definition for the latter. According to Part (a) of this definition, interception constitutes listening to, recording or copying a communication. Clearly this covers verbal and audio communications, such as a telephone conversation, or perhaps a speech recorded to a CD and sent to the intended recipient. Part (b) of the definition refers specifically to post, and refers to reading or copying the communication. For the authorities to intercept postal communications, they would have to take a person's private property, the letter or parcel, in order to examine it for the offending material. This infringes information privacy given that the authorities can gather any personal data contained therein. It is also an obvious breach of communications privacy because the state knows the content of what is said between the parties.

As mentioned, the ICA does not expand upon the definition of "monitoring". This suggests that the intention could be to provide a catch-all term for any other acts of surveillance which the Government wishes to carry out. In particular, the advantages of leaving the term undefined means that a blanket power is created in relation to newer, non-established means of communication, thus enabling the Government to keep track of technological advances. Email, text messages and website usage, for example, are more likely to be "monitored" rather than "intercepted", as there is no need to prevent the communication from reaching the recipient in order for the Government to carry out its surveillance.

Both the powers of interception and monitoring are drafted widely. The authorities can read or listen to the "whole or part" of the communication. This suggests, for example, that if the authorities intercept a letter which they suspect contains one or two lines of offending material, then they can still read the rest of the letter and collect non-offensive but private information such as the parties' contact details, bank account information or plans to organise a meeting. The authorities might also learn of any family circumstances, home or health issues which are communicated. This wide

drafting means that the power can be used as a tool for building a case against a specifically targeted individual, or fishing for information which might enable further surveillance of a person's movements or political activities.

This worry is compounded by the fact that the act does not even require "reasonable suspicion" that a criminal offence is being committed. This means that it falls below the standard grounds required by best practice in criminal codes worldwide. Rather, section 5 (g) requires that the warrant state a basis for the belief "that communication relating to the ground on which the application is made will be obtained through interception". This is an entirely subjective judgement, which can be based on false informant information or information which is otherwise entirely hearsay. There is no judicial control over whether this "belief" is justified, or whether the information grounding the belief has been obtained lawfully.

The powers contained in the ICA are also extensive with regards to the kind of communications which can be intercepted. Powers are given specifically for the Authorities to intercept post and telecommunications. However, the ICA can also be used to intercept communications sent on "any other related service or system". This compounds the impression that in drafting the ICA the Government intended for it to cover, as much as possible, any modern technological developments like email, social media such as Twitter and Facebook, and internet telecoms like Skype.

Although these technologies exist in Zimbabwe, the uptake in using them has been slowed by a combination of the economic situation and the repressive legal system. It is important to note that, with an Opennet estimation of about 11% in 2009, Internet penetration in Zimbabwe, though relatively high in Africa, is low by world standards[31]. In 2007 Opennet found no evidence of the state filtering websites.

A more recent 2012 report by Freedom House[32] reports a huge increase in smart phone usage with Internet capabilities, especially amongst young people. Between 2006 and 2011, it is estimated that the growth of mobile phone usage has gone from 6.8% to 72.1%. Many Zimbabweans use their phones and laptops to browse Facebook, the country's most popular website, and to use whatsapp, a kind of Internet text message service. It has been reported that in 2012, the Telecommunications Regulatory Authority of Zimbabwe banned the use of Blackberry Messenger because the of service's encryption of messages. By encrypting messages, the service does not comply with the requirement in the ICA that "all telecommunication services should have the capability of being intercepted".

Baba Jukwa (Literally Translated Means Father of Jukwa)

An account emerged on Facebook in January 2013 under the name of 'Baba Jukwa'. The regular posts from this pseudonymous account have rapidly become established as a major source of online political news in Zimbabwe. It is thought to be run by a member of the ruling ZANU-PF party. Many of the posts centre on accusations of state corruption and violence. Until now the person behind the posts has evaded arrest by using a number of layers of encryption. However, the Government is reportedly undertaking an intense campaign to find the poster's identity and has invested in technologies to enhance its ability to conduct digital surveillance. On May 31st, the State Security Minister publicly announced his worries that "Zimbabwe is under cyber attack" with veiled references to the Facebook account.

However, most Zimbabweans have not followed the worldwide trend of social media being used to express political opinions, and even to form campaigns online[33]. Freedom on the Net reports that, "the lack of anonymity…and fear of repercussions limit politically oriented statements, which can be traced back to those expressing them". Facebook is of course a largely public forum, and there have been instances of Zimbabweans being arrested because of their posts. Where Facebook is concerned the state can still make use of human surveillance techniques. Employing state agents to monitor the pages of HRDs and activists, in the form of what the UN Special Rapporteur[34] calls "mass communications surveillance", might still be an effective tool.

These worries are compounded by the complicity of Zimbabwean Internet Service Providers (ISPs). Under section 9 of ICA, ISPs are required to install at their own expense the hardware and software required for the state to carry out surveillance. Reports in Zimbabwe[35] suggest that at least three of the main Internet Service Providers – Econet, TelOne and Telecontract – have complied with this requirement. Furthermore, some unconfirmed reports have suggested that the Government has received surveillance technology and training from China[36]. As such, many HRDs have stopped using emails that are hosted in Zimbabwe and begun using foreign cloud servers like Google instead. It is hoped that this will provide at least some protection against state surveillance of email accounts.

Just as post is intercepted or a phone line is monitored, the state also has the power to snoop on communications travelling by email or across a social network. Having set up a Monitoring of Interception of Communications Centre, manned by "technical experts", and appointed by the Minister of Transport and Communications, the state has the legislative and institutional apparatus in place to subject Zimbabwean's digital communications to the same surveillance as any other. As the UN Special Rapporteur[37] notes, the inspection of emails prior to reaching the desired recipient is still a breach of the right to private communications.

In addition to concerns about the wide drafting of the powers, there is also concern about the lack of separation between the judicial and political roles in the Act. In particular, the main decision-maker arbitrating on whether to issue

warrants is a Government Minister. This raises serious concerns of partisanship, the politicisation of the intelligence services and the extent of state control over surveillance operations.

A warrant for interception under section 6 of the ICA can be issued by the Minister of Transport and Communications on a number of grounds:

- Where there is an actual threat to "national security", and/or;
- An actual threat to "public safety", and/or:
- An actual threat to the "national economic interest" or;
- A potential threat to any of the above.

This means that the Minister has both the power to define the standard of what constitutes a threat to the state, and also the power to decide whether that standard has been met. The ICA therefore lacks any kind of control over state abuse of the power. It falls to the Minister to decide when an individual's fundamental right of to private communication can be interfered with. The Minister is unlikely to be able to separate, in his own mind, what is an objective threat to the nation, and what is merely a political threat to the ruling Government.

Facebook Subversion Trial

A supporter of the MDC-T party, Vikas Mavhudzi, reportedly put a post on a public Facebook wall drawing parallels between the Arab Spring and the political situation in Zimbabwe. He was arrested and spent a month in jail. The prosecutor said the post was an "attempt to take over the Government by unconstitutional means or usurping the functions of the Government". However, his trial eventually collapsed because the post had been deleted and could not be offered as evidence.

This lack of judicial oversight means that its use is likely to go against the protection of an individual's right to due process and protection of the law, enshrined in all of the Lancaster House Constitution, the Global Political Agreement and the new Zimbabwean Constitution. Submissions of the ZLHR made at the time of the Lancaster House Constitution refer to the ICA as violating the freedom of expression and freedom to receive and impart information, the standards through which privacy was protected under that Constitution. They argue that the lack of a neutral or judicial arbiter means there is no guarantee that any limitation of rights will be done in a manner acceptable in a democratic society.

In addition, the fact that the fourth ground allows for interception on the basis of a "potential threat" shows that the ICA does not take fundamental privacy rights very seriously at all. By contrasting a potential threat with an actual threat, the ICA suggests that the former could justify the issuance of a warrant before any evidence is even produced. As the UN Special Rapporteur warns, without law enforcement authorities capable of establishing the factual basis for surveillance on a case-by-case basis, there is a danger that communications surveillance can be used in a broad and indiscriminate

manner[38]. If the Government is pre-empting a future threat, then this power is likely to be used as a blanket ground for surveillance to follow HRDs and collect information. This matter is compounded by a wide definition of 'national security' as "matters relating to the existence, independence and safety of the state". Any actions by opposition political parties, party activists or protest groups could be cast as "matters relating" to national security and so the danger is that the power will be used without any specific or significant threat at all.

The extremely low burden of proof required to authorise surveillance has led the UN Special Rapporteur to express worry about "the potential for surveillance to result in investigation, discrimination or violations of human rights[39]". As if the constitutional protections in the ICA were not already watered down enough, section 8 provides a mechanism for circumventing even the few existing safeguards. According to section 8, an interception which has not been authorised, and has therefore been carried out unlawfully under ICA, can still be admitted into court as evidence. Although the judiciary has been given the power to decide whether such interceptions can be admitted, it is unlikely to get much room for independence, given the Executive's deep involvement in every other decision-making role.

Indeed, Zimbabwe Lawyers for Human Rights[40] notes the major inconsistency in this portion of ICA. Whilst section 3 supposedly makes unlawful interception of communications a criminal offence, this is not supported by section 8, which provides a mechanism for the content of the interception to be used in court. Evidence obtained by criminal means should not be used in court under any circumstances. Whilst this may be "symptomatic of bad drafting" it is more likely to be indicative of the fact that section 3 will not be enforced in practice, or if it is, that its use will be limited to prosecuting anti-Government forces. Further, section 8 is likely to be used to encourage surveillance by non-state groups working in support of the Government's surveillance scheme.

Finally, given that the new Zimbabwean Constitution was only passed in March of this year, there is presently little indication of how the right to privacy in section 57 will operate. However part (d), which states that "every person has the right not to have the privacy of their communications infringed", is clearly a provision, which, in spirit, is fundamentally opposed to the powers granted by the ICA 2007. It is suggested that for this element of the right to privacy to be protected then, ideally, the ICA 2007 must be repealed.

One option would be for the Government to make the ICA 2007 workable in light of the limitation of rights and freedoms provisions in section 86 of the Constitution. This would require—as set out above—that the limitation of the right to privacy be to "the extent that the limitation is fair, reasonable, necessary, and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom". For a start, this would require that the affected person, whose communications are the subject of an interception warrant, should have a right to challenge the warrant in court. He should be able to get an explanation as to why a warrant is sought and for what material.

