AN ANALYSIS OF THE COMMUNICATIONS SURVEILLANCE LEGISLATIVE FRAMEWORK IN SOUTH AFRICA

Report compiled by Admire Mare
Contribution by Jane Duncan

Media Policy and Democracy Project

November 2015

Contents

EXECUTIVE SUMMARY 1

1. Introduction and Background to the Report 3

1.1 The Snowden Revelations and Mass Communication Surveillance 5

2. The Necessary and Proportionate Principles 8

3. The South African Political Context 10

3.1 Political Background 10
3.2 The South Africal Legislative Context 14

4. Summary of Main Findings

How do the South African communications surveillance laws measure up to the Necessary and Proportionate Principles? 18

5. Recommendations for Reform to Ensure Compliance with International Human Rights Law and Standards 31

6. Conclusions 38

Bibliography 39

Figures

FIGURE 1: SUMMARY OF THE NECESSARY AND PROPORTIONATE PRINCIPLES 9

FIGURE 2: UN GOOD PRACTICES ON OVERSIGHT INSTITUTIONS 33

FIGURE 3: STANDARDS FOR OVERSIGHT AND TRANSPARENCY OF NATIONAL INTELLIGENCE SERVICES 35

EXECUTIVE SUMMARY

The Snowden revelations have opened up a Pandora's Box with regard to the impact of technology on mass surveillance, as well as the lack of protection for user data associated with internet intermediaries. The revelations, which uncovered extensive and indiscriminate surveillance efforts worldwide, highlight that violations of fundamental rights are not merely a theoretical concern. Revelations by Edward Snowden about the working methods of national intelligence services have raised substantial legal and policy questions. In some jurisdictions, the revelations have generated momentum for reform of communications and intelligence service legislation, so that new laws are aligned with the International Principles on the Application of Human Rights to Communications Surveillance (also known as the Necessary and Proportionate Principles). In other contexts, despite calls for reform, it is important to highlight that many laws passed recently (including in Europe and Australia) codify practices of unlawful surveillance and hence violate the International Principles. Old laws, mostly formulated along technologically-neutral lines, have been lambasted for failing to catch up with the ever-changing nature of technological developments. Concerns have also been prompted over the levels of powers granted to state security agencies, as well as weak oversight bodies. Oversight[1] bodies governing communications in the era of convergence have also been reconstituted and strengthened in other political contexts. Extra-legal state surveillance has also been condemned for violating international human rights law protecting the right to privacy against unlawful surveillance. In Africa, the debate around mandatory Subscriber Identity Module (SIM) card registration has also been re-ignited in the wake of the Snowden revelations. Marriages of [in] convenience between internet intermediaries and the state have also come under the spotlight. UN human rights mechanisms have begun assessing the human rights implications of the internet and new technologies on communications surveillance and access to communications data. The United Nations Special Rapporteur, Frank La Rue, issued a report on state communications surveillance[2]. The report noted that, despite the 'clear existence of rights in international human rights law, these laws and procedures are not sufficiently nuanced to provide clear guidance to individuals and governments when applying them in individual cases' (La Rue, 2013). The Office of the High Commissioner for Human Rights (OHCHR) report also indicates that 'many states evinced a lack of adequate legislation and or enforcement, weak procedural safeguards and ineffective safeguards'. Significantly, in March 2015, the UN Human Rights Council established an independent expert –the

[1] Oversight refers to the various ways of holding the intelligence services accountable before the public and the government: internal oversight by the responsible minister, parliamentary oversight, judicial oversight and external independent oversight. It can encapsulate specific instances in which measures are implemented against a particular target on bulk interception of electronic communications or on the overall functioning of a system of secret surveillance and data collection. It is aimed at 1) avoiding abuse of power, 2) legitimising the exercise of intrusive powers and 3) achieving better outcomes after an evaluation of specific actions. Oversight can be applied at three moments: when the surveillance is first ordered and authorised, while it is being carried out and after it has been terminated (University of Amsterdam, 2015).

[2] Communications surveillance encompasses a broad range of activity that implicates the privacy and expressive value inherent in communications networks. It includes not only the actual reading of private communications by a another human being, but also the full range of monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, or arises from a person's communications in the past, present, or future.