It must also be a precondition that some criminal offence must form the grounds of the warrant. Unfortunately, given the lack of judicial oversight in the Act, it is unlikely that any of these protections for the right to privacy are currently respected in practice.

5.7. Statutory Instrument 142 of 2013 on the Postal and Telecommunications (Subscriber Registration) Regulations

Early signs from the newly elected ZANU-PF administration do little to encourage optimism. On the 1st October 2013 the new Government enacted Statutory Instrument 142 of 2013 on the Postal and Telecommunications (Subscriber Registration) Regulations was enacted by the new administration. This essentially builds upon ground already covered by the ICA, serving to undermine the Constitution yet further rather than reinforce it.

The SI requires telecommunication providers to set up a central subscriber database for all their users, connecting each SIM card with the name, address, gender, nationality and passport or ID number of its user. Within this requirement, companies will no longer be able to activate any SIM card that is not registered. Individuals must report any loss or change of ownership to their SIM card, and the provision of false information would make them liable to a six month prison sentence.

As well as compiling their own database, service providers are obliged to regularly hand over copies of this data to the Government, which will then establish its own central subscriber information database. Access to the database for the purposes of law enforcement will be available upon the written request of a "a law enforcement agent who is not below the rank of Assistant Commissioner of police or a co-ordinate rank in any other law enforcement agency", for "safeguarding national security" or for "undertaking approved educational and research purposes".

According to section 9(4) of the Regulations, information would not be released "where such release of subscriber information would constitute a breach of the Constitution". However, as with the ICA, the powers granted under the new law are framed in broad terms and are completely free from judicial oversight. Thus, in spite of the lip-service paid to the Constitution, there is an inherent danger of information collected being misused at the hands of the state. For example, individual profiles may be matched and cross-references with other private and public databases, allowing the state to keep comprehensive profiles of its own citizens. Without the required level of rigorous legal safeguards in place, it is likely that such a database would be a prima facie infringement of the right to privacy within any legal system true to the rule of law, as has been decided in international jurisprudence (see for example, Leander v Sweden[41] and Hewitt & Harman v UK[42]). Whether this can be said of the Constitution of the Republic of Zimbabwe is a matter, which remains to be seen.

5.8. The Access to Information and Protection of Privacy Act 2002

At first glance, the Access to Information and Protection of Privacy Act (AIPPA) would appear to have a positive effect on the protection of privacy in Zimbabwe. Its long title states that it aims "to protect privacy" and also "to prevent unauthorised collection, use or disclosure of personal information by public bodies".

Indeed, part of the AIPPA is devoted to freedom of information. A citizen or resident can access records held by a public body, which must respond to a request within thirty days. However, there are a number of exemptions. Cabinet and local Government documents do not have to be released, nor does advice given to public bodies. Information concerning law enforcement and which would breach client-lawyer privilege is exempted, and there are a number of exemptions for national security and public safety. The extensive nature of these exemptions has led Amnesty[43] to the conclude that the "AIPPA is not about improving access to information or protecting privacy, but protecting the Government from scrutiny by restricting access to information held by public bodies".

However, the AIPPA also brings into law a number of media restrictions, the content of which jeopardises the media's ability to make use of the right to free expression. It is not immediately obvious how these restrictions are related to the use of information or protecting privacy. This leads to the conclusion that privacy has merely been used as a pretext in order to smuggle in the provisions repressing the free media.

Firstly, section 79 of the AIPPA requires journalists to apply for accreditation to a body called the Media and Information Commission (MIC). The MIC is set up by section 38 and is essentially controlled by the Government. Although, as Amnesty[44] notes "most countries require media registration in some form", the decision-making powers in most countries lie with a professional body. This leads to a serious worry that, as the Independent Journalists Association of Zimbabwe[45] has argued, the t MIC lacks the independence required from a regulator.

There are many examples in the AIPPA of why independence is required of a media regulator. In section 39, the MIC is given the power to evaluate the accreditation of journalists. Any journalist writing articles criticising the Government is therefore likely to have his accreditation revoked. This is significant because such a power clearly compromises the ability of the media to hold the state to account. Lacking an effective independent media is dangerous for HRDs. They are vulnerable to surveillance and require a voice in the media to report instances of their property being broken into or suspicions about their communications being monitored. In practice, the media is vital to enforcing a right to privacy.

Under section 80(d), a journalist working without state accreditation can be imprisoned for up to two years. Attaching such a serious punishment to the choice to practice as a journalist clearly impinges upon the right to free expression. Journalists have to worry unduly about the content of their articles as a loss of accreditation means a loss of their profession and can even risk imprisonment. The mirror-image of this is that the journalist's readers are prevented from receiving information and making their own informed decisions. In both cases, the state illegitimately interferes in the private operating space of individuals.

In addition to requiring journalists to seek accreditation, section 66 of the AIPPA also requires any "mass media service" to register with the MIC, regardless of the size or frequency of publication. According to Amnesty[46], this means websites; small NGOs and shops, which sell newspapers, will all have to register with the Government. This is an excessive intrusion into the private lives of many businesses and individuals in civil society who have the freedom to transfer information and to consume independent sources of media without the involvement of the state.

5.9. Broadcasting Services Act 2001

The aim of this law and its predecessors was for the Government to retain its monopoly holding over all of Zimbabwe's broadcasting services. The previous 'Broadcasting Act' had made it illegal to operate any signal transmitting stations apart from the Government's own. This was declared unconstitutional under section 20 of the Lancaster House Constitution, on the grounds that it violated free expression.

The Broadcasting Services Act (BSA) was introduced to replace the unconstitutional Broadcasting Act. It replaces the de jure state monopoly over broadcasting with a "licensing" framework, under a new organisation called the Broadcasting Authority of Zimbabwe (BAZ). In many ways, parallels can be drawn with the AIPPA, since the BAZ also lacks the independence from Government required from a regulator. It operates under the power of the Minister of Information without input from the profession or civil society and, as such, preserves a de facto state monopoly over broadcasting. As the Media Institute of Southern Africa notes[47], "in the appointment of members of the BAZ there is no public involvement either in relation to public hearings or public nominations".

In section 19 of the Global Political Agreement of 2008, the Government was forced to recognise that "while the provisions of the Broadcasting Services Act permit the issuance of licences, no licences other than to the public broadcaster have been issued". The consequence of giving these licensing powers to the Government has been no different from an outright ban in practice. Under section 27 of the BSA, private broadcasters cannot operate without permission from the BAZ. The sum of these provisions means that the Government is flouting its responsibility under the African Commission's

Declaration of Principles on Freedom of Expression in Arica that, “states shall encourage a diverse, independent private broadcasting sector”[48].

A number of reforms were proposed in order to implement the GPA. First, a new board was to be appointed to the BAZ. This has still not been done as the necessary Parliamentary preliminaries for appointing new members have not been carried out. Nor has the Government delivered on the reform it promised regarding the Zimbabwe Broadcasting Corporation. Here, too, new board members should have been appointed. Given that the Government is the only shareholder in the ZBC, these appointments should have been straightforward. Although two new broadcasters have been licensed since the signing of the Global Political Agreement, it is widely believed that these broadcasters are not truly independent of the state. There have not been any community radio stations licensed.

Moreover, Section 11(1)(b) of the BSA still prevents radio and television from “broadcasting any political matte”’[49]. This means that even if new broadcasters are licensed, the Government will still use the BSA to maintain control of the political discourse in Zimbabwe. Combined with section 11(5), which compels licence holders to let the Government use its services for one hour per week in order to explain its policies, the BSA has a tight hold on free expression on the airwaves. Insofar as free expression requires ideas to be floated around, then this is not possible with the Government dictating what can and cannot be broadcasted. The right to privacy is also affected by restrictions on the flow of information.

5.10. Public Order and Security Act 2002

The Public Order and Security Act (POSA) is another tool, which the Government uses to suppress political opposition and to keep opponents under surveillance. Its provisions relate largely to the authorisation and policing of public gatherings. However, in reality, the police use the POSA to prevent public gatherings and to collect important information about attendees.

Of course, the authorities do need some powers to ensure that large public gatherings are run safely. The requirement under section 24 for organisers to give four days notice of their intention to hold a gathering is fair if it is applied appropriately. In reality, the authorities use it to further partisanship. Amnesty[50] states that “in practice, police are using [section 24] to refuse permission to hold…meetings”. Often, the police will ignore notices. Other times, according to the US DOS report, they will simply disrupt “many events whether or not they were notified”. Such arbitrary application of the power means that HRDs are unable to properly plan their events and to mount political opposition, both of which are important elements of the private operating space. In its 2013 report, Amnesty argues that the police use the “Public Order and Security Act to arbitrarily limit the rights to freedom of expression, association and peaceful assembly, including by blocking

legitimate meetings and activities of human rights defenders and other political parties"[51].

Arab Spring lecture

During a public lecture in Zimbabwe, activists showed video footage of the Arab Spring protests in Egypt. The police raided the lecture and arrested 45 people. Eventually charges were brought against six activists, who were convicted of inciting public violence in March and given community sentences.

In addition, there is concern about how the POSA may be used to police events, which are essentially private in nature. In its definition section, the POSA states that a building may constitute a "public place" so long as "the public have access" to it. This is still the case "whether or not the right of admission thereto is reserved". Clearly, this definition brings the offices and premises of many HRDs under the terrain of the POSA as "public places", notwithstanding that they are owned privately and usually limited to activists. This means that the section 57 right under the new constitutional right "not to have their home, premises or property entered without their permission" is likely to be breached by the police entering buildings to break up gatherings.[52]

Entering Buildings Without a Warrant

In November 2012, the police turned up, without a warrant, at the offices of the Counselling Services Unit, a medical facility helping the victims of torture and violence. After threatening to force entry, and then finally securing a search warrant, the police arrested a number of the staff and detained them unlawfully for four days

Section 25 gives the authorities extensive powers to dictate the time and place of any gathering, how long it lasts and the route of any procession. More significantly, subsection (8) allows the police to disperse the gathering if "public order is likely to be endangered if the gathering continues" whilst section 26 allows the authorities to prevent a gathering from taking place. These powers give the authorities too much control over political gatherings. Whilst "public order" is once again used to justify the law, it is left undefined. This gives the police powers to disperse gatherings that they simply oppose politically, rather than ones which are getting unsafe.