UN Special Rapporteur on the Right to Privacy – with a mandate to address the rising concerns about the enjoyment of the right to privacy, particularly in the context of new communication technologies.

To respond to the need to articulate what international human rights law requires of governments to respect and protect human rights when conducting communication surveillance, a group of non-governmental organisations and experts developed the International Principles on the Application of Human Rights to Communications Surveillance [https://necessaryandproportionate.org]. This report will outline the key tenets of these principles in the subsequent sections.

In view of these global concerns, this report, commissioned by the Media Policy and Democracy Project[3] (MPDP), looks at how the South African legislation on communication surveillance measures up to applicable human rights law, as illustrated in the Necessary and Proportionate Principles. This report focuses specifically on South African laws which govern mass communication surveillance. These include: the Electronic Communications and Transactions Act (Act 25 of 2002); Regulation of Interception of Communications and Provision of Communications Related Information Act (Act 70 of 2002) (RICA); General Intelligence Amendment Act of 2013; Financial Intelligence Central Act of 2001 (FICA); Intelligence Services Oversight Act; Protection of Personal Information (POPI); State Security Agency Bill and Cyber-Security and Cyber-Crimes Bill. The main goal of this report is to contribute to the debate on the urgent need to review existing laws governing communication surveillance, ensuring that transparency[4] and accountability mechanisms are built into these laws and sufficient safeguards are put in place to curb abuse by service providers and the State. The recommendations are meant to bring South African laws governing mass surveillance practices in line with the Necessary and Proportionate Principles. Notwithstanding problematic areas associated with the Principles, it is important to highlight that the United Nations General Assembly resolution on the right to privacy in the digital age (2013; 2014) calls upon member States:

(a) to respect and protect the right to privacy, including in the context of digital communication;

(b) to take measures to put an end to violations of those rights and to create conditions to prevent such violations, including ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass

[3] The Media Policy and Democracy Project (MPDP) is a joint initiative of the Department of Communication Science at the University of South Africa and the Department of Journalism at the University of Johannesburg (UJ). The project was established in 2012 to promote participatory, public interest policy-making on media and communications issues. The MPDP works closely with civil society organisations, such as SoS – Support Public Broadcasting Campaign and the Right2Know Campaign, undertaking research on areas of concern that they campaign on: However, MPDP retains its organisational independence.

[4] Transparency, namely openness, relates to public reports issued by telecommunication providers and companies that provide basic communication services. Such reports are a tool to give the public some insight into the scope of secret surveillance and data collection and allow for a further assessment of the lawfulness and effectiveness of measures. Transparency is important at multiple levels and in different relations; for instance at the level of the judiciary or in the relation between intelligence services and parliamentary oversight committees or forms of independent oversight. These institutions can contribute to transparency by reports, hearings and investigations.

surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency – as appropriate – and accountability for State surveillance of communications, their interception and the collection of personal data.

This report begins by relooking at the Snowden revelations about mass surveillance by the Five Eyes[5] (United States of America, United Kingdom, Canada, New Zealand and Australia) and then proceeds to outline the Necessary and Proportionate Principles. We then move on to look at the South African legislation on communication surveillance and case studies of state surveillance and discuss how the South African legislation measures up the Necessary & Proportionate Principles. Finally, we discuss recommendations for reform to ensure compliance with international human rights law and standards. Next, the report looks at the Edward Snowden revelations with special attention on state and corporate mass surveillance practices.

1. Introduction and Background to the Report

Surveillance has always been part of human social relations since time immemorial. Although physical[6] forms of surveillance have received substantial attention by scholars, electronic forms of surveillance have become popular in recent years. Scholars (Bentham, 1791; Foucault, 1977); Lyon, 2003; Deleuze, 1992; Haggerty & Ericson, 2000) have been at the forefront of theorising the emergence of ubiquitous surveillance in its various forms and shapes. Others (Lyon, 2015; Haggerty & Ericson, 2000; Ni Loideain, 2015; Bakir, 2015) believe that the dynamic nature of technology has not only changed 'how' surveillance can be carried out, but also 'what' can be monitored. Major advancements in digitisation and internet access have led to the convergence of communications (calls, e-mails, web searches, online shopping) to one device that is both mobile and internet-enabled (Wicker, 2013). The convergence of 'old' and 'new' communications technologies has been accompanied by surveillance of different kind of information, such as the content of communications, meta-data and user behaviour (Lyon, 2015). For instance, the constant trail of meta-data left behind from the always-on 'smart' communications devices has facilitated the collection of unprecedented amounts of data and presents unique privacy challenges (Fuchs, 2014; Human Rights Watch, 2014).

[5] The 'Five Eyes'", often abbreviated as 'FVEY', refer to an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are bound by the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.

[6] Physical surveillance is a form of monitoring where the subject is kept under physical observation. It can be combined with other modes of surveillance for complete coverage and may be used by law enforcement officers, as well as private investigators. This type of surveillance requires special skills and is labour intensive, as personnel must be continually rotated to provide coverage and it may be necessary to use an array of observers to avoid attracting attention from the subject under observation.

This information, known as communications data or meta-data[7], includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive. Meta-data are storable, accessible and searchable and their disclosure to and use by State authorities is largely unregulated (Ni Loideain, 2015).

As scholars (Bakir, 2015; Ni Loideain, 2015) observe, meta-data is a rich source of personal information as it reveals the 'who' (parties involved), the 'when', how long and how often, (time, duration and frequency), the what' (type of communication, for example, phone call, message or e-mail), the 'how' (the communication device used, for example, landline telephony, smartphone, tablet) and the 'where' (location of devices used) involved in every communication we make. Over and above the actual content of communications, the collection, aggregation and analysis of meta-data can provide very detailed information regarding an individual's beliefs, preferences and behaviour (Ni Loideain, 2015). The potential value of meta-data in mass communications surveillance was confirmed by General Michael Hayden, former director of the US National Security Agency (NSA) and the Central Intelligence Agency (CIA), when he observed that 'We kill people based on meta-data' (Hayden, 2014).

Given the revelatory potential associated with meta-data analysis and aggregation, States are increasingly drawing on this kind of information to support law enforcement or national security investigations. States are also compelling internet intermediaries and telecommunications service providers to preserve and retain communication data to enable them to conduct historical surveillance (Ni Loideain, 2015). Notwithstanding the massive developments in new media technologies, existing legislation and practices in most countries have not been reviewed and updated to address the threats and challenges of communications surveillance in the digital age (La Rue, 2013). The situation has been worsened by safeguards (including privacy/personal data protection) which are lower for meta-data than they are for content of communications and sharing arrangements and this has resulted in ad hoc practices that are beyond the supervision of any independent authority (UN General Assembly, 2013). Whilst in some countries access to communications data can be conducted by a wide range of public bodies for a wide range of purposes, often without judicial authorisation and independent oversight, most developed states have implemented surveillance arrangements that purport to have extra-territorial effects.

[7] The term 'meta-data' relates to information generated or processed as a consequence of a communication's transmission. Much can be revealed from this data, including 'latitude, longitude and altitude of the sender's or recipient's terminal, direction of travel…any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection' (Young, 2004). Meta-data therefore concerns the context as opposed to the content of a communication and covers many types of information, such as traffic data, location data, user data and the subscriber data of the device/service being used (for example, mobile phone network or Internet service provider).

1.1 The Snowden Revelations and Mass Communication Surveillance

In June 2013, the former National Security Agency (NSA) contractor, Edward Snowden, disclosed the nature of several programmes involving the mass surveillance of communications belonging to individuals both within and outside of the United States of America to a select group of journalists in the UK and US news media; mainly *The Guardian* and *Washington Post* (Greenwald, 2014). The Snowden disclosures revealed an array of activities in dozens of intelligence programmes that collected data from large American technology companies, as well as the bulk collection of phone meta-data from telecommunications companies that officials say are important to protecting national security (Lyon, 2014; 2015). The Snowden leaks indicated the extent, nature and means of contemporary mass digital surveillance of citizens by their intelligence agencies and the role of public oversight mechanisms in holding intelligence agencies to account (Bakir, 2015). For instance, it showed that the NSA was conducting mass surveillance of political leaders such as German Chancellor, Angela Merkel. The leaks also indicated the collection of web traffic around the globe, and efforts to break the security of mobile phones and web infrastructure. Some of the countries which have also been exposed as conducting mass surveillance include the United Kingdom, Australia, Canada and New Zealand.