In addition, the POSA does not define what constitutes a "likely" threat to public order. At the very least, such a broad power allows the police to constantly supervise gatherings in order to look out for any likely threats. This can lead to extensive surveillance and the collecting of information about the content of such gatherings or their attendees. Clearly, this threatens an individual's right to information privacy.

Section 29 of the POSA gives the police the power to "disperse" political rallies, using "reasonable force". The police can apply this power whenever the authorities have not given permission for a meeting to go ahead. Given that the authorities often ignore notices, this leads to many peaceful

gatherings being dispersed because of bureaucratic failures. Often, the police will also use these powers as a pretext for unlawfully arresting any HRDs in attendance. According to Amnesty, "the charges against them [are eventually] dropped or dismissed in court due to lack of evidence"[53]. However, the time spent in police custody prior to trial allows the authorities to search HRDs under a false pretence, flouting their rights to bodily privacy. The names and personal details of HRDs can be collected in custody, and possessions such as mobile phones or wallets searched for information. Such information can be used to build a profile of HRDs, with a look to keeping them under surveillance in the future.

The powers in the POSA, which enable the surveillance of HRDs, are compounded by section 32. This section allows the police to inspect the identity documents of any person over 16 in a public place. This is a blanket power, which does not require an individual to commit any wrongdoing. Restricting an individual's rights to keep their personal identity secret flouts their right to information privacy. In the context of state violence against political opponents, making oneself known to the authorities can have serious repercussions. Amnesty believes that the overall effect of these provisions is to "discourage people from attending political gatherings"[54].

5.11. Criminal Law (Codification and Reform) Act 2004

The POSA originally contained a number of repressive provisions criminalising negative statements made about the Government, the police and other authorities. These were a significant and unjustified assault on free expression, aimed at criminalising the opinions of the Government's political opponents. Unfortunately, these provisions were revived in the Criminal Law (Codification and Reform) Act 2004 (CODE) and, in many cases, the punishments became more severe.

The main provisions for our purposes are section 31, section 33 and section 177. The first of these sections reintroduces sections 15 and 16 of the POSA, making it an offence to publish "wholly or materially false" statements which incite or promote public disorder, adversely affect the defence or economic interests of Zimbabwe, undermine public confidence in law enforcement or interfere with any essential service. These provisions are extremely broad and as Amnesty stated about the POSA provisions:

> The authorities may use these provisions to target the independent media and human rights activists who document and expose human rights violations perpetrated by the Government and its agents, as these activities could now fall into the category of undermining public confidence in the security forces[55].

Section 33 introduces an offence, punishable by up to one year in prison, of making a statement which "engenders feelings of hostility towards or causes hatred, contempt or ridicule of" the President. This is clearly antithetical to democratic expression, a free media, and the ability to criticise elected

leaders without fear of criminal punishment. Moreover, the Supreme Court came close to endorsing this view in November 2013, declaring that the law was unconstitutional and advising prosecutors not to be overzealous in charging people who comment about the President "in drinking halls and other social places"[56]. Over 80 cases have been filed in recent years under the law. Thus, while the number of independent newspapers has increased during 2012, many have felt forced to exercise self-censorship due to the threat of criminal prosecution[57]. Moreover, as Freedom on the Net highlights, "CODE applies equally to online journalists and reporters for traditional media"[58].

These provisions have, in fact, led to a number of arrests and trials in Zimbabwe. According to Zimbabwe Lawyers for Human Rights, the drafting is "too broad, wide and vague so as to make the law uncertain"[59]. This means that individuals are unable to regulate their private lives in deciding what they can and cannot say, for fear of the possibility that it will be taken as an insult to the President.

Breaking the law in section 177 could lead to imprisonment for up to two years. This criminalises making statements undermining the authority of the police. This includes making statements exposing a police officer to contempt, ridicule or disesteem. Given that many sources suggest that there is significant corruption in the Zimbabwean police force, this provision gives the police a worrying amount of protection and impunity against the democratic opinions of Zimbabwean citizens.

The Insult Cases

MP Douglas Mwonzora was arrested under section 33 of the CODE after speaking at a rally in which he allegedly compared President Mugabe to a goblin and called the Government "full of thieves". In defence, he argued that, as a politician, his freedom of expression required him to be able to make "political utterances" against a political opponent without the fear of being imprisoned.

In May 2013, MDC-T Youth Leader Solomon Madzore was arrested and detained for allegedly calling the President a "limping donkey" who should be put out to pasture. His representative has since filed an application to the Constitutional Court for the offence provided for by section 33 of the CODE to be struck down, on the basis that it violates three of Mr Madzore's rights under the new Constitution: the right to campaign, the right to hold and communicate opinions, and the freedom of expression.

There is also concern that the provisions will limit the ability of HRDs to mount an effective defence in court where they have been arbitrarily arrested by the police. As Human Rights Watch reports, "police and prosecutors have been highly partisan and biased in their investigations and prosecution of acts of violence between supporters of [ZANU-PF and MDC-T]"[60].

A particularly worrying application of the law can be seen in the recent arrest of lawyer Beatrice Mtetwa[61]. Ms Mtetwa was arrested whilst trying to represent one of her clients whose house was being searched by the police,

she believed unlawfully. An order from the High Court for her release was subsequently ignored. Cases such as this show that the state's infringement of the right to privacy even intrudes on the constitutionally protected lawyer-client relationship. By ignoring a subsequent court order, the police also flouted the constitutional role of the judiciary. This kind of political interference in the justice system should not be allowed in law. However, Beatrice Mtetwa's case is not unique; it is just one example of the "sustained and unrelenting attack"[62] that is currently being waged against the legal profession in Zimbabwe[63].

5.12. Privacy and Democracy: the 2013 Elections

Against the current legal backdrop in Zimbabwe, it should be of little surprise that instances of invasive state surveillance on civil society are uncovered on almost a daily basis. While the new Constitutional guarantees basic freedoms, evidence on the ground indicates there is a long way to go before standards such as privacy and freedom of expression are properly protected in practice.

It is important to realise that this has knock on effects for the entire democratic process. It would seem a reasonable hypothesis to suggest that surveillance in Zimbabwe tends to increase during periods of high political activity. In fact, the evidence of surveillance surrounding the 2013 elections neatly supports this conclusion.

It was alleged by the MDC and the outgoing Prime Minister Morgan Tsvangirai as part of an application to the Constitutional Court that the Israeli company Nikuv Projects International (NPI) has been contracted by ZANU-PF to help rig the July elections[64]. In particular, the security firm was accused of manipulating the voters' roll in MDC strongholds under the direction of the Central Intelligence Organisation, Zimbabwe's internal security arm. The ZANU-PF Registrar-General Tobaiwa Mudede has refused to explain why his department paid over $10 million to NPI. The company had a history of controversy in Africa, having been subjected to similar accusations after Zambia's 1996 elections, as well Zimbabwe's much disputed elections in 2008. Over the years, NPI has been forced to deny claims that it is in fact a front for the Israeli intelligence agency Mossad. Whether the MDC's legal challenge is capable of lifting the lid of secrecy from Nikuv's activities in Zimbabwe is a matter which remains to be seen. Further, there were numerous reports of heavy police presence in the voting booths, thereby compromising the secrecy of the vote and privacy of the voters

To cite a separate case, in the weeks surrounding August 2013, several human rights and independent media organisations were hit by internet-based attacks, disabling their websites and preventing their users from accessing information. Among the sites that were immobilised were www.electionride.com and www.hrforumzim.org, both of which were in the process of monitoring the election results. While it remains beyond the capabilities of such organisations to establish the true sources of these highly

sophisticated attacks, their convenient timing so as to coincide with the allegedly irregular elections of that month has led many observers to draw their own conclusions. According to Lance Guma of Nehanda Radio, one of the hosting providers that was hit, “every time you have a big story, it depends on whether the Government wants people to read it or not,” the suggestion clearly being that efforts were being made by the Government to curtail the information about the election results.

Reports that the Government has been seeking Chinese assistance to try to increase its ICT monitoring capacity perhaps shed further light. At the Robert Mugabe School of Intelligence, also known as the National Defense College, Chinese instructors were reportedly set to train Zimbabwean military personnel in a range of intelligence technical skill areas and the institute was to “feature Chinese equipment built by technology giant Huawei to eavesdrop on diplomatic, political, business and private communications”. The institute would reportedly train Cryptologic Linguists, Signals Intelligence Analysts, Human Intelligence Collectors, Military Intelligence (MI) Systems Maintainers and Integrators, Counterintelligence Agents, Imagery Analysts, Common Ground Station (CGS) Analysts, Intelligence Analysts, [and] Signals Collectors or Analysts.

Whatever the background, it is clear that the deployment of surveillance tactics in Zimbabwe poses a wider danger than merely to each individual’s right to a private life.