As Bakir (2015) points out, the Snowden disclosures have also drawn attention to the significant role played by the private sector in the mass surveillance of communications for governments. This refers to a practice where 'hybrid surveillance agencies' (government-corporate interactions) (Lyon, 2015) collaborate or share information about users' online behaviours. On the one hand, Ni Loideain (2015) has questioned whether it is lawful for governments to have 'back doors[8]' to the encrypted communications of the customers belonging to private companies. On the other hand, the OHCHR (2014) has raised concerns regarding the extent to which private actors should be co-opted into the blanket monitoring of individuals' communications for governments. It also came to light through these revelations that some of the States are imposing the intermediary liability clause in their national legislation, thereby forcing internet intermediaries to act as 'extensions' of intelligence services. It revealed that internet intermediaries such as Facebook, Verizon, Microsoft, Yahoo! Google, YouTube, AOL, Skype, Apple and others participated in PRISM (Planning Tool for Resource Integration, Synchronisation and Management), a government programme that allowed the NSA and the FBI broad access to the companies' servers (Lyon, 2014). Through court orders issued under the Foreign Intelligence Surveillance Act 1978 (FISA), internet intermediaries were required to provide meta-data of millions of users (both US and non-US citizens) to the NSA. Although most of the internet intermediaries have denied ever participating in the PRISM programme, they have acknowledged that their servers had the capacity to store and archive massive amounts of meta-data. According to Snowden, the monitoring involved the mass retention and access to meta-data from

[8] A back door in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorised remote access to a computer, or obtaining access to plaintext while attempting to remain undetected. The back door may take the form of a hidden part of a programme; a separate programme may subvert the system through a root-kit.

the use of mobile phones for national security and law enforcement purposes (Human Rights Watch, 2014).

The leaks revealed that communication content and communications data/meta-data are collected in bulk from two sources; firstly, the servers of US companies (via PRISM) (Bakir, 2015). Due to the internet's architecture, the USA is a primary hub for worldwide telecommunications, making these servers data-rich. The second source of bulk data collection is directly tapping fibre-optic cables carrying internet traffic. The NSA does this through the UPSTREAM programme. The UK does this through TEMPORA, run since 2011 by the UK's signal intelligence agency, Government Communications Headquarters (GCHQ), in participation with BT, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel and Interoute.

The revelations by Snowden have also stirred up an on-going global debate on the implications posed by the large-scale secret monitoring for individuals' rights to privacy and the security of their personal data. These leaks also show that the United States routinely collects the content of international chats, emails and voice calls. It has engaged in the large-scale collection of massive amounts of cell phone location data (Human Rights Watch, 2014: 1). As intimated earlier, all these revelations have prompted major debates around the topics of privacy, national security and mass communications surveillance.

The Snowden revelations also highlighted the extent of cooperation and intelligence-sharing between the NSA, GCHQ and other Five Eyes partners, in which material gathered under one country's surveillance regime was readily shared with the others. It demonstrated that the foreign intelligence agencies of the Five Eyes had constructed a web of inter-operability at the technical and operational levels that span the global communications network. Besides this cooperation between the Five Eyes partners, secretive intelligence-sharing arrangements exist between non-Five Eyes countries. These intelligence sharing practices have been used to circumvent national legislations limiting the capacity of security services to collect and examine personal communication and personal data (Bakir, 2015). There is cooperation between law enforcement agencies through more formalised arrangements such as the Mutual Legal Assistance Treaties (MLATs). These intelligence-sharing agreements between governments raise questions as to how and when States may be liable under national and international law for their surveillance activities, which may have an impact far beyond their own borders.

Another issue which has arisen as a result of the leaks relates to the extent to which States can be 'extra-territorially' accountable for their human rights violations overseas. This kind of extra-territorial surveillance (monitoring of international traffic) has been made possible by the proliferation of new media technologies (Ni Loideain, 2015). This further complicates the overreliance on a narrow territorial protection of human rights when communication has become transnational and borderless. The nature of new media technologies, which rely on borderless routing and storage for their efficiency and robustness, permits states to intercept vast amounts of foreign information from the comfort of their territorial homes (Human Rights Watch, 2014). Whereas foreign intelligence agencies are often provided with significant latitude to spy on the communications of foreigners, the

highly integrated nature of communications networks has led many of these agencies to sweep up all data indiscriminately, citing difficulties between distinguishing foreign and domestic communications as a justification (University of Amsterdam, 2015). It should be noted that since 2013, a number of countries have introduced new laws in this field.

The Snowden revelations have also been accompanied by important landmark court rulings related to data protection and 'Safe Harbour[9]' arrangement between continental bodies, countries and internet intermediaries, mostly based in the USA. On 6 of October 2015, the European Court of Justice ruled that the transfer of personal data from Europe to the USA is invalid due to the latter's lack of data protection against mass surveillance (Nyst, 2015; Hintz, 2015). The judgement also questioned the compliance of US law on privacy and surveillance with European human rights standards. The case was brought forward by Austrian law student Maximilian Schrems, who challenged Facebook's practice of transferring personal data from its European subsidiaries to the USA (Hintz, 2015). The Safe Harbour agreement regulates the lawful transfer of personal data by companies between the EU, the USA and other countries.

In the USA, Congress passed the Communication Assistance for Law Enforcement Act (CALEA) in 1994 to respond to law enforcement concerns that their ability to monitor networks was declining (or 'going dark') as more networks were digitised. The US telephone industry developed a handover interface standard for these purposes (the CALEA standard), which allows communications to be routed to government interception centres. As part of the CALEA Act, internet intermediaries are required to use digital switches that have surveillance capabilities built into them – just like RICA in South Africa. Similar to the European Telecommunications Standards Institute (ETSI) standard, CALEA has been exported to many countries as the surveillance standard. Like many other countries, South Africa adopted CALEA and ETSI standards in 2005, allowing users' data to be routed to interception centres.

In the wake of the Snowden leaks, human rights advocates have argued that handover interfaces[10] between national interception centres and internet intermediaries can easily be exploited by intelligence agencies and criminals. For instance, in 2004 and 2005, senior government officials in Greece had their communications intercepted through exploiting the in-built weaknesses of handover interfaces. Similarly, over 6000 Italians, including judges, politicians and celebrities, also had their communications intercepted by criminals over a period of a decade. Cognisant of these inherent vulnerabilities, the EU court ruled that internet companies may continue transferring data but their practice of using safe harbour interfaces may now be reviewed by a variety of national data protection agencies (Hintz, 2015).

Amongst other issues brought to the fore by the Snowden revelations is that human rights (right to

[9] Safe harbour, an agreement made between the EU and the US in 2000, was supposed to protect private data collected by internet companies.

[10] Handover interface is connected between the telecommunications service provider and the equipment of the State interception office. It comprises hardware and software and is usually situated in the service provider's mobile switching centre; the device enables the service provider to send, or 'hand over'.

privacy, freedom of expression, freedom of assembly and so forth) can be systematically eroded if technologically-driven challenges are not addressed (Access, 2013). On the policy front, it has led to the drafting of a new set of international principles to protect human rights in an era of mass surveillance. The next section focuses on the Necessary and Proportionate Principles.