---

[1] US Department of State, Bureau of Democracy, Human Rights and Labor, ‘2010 Human Rights Report: Zimbabwe’, p. 12
[2] Constitution of Zimbabwe as amended at 30th October 2007, up to and including amendments made by Constitution of Zimbabwe (Amendment) No. 18 Act, 2007 (Act No. 11 of 2007)
[3] Davies, A. ‘Case comment: RT(Zimbabwe) & Others v SSHD; KM (Zimbabwe) (FC) v SShd [2012] UKSC 38, accessed at: http://ukscblog.com/case-comment-rt-zimbabwe-km-zimbabwe-fc-v-sshd-2012-uksc-38
[4] US-DOS report, p. 26
[5] A copy of the Global Political Agreement can be found at: http://www.copac.org.zw/index.php?option=com_content&view=article&id=19&Itemid=128
[6] Human Rights Watch ‘World Report 2013: Zimbabwe’, accessed at http://www.hrw.org/world-report/2013/country-chapters/zimbabwe
[7] Sokwanele, ‘GPA demands a genuine commitment towards achieving freedom of expression in Zimbabwe’, May 19 2009
[8] US-DOS report, p. 13
[9] United Nations Human Rights Office (2012) ‘Opening remarks by UN High Commissioner for Human Rights Navi Pillay at a press conference during her mission to Zimbabwe’, accessed at: http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=12192&LangID=E
[10] Foreign & Commonwealth Office, 2013
[11] OHCHR, 2013c
[12] A copy of the constitution, in it’s draft form, can be found at: http://www.copac.org.zw/index.php?option=com_content&view=category&layout=blog&id=66&Itemid=329
[13] Solidarity Peace Trust, ‘The Constitution and the Constitutional Process in Zimbabwe’, accessed at http://www.solidaritypeacetrust.org/703/the-constitution-and-the-constitutional-process-in-zimbabwe/
[14] A copy of the UN Declaration of Human Rights can be found at: http://www.un.org/en/documents/udhr/
[15] Heyns, C (2002) ‘Civil and Political Rights in the African Charter’ in Evans, M. and Murray, R. (eds.), The African Charter on Human and People’s Rights, Cambridge: Cambridge University Press

[16] See Article 8, 'Right to Respect for Private and Family Life' in the European Convention on Human Rights
[17] Zimbabwe Lawyers for Human Rights, 'An analysis of the COPA Final Draft Constitution of 1 February 2013'
[18] Constitution Watch 35/2013. 2013. "Giving Effect to the New Constitution: Criminal Proceedings". Retrieved November 20 from http://www.zimbabwesituation.com/news/constitution-watch-352013-2/
[19] Ibid
[20] Amnesty International, 'Zimbabwe: Rights Under Siege 2003' AFR 46/012/2003, p. 13
[21] US-DOS report, p. 23
[22] Ibid.
[23] Rights Under Siege, p. 22
[24] Zimbabwe Lawyer's for Human Rights petition to the African Charter, accessed at: http://www.achpr.org/files/sessions/6th-eo/comunications/284.03/achpreo6_284_03_eng.pdf
[25] MISA-Zimbabwe (2009) 'Amend AIPPA: African Commission', accessed at: http://www.kubatana.net/html/archive/media/090828misaz.asp?sector=MEDIA
[26] Zunguze, M. 'E-Knowledge for Women in South Africa', accessed at: http://www.giswatch.org/sites/default/files/Zimbabwe.pdf
[27] Rights Under Siege, p. 17
[28] Special Representative of the Secretary General on Human Rights Defenders, Report to the 59th Session of the UN Commission on Human Rights, February 2003, E/CN.4/2003/104/Add.1
[29] Coltart, D. (Sep 2012) "Promoting the universality of the Rome Statute 10 years after its entry into force: Challenges for States and international Organisations and the role of Parliamentarians - a Zimbabwean perspective.",
[30] A copy of the Interception of Communications Act can be found at: http://www.kubatana.net/docs/legisl/ica_070803.pdf
[31] OpenNet Initiative, 'Internet filtering in Zimbabwe 2006-2007', accessed at: https://opennet.net/studies/Zimbabwe2007
[32] Freedom House, 'Freedom on the Net 2012: Zimbabwe', p. 9
[33] Blagbrough, Charlie (2013), 'State Surveillance in the digital age: the implications for freedom of expression and the right to privacy', Side event to the 23rd session of the Human Rights Council
[34] La Rue, Frank (2013) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', Human Rights Council 23rd Session, A/HRC/23/40
[35] Manika, C. (2007) 'Interception of Communications Act sparks debate and fear: Zimbabwean Human Rights Activists Up in Arms', accessed at: http://thewip.net/contributors/2007/09/zimbabwean_human_rights_activi.html
[36] Freedom House (2012), 'Freedom on the Net 2012 - Zimbabwe', accessed at: http://www.ecoi.net/local_link/227488/335378_en.html
[37] La Rue (2013)
[38] Ibid. p. 14-15
[39] Ibid. p. 14
[40] Zimbabwe Lawyers for Human Rights (2006), 'Submissions to the parliamentary portfolio committee on transport and communication, about the interception of communications bill'
[41] 9 EHRR 433(1987)
[42] (1989) 67 DR 98
[43] Rights Under Siege, p. 21
[44] Ibid.
[45] Independent Journalists Association of Zimbabwe, 'Submission on the Access to Information and Protection of Privacy Act', accessed at: http://caselaw.ihrda.org/doc/297.05/view/
[46] Rights Under Siege, p. 38
[47] MISA report on the Broadcasting Services Act, accessed at: http://www1.umn.edu/humanrts/research/ZIM%20Broadcasting%20Draft.pdf)
[48] Rights Under Siege, p. 16
[49] Coltart, D. (2001) 'A critique of the Zimbabwean Broadcasting Services and Political Parties Finances Acts', accessed at: http://davidcoltart.com/2001/10/a-critique-of-the-zimbabwean-broadcasting-services-and-political-parties-finances-acts/.
[50] Rights Under Siege, p. 20
[51] Amnesty International, 'International Report 2013', accessed at: http://www.amnesty.org/en/library/asset/POL10/001/2013/en/b093912e-8d30-4480-9ad1-acbb82be7f29/pol100012013en.pdf,
[52] Ibid. p. 301
[53] Rights Under Siege, p. 17
[54] Rights Under Siege, p. 21
[55] Ibid. p. 19
[56] www.zimbabweelection.com/2013/11/10/bbc-reports-zim-court-says-robert-mugabe-insult-law-invalid/

[57] US-DOS report, p. 24
[58] Freedom on the Net
[59] Zimbabwe Lawyers for Human Rights (October 2012), 'The Legal Monitor: Edition 163'
[60] Human Rights Watch ,'World Report 2012: Zimbabwe', accessed at: http://www.hrw.org/world-report-2012/world-report-2012-zimbabwe-0
[61] Webber, F. (2013) 'The arrest of lawyer Beatrice Mtetwa: a new low for lawyers in Zimbabwe' in The New Statesman
[62] Zimbabwe Lawyers for Human Rights (June 2013), 'Right of Reply to Herald Article of 12 June 2013'
[63] See the client-lawyer confidentiality example above.
[64] www.dailynews.co.zw/articles/2013/08/10/nikuv-paid-10-million-to-rig-polls-mdc

6. Surveillance and Privacy in South Africa

6.1. The Legal and Constitutional Definition of Privacy

We have previously outlined a working definition of the term privacy, clarifying four main aspects of the individual's right to privacy: information privacy, bodily privacy, privacy of communications, and territorial privacy. We have also noted that privacy might be viewed as “the right to be left alone”, and “the right to control who knows what about you, and under what conditions”.

In order to determine examples of best practice that are relevant to Zimbabwe, it is necessary to also examine surveillance and constitutional and legal definitions of the term “privacy” in a comparable region. This section will therefore examine the definition and application of the term in South Africa, as well as how it is applied and regulated by regional and international initiatives such as the African Charter on Human and Peoples' Rights (ACHPR).

6.2. Privacy in South Africa

The South African Constitution provides for the protection of many fundamental human rights. In response to widespread violations of privacy during the apartheid era, the South African Constitution of 1996 now specifically addresses and protects citizens' rights to privacy and personal liberty, balancing the need to protect these rights with the need to maintain national security. Under Section 14 of the Constitution, the term “privacy” is defined as every citizen's right not to have their person or home searched, their property searched, their possessions seized, or the privacy of their communications infringed[1]. The right to freedom of expression, which includes the freedom to receive or impart information or ideas and the right to freedom of the press and other media, is constitutionally protected[2], along with the rights to peacefully assemble, demonstrate, picket, and present petitions[3]. These provisions might be considered relevant to our study because HRDs frequently find themselves advocating against violations of such rights.

Additionally, Government surveillance is often a precursor to the curtailment of such fundamental rights. Chapter 11 of the Constitution, relating to the operation of the security services, states that the Republic’s security services, which include the police service and “any intelligence services established in terms of the Constitution”, “must act, and must teach and require their members to act, in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic”, and that in order to ensure transparency and accountability, “multi-party parliamentary committees must have oversight of all security services”[4]. It is clear, therefore, that the right to privacy and the need to constitutionally protect this right are recognised in South Africa's Constitution.

Whilst both the right to privacy and the perceived importance of this right are clear from the Constitution, the document also outlines circumstances under which personal privacy may be breached. Broadly speaking, breaches of the rights set out in the Bill of Rights are allowed only “to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom”[5]. In the case of the right to privacy of communications, the circumstances under which the right may be violated are explicitly set out by the Regulation of Interception of Communications Act 2002 (RICA)[6]. The RICA governs the technical and security requirements for the interception, routing, storage and provision of fixed and mobile telephone communications, online communications, radio signals and metadata.

However, the extent of communications surveillance allowed under the Act has faced criticism. The most publicly evident effects of the Act, when it was introduced in 2002, were the requirements for citizens to register telephone SIM cards, and to identify themselves for Internet services. However, less clearly, the RICA also prohibited the provision of telecommunication services which can not be intercepted, and required service providers to store communication-related information, such as numbers dialled and the duration of telephone calls, pursuant to a warrant. Critics have expressed concern about the amount of personal data that these provisions theoretically make available to the Government. Reports that two FinFisher spyware command and control centres have been hosted by South Africa's Telekom network have done little to allay fears about the extent of communications surveillance in the country—although the presence of these centres does not demonstrate that the Government is making use of them[7].

Further concerns have recently been raised about a number of bills, which arguably have the potential to enable state monitoring and interception of online communications, whilst inhibiting the free transmission of ideas and information protected by Section 16 of the Constitution. The General Intelligence Laws Amendment Bill, debated by a parliamentary committee in April 2013, proposed amendments to the 1994 National Strategic Intelligence Act No 39 that would allow the interception of “foreign signals intelligence”—signals emanating from, passing through, or ending in the Republic—in line with the “intelligence priorities of the Republic”.

Whilst this appears to directly contravene the guidelines established by the RICA, the minister of state security and the State Security Agency have reportedly clarified that the RICA only applies to domestic situations. As such, judicial permission would not be required before such communications interceptions could be conducted, introducing the potential for unconstitutional invasions of privacy. Since any electronic communications services operating within South Africa but relying on a foreign server would result in signals crossing the Republic's borders, this Act would also potentially allow for the surveillance of communications originating from the country.

Whilst the RICA enables the collection of personal data, Section 32 of the South African Constitution also states that citizens have the right to access "any information held by the state"[8]. This right is notionally supported by the 2001 Protection of Access to Information Act (PAIA), which, enforced by the judiciary and South Africa's Human Rights Commission, allows individuals the right to access personal information held by either the public or the private sector. In theory, the right to obtain any personal information held by the state supports the individual's right to privacy by promoting governmental transparency. However, the PAIA requests are often dealt with inefficiently or ignored altogether, thus limiting the potential benefits of the Act[9]. For example, a request submitted by the South African History Archive's (SAHA) for access to archived Truth and Reconciliation documents relating to the apartheid era did not result in access to the information being granted until two years and six months after the request was made. This demonstrates that, although legislation is in place to support the right of access to information, not all institutions fully recognise this right, and the mechanisms regulating the processing of such requests are still inefficient.

Compounding this problem is South Africa's current Protection of State Information bill, which, despite having been substantially amended in 2013, still contains elements that have attracted heavy criticism, and are likely to have a significant effect on citizens' ability to access state-held information. Not only does the Bill grant the power to classify information to a wide number of authorities other than the security services, thus potentially paving the way for information to be unjustly rendered inaccessible in the name of "national security", it also provides inadequate protection for whistle-blowers, journalists, or public advocates who reveal classified information in order to expose wrongdoing, and contradicts the PAIA with regards to the procedure permitting applications for the declassification of information. It is evident, therefore, that access to personal information held by the state may be obstructed in a number of ways, despite the existence of legislature designed to combat this.

Prompted in part by stipulations of the 1995 European Union (EU) Data Protection Directive, which required the guarantee of an "adequate level of protection" for personal data in countries conducting business with the EU, South Africa has also addressed issues of personal data protection[10]. A South African Law Reform Commission discussion paper commissioned by the Parliament in 2000 stated that "[data] or information protection forms an element of safeguarding a person's right to privacy", providing for the legal protection of an individual whose personal information is being "collected, stored, used or communicated by another person or institution"[11]. The Commission recommended the enactment of legislation to ensure the protection of eight core information protection principles, and to regulate the processing of personal data in both the private and public sectors[12].

It was recommended that a data protection authority be established in order to ensure that the use, storage and dissemination of personal data intruded on the constitutionally guaranteed right to privacy as little as possible. The Protection of Personal Information (POPI) Bill passed by the South African

Parliament on 22nd August 2013 offers the country's first comprehensive data protection legislation. As recommended, the Bill established eight core data protection principles, based on models used by countries complying with the EU Data Protection Directive. Significantly, it requires individuals to consent to having their personal information processed; introduces mandatory notifications of data breaches; and limits the processing of information relating to religious beliefs, race or ethnicity, trade union membership, sexual orientation, and political opinions. At the time of writing, the Bill is still awaiting the signature of President Zuma, but, if signed into law, would amount to a significant improvement in the protection of citizens' personal data.

Although the right to "privacy" as a concept has evidently been addressed by South Africa's Constitution and, to an extent, its legislation, it is undeniable that technological developments have posed threats to this right that have not yet been adequately addressed. When considering how privacy in Zimbabwe is to be protected, it will be necessary to consider the impact of technological developments and availability, in order to avoid, as far as possible, such issues threatening privacy in the future.

6.3. Relevant Regional and International Treaties and Conventions

In addition to the Constitutional provisions outlined above, South Africa has ratified major international human rights treaties including the African Charter on Human and Peoples' Rights (ACHPR) and the International Covenant on Civil and Political Rights (ICCPR). South Africa is also a member state of a number of international organisations that aim to protect human rights, including the Southern Africa Development Community Organisation of Public Accounts Committees (SADCOPAC). The way in which these organisations work to support human rights in South Africa is particularly relevant to Zimbabwe because both countries have ratified the ACHPR and ICCPR. As such, it is beneficial to examine the impact that supranational bodies, particularly the ACHPR, have had an impact within the South African legal framework, and the extent to which international standards have been incorporated into national law.

The African Charter on Human and Peoples' Rights is comprehensive in its coverage and protection of human rights, guaranteeing the individual's right to respect for dignity, respect for the integrity of his person, and respect for "liberty and... the security of his person"[13]. The rights to freedom of conscience, and the profession and free practice of religion are also protected, as well as the rights to receive information, express and disseminate opinions within the law, and to freely associate and assemble within the boundaries of the law[14]. The expressly guaranteed right to "privacy", however, is notably absent. In addition to this omission, the ACHPR has been criticised for failing to provide the African Commission on Human and Peoples' Rights, established by Article 30 of the Charter, with sufficient powers with which to effectively implement decisions or recommendations in

cases in which a state has been found to have violated a guaranteed human right. Reports produced by the Commission are to be transferred to the states concerned, and although the Commission "may make... such recommendations as it deems useful", critics have argued that it has been denied "teeth with which to bite those found to have flouted it"[15].

The South African Constitutional Court, however, has produced a number of privacy-related rulings. For example, in the case of De Rueck vs. Director of Public Prosecutions (Witwatersrand Local Division) and Others, the Court considered a challenge to the validity of constitutional provisions prohibiting the possession of child pornography. The Court ruled that, in this instance, it was justifiable to limit the right to personal privacy and the right to freedom of expression in order to protect the dignity of children, and to avoid potentially harmful situations from arising. In this case, despite the ruling, it is evident that the Court as a fundamental entitlement considered the constitutionally protected right to privacy.

Although the ACHPR may be more effective if it were able to provide methods through which decisions and recommendations could be implemented, in South Africa's case, the South African Human Rights Commission (SAHRC) has the power not only to investigate and report on the observance of human rights, but also to secure appropriate redress in cases of human rights violations[16]. As such, the ACHPR's lack of power to ensure redress or punishment for human rights violations does not present an insurmountable obstacle. When considering the protection of the right to privacy in Zimbabwe, it would be advisable to note the additional powers that have been afforded by the Constitution to the SAHRC in order to ensure that its decisions and recommendations are respected at a national level.

In view of the absence of the right to privacy in the ACHPR, it is necessary to examine the privacy protection provided by other supranational bodies. The African Union (AU), of which Zimbabwe is a member state, provides an additional source of regional legislation. Of particular relevance for present purposes is the Draft Convention on Cyber Security. This Convention seeks to establish an integrated regional legal framework for cyber security, which simultaneously protects the fundamental rights and freedoms of persons affected.

Whilst the Draft Convention does not contain a direct right to privacy, it does indicate at a number of points that it is compatible with such a right. Article II – 2 states that AU member states should "put in place a legal framework with a view to establishing a mechanism to combat breaches of private life likely to arise from data gathering, processing, transmission, storage and use of personal data". In addition, it provides a number of substantive provisions, which guarantee a degree of privacy in relation to online "personal data". For example, according to Article II – 35, member states must take necessary measures to prevent the gathering of "sensitive data" on the basis of political views, trade union membership, racial or ethnic considerations.

In spite of some valuable provisions, critics have also identified a number of contentious clauses have. Article II - 28(2) and Article II – 36(9) permit the processing of personal and sensitive data by anyone acting on behalf of the state or any public institution working for public interest and state security. To include such broadly worded exceptions would be a serious caveat in the Draft Convention's protection of privacy and will be particularly liable to abuse within the African context. Until such clauses are removed from the Draft Convention, its implementation does little to bolster the right to privacy across Africa.

---

[1] Constitution of the Republic of South Africa, 1996, Section 14.
[2] Constitution of the Republic of South Africa, 1996, Section 16.
[3] Constitution of the Republic of South Africa, 1996, Section 17.
[4] Constitution of the Republic of South Africa, 1996, Section 199.
[5] Constitution of the Republic of South Africa, 1996, Section 36.
[6] Regulation of Interception of Communications Act 2003, amended 2006.
[7] Marquis-Boire, Marczak, Gaurnieri and Scott-Railton. 2013. Their Eyes Only: The Commercialization of Digital Spying. Citizen Lab and Canada Centre for Global Security Studies. P.101.
[8] Constitution of the Republic of South Africa, 1996, Section 32.
[9] Open Democracy Advice Centre 'Southern Africa Summary Country Report: Open Society Institute Justice Initiative: 2004 Monitoring Study'.
[10] South African Law Reform Commission Discussion Paper 109, Privacy and Data Protection, 2005, p. v-vi.
[11] South African Law Reform Commission Discussion Paper 109, Privacy and Data Protection, 2005, p. iv.
[12] South African Law Reform Commission Discussion Paper 109, Privacy and Data Protection, 2005, p. vi.
[13] ACHPR 1981 Articles 4, 5 and 6.
[14] ACHPR 1981 Articles 8, 9, 10 and 11.
[15] ACHPR 1981 Articles 52 and 53; Hansungule 2009: 233-234.
[16] Constitution of the Republic of South Africa, 1996, Section 184.

Part II – FIELD RESEARCH

7. Human rights and Experts' views on surveillance and privacy issue in Zimbabwe

Findings in this part are drawn from dialogues with key informants working in leading NGOs, and with legal experts, ISPs, Internet Access Providers (IAPs) and lastly with the regulator Portraz. The purpose of the interviews and focus groups was mainly to fill in the gaps identified in the literature review. Notes from the interviews are summarized and full interview transcripts can be accessed on request. Most interviews did not follow the prescribed questionnaire, which was merely used as a guide.

These leading activists, most of whose names are withheld shared their views about surveillance generally and specifically on HRDs and how it relates to privacy in Zimbabwe in the dimensions that follows.

7.1. Key Findings and Recommendations from the Field Interviews

7.1.1. The Government's Legal Capabilities

- A key informant from an IAP stated that Government's powers to monitor as opposed to intercepting are drafted in very wide terms and enables the government to monitor anything that passes through the network, even private conversations that are not intended for them, leaving IAPs and ISPs with little room to protest.
- While the Government has wide legal capabilities under the ICA, it appears officials have little grasp of Internet law in order to aid prosecutions. For example, a famous facebook prosecution failed because the post had been deleted. However, in 2009 the state sustained a prosecution of bank workers on the basis of an intercepted email, which the prosecution subsequently printed out.

7.1.2. The Government's Technical Capabilities

- According to a leading IAP, the Government has sufficient technical capabilities to intercept communications. Although Zimbabwe receives technical expertise from other nationalities, this is done in such a way as to transfer the skills in order to boost the Government personnel's technical capacity.
- IAPs are afraid to disclose where the Government acquires its technical expertise from, due to the political set up in the country.
- All key informants agreed that there is evidence that, during the 2013 elections, the Zimbabwean Government might have contracted the Chinese Intelligence services to deny web access on leading websites reporting about the elections.
- In order to aid its capabilities, the Government requires IAPs, under the ICA, to install systems, at their own cost, that would be incompatible with their own interception operating system. However, it is the Government's personnel that carry out the interception.