2. The Necessary and Proportionate Principles

The process of elaborating the Principles began in October 2012 at a meeting of more than 40 privacy and security experts in Brussels. After an initial broad consultation, which included a second meeting in Rio de Janeiro in December 2012, Access, EFF and Privacy International led a collaborative drafting process that drew on the expertise of human rights and digital rights experts across the world. The first version of the Principles was finalised on 10 July 2013 and was officially launched at the UN Human Rights Council in Geneva in September 2013. This was followed by a number of specific, primarily superficial textual changes in the language of the Principles in order to ensure their consistent interpretation and application across jurisdictions. The final and current version of the Principles was published in May 2014. The Principles outline how international human rights law applies in the context of communication surveillance. They are founded on established international human rights law and jurisprudence. Cognisant of the fact that new media technologies have complicated the realisation of human rights norms across the globe, the Necessary and Proportionate Principles call on all national laws to adhere to human rights norms in communication surveillance (https://es.necessaryandproportionate.org). Acknowledging that new media technologies have facilitated increased state surveillance and intervention into individuals' private lives, the Principles call upon the States to update their understandings and regulation of surveillance and modify their practices to ensure that individuals' human rights are respected and protected. The Principles further argue that mass surveillance in all its manifestations is unnecessary, disproportionate and fundamentally lacking in transparency and oversight. According to its founding documents, the main purpose of the Principles was to provide civil society groups, states, the courts, legislative and regulatory bodies, industry and others with a framework to evaluate whether current or proposed surveillance laws and practices around the world are compatible with human rights. Human rights advocates have also urged member states to revise and adopt national surveillance laws and practices that comply with the Principles and to ensure cross-border privacy protections are sufficiently safeguarded (https://es.necessaryandproportionate.org). In view of this, this report seeks to assess whether the South African legislation on communication surveillance is compatible with the Necessary and Proportionate Principles (see Figure 1 overleaf for an overview of these principles).

FIGURE 1: SUMMARY OF THE NECESSARY AND PROPORTIONATE PRINCIPLES

The Principles provide a framework for assessing human rights obligations and duties when conducting communications surveillance.

LEGALITY

Any limitation on the right to privacy must be prescribed by law.

LEGITIMATE AIM

Laws should only permit communications surveillance by specified state authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.

NECESSITY

Laws permitting communications surveillance by the state must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim.

ADEQUACY

Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific Legitimate Aim identified and effective in doing so.

PROPORTIONALITY

Decisions about communications surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

COMPETENT JUDICIAL AUTHORITY

Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.

DUE PROCESS

States must respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced and available to the general public.

USER NOTIFICATION

Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation.

TRANSPARENCY

States should be transparent about the use and scope of communications surveillance laws, regulations, activities, powers, or authorities.

PUBLIC OVERSIGHT

States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS

States should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems or to collect or retain particular information purely for state communications surveillance purposes.

SAFEGUARDS FOR INTERNATIONAL COOPERATION

Mutual Legal Assistance Treaties (MLATs) entered into by States should ensure that, where the laws of more than one State could apply to communications surveillance, the available standard with the higher level of protection for individuals should apply.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS

States should enact legislation criminalising illegal communications surveillance by public and private actors.

Source: Access, 2013: 2

Having outlined the basic tenets of the Necessary and Proportionate Principles, it is also important to highlight some of the problems associated with these principles. For instance, the user notification principle raises serious terrorist crimes. Notifying the person concerned can therefore jeopardise chances of apprehending the culprits and averting a possible calamitous situation. This requirement by the Necessary and Proportionate principles somehow makes them an imperfect template for reform. Another critique relates to the requirement by the principles for telecommunications to desist from embedding communication surveillance capacities into their networks. Such a requirement makes it difficult for law enforcement agencies to monitor national security threats which are legitimate and necessary, especially in countries like France and the United States of America, which are vulnerable to terrorist attacks.

With the Necessary and Proportionate Principles in mind, some of the most pertinent questions that can be posed relating to the South African context include: How do South African laws governing mass and targeted communications surveillance measure up to the aforementioned principles? How do South African laws governing intelligence compare when assessed in light of the Necessary and Proportionate Principles? How does the South African Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA), which governs targeted interceptions, measure up to these principles? How does the State Security Agency Bill fare up when assessed in light of these principles? Which aspects of RICA violate the Necessary and Proportionate Principles? How can those aspects be reformed in order to meet the Necessary and Proportionate Principles? These are some of the questions which will be answered in section four of this report. Next I look at the South African political context.