7.1.3. On adequate safeguards e.g. judicial oversight

- There is a lack of judicial oversight, as demonstrated by the tendency to keep the remit to intercept communications under the President's office, to prevent the opposition from having access to powerful ministries when it was in power, as well as the fact that the Ministry for Communications—rather than the courts—decides on whether to authorise interception or not.
- With the ascendance of a new Constitution, there is a presumption of constitutionality for all the laws including the ICA, until the Parliament passes amendment or until the constitutionality of the laws is successfully challenged in the Constitutional Court.
- The new Constitution has an explicit right to privacy. The contents of the first draft came from the South African and Kenyan Constitutions and the final draft was slightly modified, without adding anything to the provisions.
- The Constitution contains the "necessary and proportionate" clause. The clause, which was deliberately placed at the back of the Constitution, tends to protect state interests.
- There are few legal provisions governing digital information. The previous attempt of the Government to modify the Post and Telecommunications Act, the legal and technical language used was inappropriate.

7.1.4. The Government's Attitude towards Digital Rights

- The Government of Zimbabwe has always been wary of the power of technology, as exemplified by the early cases between Econet Wireless and the Minister of Technology, where the Government wanted to retain a communication's monopoly, as well as in the recent directive to ban mass texting.

7.1.5. The Motive for Intercepting, the Modes of Interception & the Use of Intercept Evidence

- As stated in the objectives of that Act, interception is not necessarily for the purpose of prosecuting but in the purpose of combat the real or perceived national threats and other criminal activities.
- A number of interceptions have nothing to do with people posing a threat to the state in any way but are a manifestation of institutional invasion of privacy, sometimes motivated by sheer malice. An example of this is the interception and publishing of Mrs Tsvangirai's intimate emails.
- Not all HRDs constitute a sufficient threat to the state. Interception may hence be primarily used for intimidation or harassment than seeing cases brought for prosecution. It induces self-censorship, as people might be unwilling to say something of importance for fear that it may be used against them.
- There have been cases of communications of interception which do not exactly fall under the ICA. The Andy Meldrum case, for example, which entailed downloaded information from the website, those involving video recorded evidence, as for example the Asiagate scandal hearing, confiscation of laptops, and so on.
- Non-state actors, for example Nigerian actors, also intercept communications for criminal purposes by using malwares.

7.1.6. Impact on other Rights

- In the Zimbabwean context, there is an overlap between the freedom of speech and the right to privacy. For example, the confiscation of radios invokes both the freedom of speech, the right to privacy and access to information, but also impacts on the right to privacy in voting.
- The inter-relation is also seen in other laws—apart from the ICA—which need to be reformed in order to bring about holistic changes. An example of this is the AIPPA.
- In Zimbabwe, there is generally a lack of transparency, as well as broader issues relating to the access to information.

7.1.7. Advocacy Strategy

- From an advocacy perspective, it is always better to approach the legislator and the authorities with a plan that advances the right to privacy without undermining state security.
- There is no parliamentarian at the moment who is known to be keen on privacy issues, contrary to the freedom of expression and laws such as the POSA and the AIPPA.
- A significant barrier to advocacy is that as the ICA criminalises talking about what has been done on the law, making it difficult to discuss specific cases.

7.2. Interview summaries

7.2.1. Informant 1: IAP

Distinction between interception and monitoring

Does the Government monitor and intercept communications?

Question: Does the Government intercept and monitor private communications?
Answer: The Government intercepts and monitors private communications. The ICA gives a blank check to the Government to monitor. While interception follows a proper procedure, monitoring can be done anytime and they monitor anything that passes through our network, “We as operators we really don’t have much power, because whatever they have is mirrored on their platform so when they are monitoring its not as if their personnel is present to see what they are seeing so you are right if they want to monitor part of the conversation they think they are interested in then it develops into something else there is nothing that stops them from listening to what is not intended for them or on anything that has no bearing to what they are looking for”.

The Government’s & IAPs’ technical capabilities to intercept

Question: What is your view on the provision in the ICA, which compels ISPs and IAPs to have technical capabilities to intercept on behalf of the Government and whether IAPs can also do the work behalf of the Government or whether the Government does so independently?

Answer: The ICA compels IAPs to make sure that ‘our system can be intercepted so you make it comparable with whatever system that they are going to put on our system so that its enabled for interception so we don’t have to intercept on their behalf its their system that is has to be compatible with ours. So we went through a whole process of making sure that the platform is compatible with whatever equipment they were going to install on

our system. So they do the job themselves and use their own equipment so we do not have time to do the interception on their behalf.

Question: Does the Zimbabwean Government really have advanced expertise to intercept since some people think Zimbabwe has not yet reached that level of expertise?

Answer: Yes they do. You will be surprised. Here and there of course people get assistance form other nationalities that are probably more advanced and there is skills transfer. Once they get those people they train their locals, so there is skills transfer and these people cannot be here to train for them so they transfer their skills, train these guys and they intercept for them.

Question: Where do you think they get their technical capabilities, both in terms of training and equipment?

Answer: To be honest I wouldn't know. Probably POTRAZ would have known because they work with the Government and they are the implementers. You can speak to the Director General Mr Marisa. It is important you speak to the highest level. We also have people with expertise that you would also want to speak to like we have 200 engineers in this company, though due to the company policy they might not want to answer so the communications manager who will then seek permission from the team executive officer. Because you know the political set up in this country you don't want to say too many things and end up in trouble with the company. You may end up getting generalized information whereby particularized information could be obtained from those with the expertise.

The Government's attitude towards digital rights:

Question: Access to the Internet and mobile technology came quite late to Zimbabwe because the Government was paranoid of the Internet and what it was capable of doing, what would be your comment to this?

Answer: You can't beat technology: whilst the Government was being paranoid, the industry was just moving on. Zimbabwe is one of those countries whereby we advanced technologically very fast.

Question: Have you ever heard of the Econet Supreme Court decision that involved the Government and Telecel implicating the rights to privacy and free expression? Do you have any views on that?

Answer: There are quite a number of cases anyway of ECONET versus the Minister of Telecommunications. They are all about the right the right to freedom of expression, the breakdown of the monopoly of Telecommunications industry resulting in Econet being licensed. So it's a series of judgments around such issues.

Judicial oversight

Question: Apart from the fact that the ICA doesn't require reasonable suspicion and that it has blanket powers to monitor, the other concern we picked up relates to the lack of separation between the judiciary and political roles because a Government minister is the one who authorizes interception, what is your comment?

Answer: I think that is driven by need to keep everything under the President's office and not spread it to the ministries. It is sensitive and interception is very serious.

Question: Another informant told me that when the Government realized that the Interception Department was likely to fall under the opposition portfolio, they moved to separate ministries and allocated it to the Ministry of Transport instead of the Ministry of Information Technology.

Answer: Everything under the GNU was to try and stop other people from having access to powerful positions.

Usage of intercepted messages

Question: When they intercept communication, are they going to use it in courts or is it for intelligence purposes?

Answer: I think if you go to the objectives of that Act, it will tell you what their concerns are, it defines the need for interception and they are basically trying to defend the interception. It is not necessarily for purposes of prosecuting but purposes of whatever they perceive as a national threat and other criminal activities.

Question: Do you know of any case where intercept evidence has been used in court?

Answer: No I am not aware of any. Not that I have not had any time to research on it.

7.2.2. Informant 2: AB

Background: AB is a renowned civil rights organisation.

Threat to national security argument:

Question: Please describe the ways surveillance impacts on civil liberties, in particular the right to privacy for human rights defenders and other people opposed—or perceived to be opposed—to government policies in Zimbabwe?

Answer: Well, the phenomenon of interception of communication is not uncommon. The real deal is about the notion of interception of communication vis-a-vis state security. The main purpose for intercepting communication in Zimbabwe as the ICA rightly state is for security purposes and those that are targeted are thought to be a threat to the state. Whilst we have heard about interception of communication in Zimbabwe, much of the intercepted information has not been used for prosecution.

Adequacy of safeguards:

Question: What national laws, regulations, practices and safeguards are there in Zimbabwe relating to political intelligence oversight and communications surveillance? In your own view, are these safeguards adequate?

Answer: There are primarily three issues**:**

1. In my own view, much of the interception of communication emanates not from a statutory point. A case in point is the issue of Elizabeth Tsvangirai's alleged adultery case, in which the state controlled media was awash with allegations that emails unscrupulously gotten from Elizabeth's account carried overwhelming evidence that she was seeing another man outside marriage. In this case, there was no warrant issued so as to justify entry into Elizabeth's account. Besides Elizabeth poses no threat at all to the state and it can be seen that the major motive for intercepting and publicizing her emails are primarily malicious and an unwarranted invasion of privacy. This is what is called institutional invasion of privacy.

Law reform

2. With the ascendance of a new Constitution, there is presumption of constitutionality of all the laws until Parliament passes amends or until the Constitutional Court sits and say this law is unconstitutional and in order for the Constitutional Court to do that someone has to approach the Constitutional Court and say this law is infringing on my right. The major question is there going to be appetite in the constitutional court to do that or from the ZANU-PF dominated Parliament?

This is very debatable. A likely scenario is that many of these laws are going to remain in effect and in the absence of strategic public litigation coupled with advocacy, it's going to be very difficult to see changes in some of the laws. In terms of operating space for some of these human rights defenders, my view is that not all activists constitute a sufficient threat to the state; hence interception may be primarily for intimidation or harassment than seeing cases brought for prosecution.

Rather it induces self-censorship. You will be unwilling to say something of importance for fear that it may be used against you. My other observation is that social platforms are not to be taken seriously. For example, the baba Jukwa, I think it was a timeous creation by the intelligence to cause diversion of attention to the real issues during a time emotions were high in the country. I for sure just did not take him seriously, it was a diversionary strategy as seen

by the number of hits, likes and friends as then it became apparent that what become talk was what baba Jukwa was saying rather than what was happening in the country.

What he was saying you could have read in the herald or H-metro and then it became of no value addition. Looking also at the kind of stuff that he is now posting after the election, he is like taking from what Zim-eye has said. Such platforms, whether he was giving information that he had intercepted or gathered, we never get to know but such its obvious that such platform was giving that got people excited but not in any way making any significant contribution to the democratic agenda.

I would have imagined that during the time we were going to have increased interface on people on social media and the numbers were going to get into millions and not hundreds and that the number of people following up on civil society on facebook was going to increase but it did not translate into any social catalytic kind of actions. There was just this excitement about it but there was no movement towards anything, it just became one of those things. Hence, my conclusion that it was an intelligence creation to occupy people while the real deal was happening somewhere, God knows where.

Government technical capabilities

3. The other aspect that has sort of proved that the level of sophistry that we need for interception of communication is not well developed as we think it is, case in point: the prosecution of this guy in Bulawayo for a post he is alleged to have posted on facebook would show that within the country, there is no one who has sufficiently grasped Internet law, and I was talking to this law professor and said, how can we modernize and incorporate aspects of Internet law in our curriculum because ours is just about how to practice law. For example, if we take a graduate of law from the US and our own from the UZ, we will be whipped because we have not been able to do that and so arguing and evidence based arguing becomes weak. So the state prosecutor will not be able to speak Internet language to say this website was accessed on this day, but that is what the Internet does, it tells you this page was accessed on such date, it was moved----, therefore being unable to sustain prosecution. If they could have say a few guys and send them to study Internet law, the security processes, what happens on a website if today is not where it was, how are we going to retrieve it. My view is we are going to get more cases of interception but there wont be successful prosecution.

There was one case, which I think, was in 2009 which is related where people worked in the banks and they were allegedly said to have insulted the president, not sure the finer details but you can check with the lawyers at Beverley court. They managed to successful prosecute them because it was an email printout but one could have argued that how sure are you that this was me, like arguing that one is not in control of the server and other unforeseeable, but unfortunately the lawyers did not explore all that. Whilst there is interception, there lacks sophistry in infringing on civil society related work.

Another good point is when Mukoko was arrested last year or this year, the police were saying those little radios are transmitters, are gadgets of transmitting into GBS but you see from the face of it anything that has FM is not a two way and even two way radios are limited. It's to a known receiver and the frequencies are in control of those spectrums. They should have therefore known that someone was abusing those transmitters if they had been abused. You see then that there is deliberate unwillingness to acknowledge what these things are and unable to do.

On advocacy tips

From an advocacy perspective, it is always good to approach the legislator and the authority that with a plan, because this research might help them tighten the loopholes because they will say ok its there so whatever product you are going to come up with, you need to advance the right to privacy but not undermine state security but even in the UK its a fact. It's even worse in the UK. Whether we have sufficient technology or not here, but it has been happening.

Necessary and proportionate clause in the constitution

Question: What does the Constitution say on privacy?

Answer: It provides for the right to privacy. There is however what is termed claw-back clauses to the Constitution, which work in the interests of the state. In the new Constitution, these have deliberately been placed at the back. There is a case involving Tawanda Nyambirai**.** The Constitutional Court is mandated to look at those issues.

7.2.3. Informants 3,4,5, and 6

Focus group with a team of technical and legal experts who requested anonymity

Privacy and freedom of expression

Question: We have seen the seizure of short wave radios and a rise in the clampdown of HRDs. Today we would like to look at all that but also communications interception specifically. How does it work in theory and how does it work in practice, are there any legal gaps and what needs to be done to fill in those gaps. Is the law and policy in line with international norms and standards?

Answer from V: Well most of it seems to be an overlap with freedom of speech and privacy because what you are saying about radios is freedom of speech as opposed to privacy, one cant expect radios to have much privacy.

Comments [A]: Well its arguable really because the definition of privacy differs, you know when we are looking interception, you need privacy in the first place to be given your space so once the state comes and takes your radio that's interception.

V: Yah, its against the law to confiscate radios. That is interfering with people's privacy.

Comments [A]: Last year when I spoke to ZLHR seeking their opinion on the confiscation of radios, they said if you have a radio and you don't have a license and the police are saying one should have a license, they should not confiscate the radio but ask you to get the license and if you fail within a certain period time, you would then be prosecuted.

Question: You raised an interesting point about the relationship between privacy and expression; in fact I was going to refer you to a report that was done by Frank Larue, you know that you cannot freely express yourself without the element of privacy. Like now we are expressing ourselves because we have been given our privacy, and if someone like a state agent would be listening, we would not be able to express ourselves freely. Do you agree?

Answer from V: You are taping us, which is not privacy.

Law reform (ICA, AIPPA, Communications bill etc)

Question: J you talked about the AIPPA and that the biggest challenge is not the ICA but AIPPA that needs to be reformed, would you mind expanding on that

J: That is what was in the GPA and nothing has been done.

Question: On what basis may the Government refuse access to information, do we have any law or any principles that govern access to personal information or maybe proportionality and necessity principles that adhere to international standards and norms? For example, other countries have data protection laws.

J: But there will remain the bill of rights that require referendums

BC: Another referendum would be too expensive.

J: I have one remark that you should put on the record because I think that it actually sums up the whole situation. It was a very long time ago but it was in relation to the communication bill. There was one public forum where the government was presenting its point of view and then there was discretion afterwards. The key speaker was someone from the University who since died, I wish I could remember his name but responded to the criticism I made about the bill and said look I don't know why anyone is worried here because

its only going to affect criminals and human rights activists, they didn't even mention terrorists. So I think that made it very clear what the whole purpose of this legislation intended to be.

V: So the original bill interestingly was something that could be directly used by political parties. It had a clause that obviously applied to political parties and we lobbied very hard but the MDC didn't really play ball with us but we did get it removed. But there was something that could apply directly to suppression of political parties.

Judicial oversight

J: The other crucial thing was the fact that there is no judicial oversight. But look at the end of the day I mean when I was talking to the portfolio committee I said look why are you doing this when any person who seriously wants to protect their communications is going to be using high level of inscription and Tafataona Mahoso responded, well just because we cant doesn't mean we shouldn't try.

V: We will look into that, I remember that.

Confiscation of laptops & usage of intercept evidence in courts

J: It's just pathetic really but at the end of the day, we need to look at whether or not there are any cases in the courts where evidence is being produced. I mentioned the Andy Meldrum one but that didn't involve interception of communications act at all it was just downloaded stuff from the website.

V: I thought they confiscated his laptop and certainly Farai Maguwu's trial there was a huge lot and they were not able to track him because they only have an email.

J: But taking his laptop wouldn't be something that requires the provisions of the ICA.

A: But it's related.

The Government's technical capabilities, overlap of communication interception and other forms of techno-based surveillance

J: As I also mentioned there have been a number of cases where people's emails are produced in court because they forwarded some joke about the top guy and it ends up in the wrong hands. So you are just asking for trouble, so just be sensible in what you say and what you forward. So that doesn't fall under the Act, so I am not able to point a finger at cases where the law has been used in public but clearly the fundamental thing is to set up the Interceptions of Communications Center, CIC I think its called and that does exist and I presume its operated by well I know nothing about where it is operated. If I look at where the Government operates other IT centers, it is unbelievably incompetent which makes me think that I really don't care what

they say. On the other hand, the Chinese built the centre so if they are serious they should employ Chinese experts. I think its very important to find out how Mr Tsvangirai's communications and emails end up on the front page of Sunday Mail. It's an outrageous breach of the Constitution, its absolutely illegal. I would like to know if someone had a laptop and forwarded things or did they get hold of a cell phone that did not have a password. Clearly it has nothing to do with the divisions of the Act.

A: yes that's what the POTRAZ lawyer was saying that we intercept where there is evidence that a crime is likely to be committed but she said we don't intercept private communication between you and your mum or between friends but again there are two cases that are somehow related the ZIFA case and the Asia Gate scandal where video evidence was used. It's similar to the Ari Ben Menashe and Tsvangirai case in Canada. In the ZIFA case, they recorded someone trying to offer a bribe and that gentleman was nailed on the basis of that evidence.

V: We look at the Pius Ncube case, installing cameras in the bedroom.

J: Well according to my imagination we were going to see videos of Tsvangirai on ZTV and they threaten that they will do that unless he does this.

A: Unless he becomes Vice President

J: Which is do you prefer being a Vice President or having a sex tape on TV.

A: Oh my gosh but I think people spoke about it saying how can Tsvangirai move into a house built by ZANU-PF and he was also naive that the driver was a top ZANU-PF supporter which actually brings a broader issue of how naïve they were, they didn't have their own central intelligence organisation.

J: Do the courts here have provisions for total secrecy or you are not even allowed to communicate that you are involved in a court case.

BC: Yes the court has to make the rule. I'm not sure if money laundering precedes crime or it is being corrected with so many mistakes in it. Money laundering requires banks to do it on their customers and inform authorities about their suspicions to prevent crime and terrorism.

A: So is it lawful in Zimbabwe now?

BC: Yes it is but the bill is passed with so many mistakes like it has wrong references and so on and its being corrected.

V: But it true that when everyone was going through hyperinflation we were all terrified that of you wrote anything about money or dollar they would intercept so I think they used to do it then. We practiced a lot of self-censorship and we were quite anxious about getting the US dollar and everybody was scared of talking on the Internet about it.

J: I remember ironically a case where a woman on NANGO was writing to a friend of hers about getting a suitcase full of cash through customs at this particular time and she made a mistake of posting it on a public mailing list instead of a private one to one email.

A: But what you are saying brings an interesting dimension to the discussion that interception is not only done under the ICA but the other pieces of legislation that could equally breech the right to privacy.

BC: B has just mentioning that the Telecommunications Act has provisions. We need to just check whether they are still there.

J: Do they require the magistrate to give an order?

BC: Sometimes it's the attorney general who gives authorisation and customs system applies to privacy.

J: They can take laptops flash drives etc

V: Every time they raid human rights defenders they take their laptops.

J: They have taken the MDC computers on a number of occasions.

A: I think there was paper written by Brian Kagoro in order for MDC to win they need a million voters in the urban areas.

J: Another piece of legislation is one that refers to insult to the President that violates freedom of speech.

V: If you are overheard on a public taxi or in a bar insulting the President someone can actually report you.

BC: Look that applies to any crime. If we were planning a robbery we could be reported if someone heard us, we could be victims.

J: It is absurd that on an occasion such as an election campaign where one insults the other and the other would be insulted if they said the same thing to the other person. So I was advising people that don't get paranoid and shut down your email all together but then I tell NGOs when you connect to Gmail just make sure you are using https and not standard http because the latter can easily be intercepted. Well I talked to one organisation and they said we are really safe now because we are using Gmail and I was saying that is a complete joke because what you have done is actually that you have given them access to all your information.

Access to information

V: The other thing is it adds into what J said because access to real information is very difficult in this country, it is very difficult to access information; it should be in the public domain and this instills cultural fear and paranoia

A: Its not just the Government, it is pervasive in society even CSOs. The issue of the voters roll is symptomatic of a greater problem, a society that is not transparent.

J: That's a clear breach of the provisions of the Electoral Act isn't it? Isn't it now a requirement that they release the voter's roll?

BB: Yes, there has always been a right to it being inspected but I think the big complaint this time around was provision of copies particularly the electronic copy which still hasn't been brought to the public.

V: It clearly says in the Act that they should provide it.

J: And they haven't provided any explanation whatsoever as to why they haven't provided it.

A: I was speaking to V thinking that if Justice Bhunu had dealt with these substantive issues then we may be in a position to know why but unfortunately the judgment was too short only rebuking the lawyers.

Interception by non-state actors

J: Can I change the subject to another issue of interception that is non- state actors? On the Internet we are concerned about hacking into servers by criminals trying to get hold of peoples' passwords, bank account details so there is some measure of criminalization.

A: Is it happening in Zimbabwe now, I think there are a lot of Nigerians?

BC: No the Nigerians are not involved in interception.

J: I am actually talking about interception by virtue of malware and hacking attempts to servers and things like that.

The Government's technical and legal capabilities

A: And during the elections I am not sure whether you where aware that there were cyber attacks, we suffered what is called denial of service attack and Nehanda radio and SW Radio and election right because they wanted to target all those things that are likely to announce the elections before the ZEC did, because I was operating a situation room, there in London I was crowd sourcing information and then we were attacked and for six days we were not operational.

J: V your server has been attacked as well by China, I saw three thousand six hundred attacks. I brought the IP address concern.

A: I think the Government are outsourcing because those attacks I don't think they were coming from Zimbabwe, I think they were coming from China. But although there was evidence and reports that government websites were also attacked by Herald it was more attacks than counter attacks.

BB: They could come from China if the Chinese were running the interception center.

J: Oh you never know where that attacks originate all you can see is the last part, and by the way China made attacks on V server I think when I was watching the other night there were three and a half thousand attempts to log in and I blocked the IP address.

V: Well the number of mails I get from China is incredible, where do they get the address?

J: Well the website.

A: What they did also before the elections, I got about 50 subscribers to our mailing list from China and when you don't look at who has subscribed and when you finally do, all I saw were Chinese names. For what reason I am not sure but we were talking about cyber attacks during the elections, SW Radio, Nehanda Radio, our website, election ride suffered denial of service attacks.

V: There is vey little law governing digital information. We pointed it out to Timba.

J: Even when they last modified the Post and Telecommunications Act, the references to the Internet were just childish. They got definitions all wrong and it required Internet services providers to register with POTRAZ but then they brought out regulations that used completely different language from the Act and they don't really know what they are doing.

The African charter and the new Constitution

A: But its also when you are looking at the African Charter on Human and Peoples Rights it lacks provisions on privacy, and digital media so we are going to be having a discussion at the NGO Forum during the 54th session on the right to privacy and digital issues so that language is also mainstreamed in policy decisions at African level. But another question that I wanted to ask is do you know who sponsored the provision on privacy in our New Constitution that is section 57 talks about privacy or they simply duplicated it from South Africa.

BB: South Africa and Kenya, yes. The content comes from the first draft of South Africa and Kenya and it was modified though they did not add anything to the provisions.

A: So there is no parliamentarian at the moment, I know they are keen on Expression, POSA and AIPPA but not on privacy, do you think there is anyone who might be looking at that and the advocacy as well?

BC: Well I'm sure there are, but I don't know them.

J: Where there any key provisions to protect an Act.

BC: In terms of privacy, No.

A: There doesn't seem to be many drafters in Zimbabwe

BC: We are doing a training exercise on the drafters. It's just that the Government does not pay enough money so people do not stay.

J: Another angle might be to look at it from the ZANU-PF side; I was interested when I went to Parliament I had written the presentation though it was meant to be presented by the chair of ZISPA but they weren't there so I made the presentation but instead of getting hostile reception as you would expect the chairman of the committee at that time was Leo Mugabe and he in fact was very interested in what I had to say and when then I started to talk about the impact on the economy for example not having protection from interception of private business.

J: When I look at the nations' Internet infrastructure and how incompetent the management is I just speculate their failure, they don't do the simplest things.

Engaging with IAPs and ISPs

What would be good is to see if you can get to meet key people in the local IAPs and ISPs. ISPs are the service providers and IAPS are the ones that operate the gateways like telone, Econet and Telco.

V: The Trans media are not doing anything at the moment because the Chinese are busy installing Interception of Communications.

J: Certainly they have to have an interface

V: Econet was forbidden sending of mass sms during the elections so I think it's also worth talking to them.

Off record conversation ad tips on advocacy

As the ICA makes it a crime to talk about what has been done on the law we could not discuss specific cases.

7.2.4. Informant 7

Interview with Portraz lawyer

Question: Does the Government intercept or listen on private communication?

Answer: The Government does not intercept private conversations without lawful grounds for doing so. If that happens as an example then that would be an offence which one can report to the police and whosoever is doing that will be prosecuted.

Question: How come the Government requires people to get permission to videoconference outside the borders and why did the Government issue a directive to Econet Wireless and other IAPs and ISPs preventing them from processing bulky or mass texts during the elections, purportedly out of security concern?

Answer: The issue of mass texting has implications on national security and also the borderline between telecommunication and broadcasting is so thin, for you to broadcast a thousand messages at a given time, it requires a broadcasting license because you are as good as any broadcaster now. Those are some of the reasons why mass texting of messages is being prohibited because they are sort of broadcasting illegally because their license their license does not allow them to broadcast legally.

On law reform

Question: Is there a need for a law reform, for example to re-align the current interception of communications laws with the Constitution?

Answer: We can not do such research for you but if you feel that this needed to be done that would be most welcome to them and, “if there is any help or support we can give in that regard we will be more than willing because law reform is also one of our many objectives. As a regulator, we want to make sure that our laws are constantly reviewed and updated in line with practice and also that they are constitutional, so if you can find out areas you think require reform that will be very welcome”.

7.2.5. Informant 3’s pre-filled questionnaire

Communications & Political Intelligence surveillance on Zimbabwean, Human Rights Defenders: Zimbabwean officials and experts’ questionnaire
About the form: This generic form may be used for a wide range of experts ranging from internet service providers, and experts from the fields such as legal, technological, political and security and government officials. Additional sheets may be used if the spaces provided are not adequate. Your information will be kept in accordance with our data protection policy and

should you wish to fill this form anonymously, please indicate on the release form below.

1. What is your name?
HJ
2. Which organisation do you work for?
--
3. What is your role in the organisation?
I am the system administrator for each of the above and former Board member of both.
4. Please describe your direct or indirect experience of dealing with issues relating to political and communication surveillance in Zimbabwe?
I prepared a paper objecting to the Interception of Communications Bill, which I present to the Parliamentary Portfolio Committee on Transport, and Communications on behalf of ZISPA in 2006.
5. Which countries mostly provide the expertise and equipment used in surveillance in Zimbabwe?
China is the country most well-known for the above, but I also suspect Iran.
6. Please describe the ways surveillance impacts on civil liberties, in particular the right to privacy for human rights defenders and other people opposed to government policies or those who are perceived as such in Zimbabwe, or any other country you are familiar with?
The fear of interception of communications is probably the most serious issue, given technical limitations in the Government's ability to manage the interception program. The result is that they fear to use email and cell phones, thereby reducing their ability to work effectively. However given the wide range of options the State has to harass perceived opponents I don't believe that the current regulatory environment for interception of communications has been of major significance in terms of punitive use. I believe its main role has been to monitor and to intimidate.
7. What national laws, regulations, practices and safeguards are there in Zimbabwe relating to political intelligence oversight and communications surveillance? In your own view, are these safeguards adequate?
The key Act in terms of surveillance is the Interception of Communications Act of 2006. However in terms of practical effect in relation to freedom of speech I would consider the Access to Information and Protection of Privacy Act of much greater significance as it has been used directly on many occasions to arrest and charge journalists and editors.
8. Are there comparable regulatory standards and best practices in your region or any other country you are aware of?
Most countries seem to have draconian interception laws now. Zimbabwe legislation follows the Regulation of Investigatory Powers Act 2000 in the UK. America is worse.
9. How can Zimbabwe's current surveillance practice be brought in line with international standards and norms and comparative best practice?
Sadly there are no such international standards and norms.
10. How did the provision on privacy get included in the new constitution?
Not known.

11. Are there any individuals/organisations that you would recommend we speak to?
You could start with the Chairman of ZISPA
12. Do you have additional observations not covered above?
I was involved as a witness for the defense in the case of journalist Andy Meldrum when he was charged with publishing falsehoods on the Internet. The Government case initially relied on material that they had downloaded from the Guardian website, a printed copy of which was presented in court. I showed that a printout was meaningless as evidence as it could easily be tampered with. As an example I provided the court with a printout of an article by Andy Meldrum but it indicated Thabani Mpofu had written it instead – who happened to be the prosecutor in the case! They dropped that line of argument very quickly. However the police witness was also totally incompetent. When he wanted to demonstrate the downloading of the original article he turned to Google instead of typing in the URL that was clearly indicated at the bottom of his printout. It would be worth going through the records to see if intercepted communications had in fact been used in any cases before the courts. I can't think of any off hand, but know some people have been charged when emails they circulated as chain letters ended up in unsympathetic hands.

I hereby grant permission to the information above to be used in the ensuing report "Surveillance and Freedom: Global Understandings and Rights Development (SAFEGUARD)" to be published in 2014.
Date: 28 August 2013
Name: HJ
Signature:
I would like to remain anonymous: Yes

15 Years: Zimbabwe Human Rights NGO Forum
Working to protect all human rights

Human Rights Forum
Blue Bridge, 8th Floor, Eastgate
P O Box 9077 Harare, Zimbabwe

Tel (+263) 04-250 511

International Liaison Office

54 Commercial Street London E1 6LT, UK

Intlo@hrforumzim.com
www.hrforum.org

The Forum thanks the International Development & Research Centre for its support.