3. The South African Political Context

3.1 Political Background

Although Snowden's revelations about mass communications surveillance provided some space for the debate globally, this section will outline some of the South African specific issues related to abuse of surveillance which have raised concerns amongst academics, journalists, politicians, trade unionists and civic activists. Whilst South Africa is not a terrorist target, Duncan (2014) argues that high incidences of social protests and xenophobic attacks against foreign nationals suggest that the temptation is there for less principled members of the security apparatus to abuse the state's surveillance capabilities to advantage the faction currently in control of the ruling African National Congress (ANC) and disadvantage their perceived detractors. High rates of service delivery-related protests have seen Alexander (2012) characterising South Africa as the 'capital of social protests in the world', although there is no comparative measure of protests around the world. Another key area which makes South Africa an interesting case for studying communication surveillance is its strong tradition of investigative journalism, trade unionism and social movements. As Duncan (2014) notes,

the state could easily misuse its surveillance capabilities to harass certain constituencies which are seen as endangering the hegemonic project of the ruling class.

There are reports (Swart, 2015; Right2Know Campaign, 2014; Duncan, 2014) of academics, investigative journalists, political opponents and trade unionists being subjected to various kinds of physical and electronic surveillance in recent years. The Intelligence Services Amendment Bill was meant to govern the operations of the National Communications Centre (NCC), but it was never passed into law. It was in fact held over to the debates on intelligence policy and the State Security Agency Bill. South African media reports (*Mail & Guardian*, 2014; *The Sunday Times*, 2014; Swart, 2015) also show that state surveillance has been carried out outside of the RICA legal framework in ways that violate the right to privacy as enshrined in the Constitution. For instance, in 2005, the state's mass surveillance capacity was misused to spy on perceived opponents of the then contender for the presidency, Jacob Zuma (Duncan, 2014). In a related incident, some of the leading figures in the Scorpions[11] had their phone calls listened to while they were finalising corruption charges against Jacob Zuma during his ascendency to the Presidency. This constituted mass surveillance practices in contravention of the RICA law which regulates targeted surveillance. Public officials in South Africa have also had their communications intercepted by the state. For instance, the former Chief of the South African Revenue Service, Oupa Magashula, was caught on tape making an improper offer of employment to a young woman (Duncan, 2014). The tapes were intercepted as part of a sting operation on the former South African Police Service (SAPS) chief, Bheki Cele (Duncan et al., 2014). It is important to bear in mind that although the media has been instrumental in raising red flags on mass surveillance practices, it tends to focus on exceptional cases involving the elite and public officials at the expense of the ordinary, everyday workings of the RICA process.

The Crime Intelligence Division of the SAPS have also taken advantage of the low threshold of surveillance to obtain judicial approval to intercept the mobile phones of two *Sunday Times* journalists – Stephan Hofstätter and Mzilikazi wa Afrika – in 2010 by giving fictional names and suggesting such interception was needed to investigate a criminal syndicate. Subsequently, the *Sunday Times* took the case to court and two officers were charged with violations of RICA. This incident has fuelled fears that other applications to tap the communications of journalists and public figures may have been granted under false pretences. Not only journalists have been targeted for state surveillance – trade unionists have also not been spared, with media reports indicating that state intelligence officers were spying on senior National Union of Metalworkers of South Africa[12] (NUMSA) officials and were attempting to recruit some of their members to work as spies. In the leaked intelligence document, titled *Exposed: Secret Regime Change Plot to Destabilise South Africa*, NUMSA general secretary Irvin Jim and deputy general secretary Karl Cloete were identified as leading the plot against the state. The document also named former intelligence minister Ronnie Kasrils, Professor Chris Malekane, Professor Patrick Bond, Professor Noor Nieftagodien, Professor Peter Jordi and Moeletsi Mbeki,

[11] The Directorate of Special Operations (also, DSO or Scorpions) was a multidisciplinary agency that investigated and prosecuted organised crime and corruption. It was a unit of The National Prosecuting Authority of South Africa.

[12] The union was recently expelled from COSATU for rejecting the tripartite alliance with the ANC. It is in the process of forming the United Front (a political platform) aimed at merging workplace and community struggles.

brother of former president Thabo Mbeki, as some of the plotters (*Mail & Guardian*, 2014). Following the leak, NUMSA indicated that they would approach the Inspector-General of Intelligence's Office to ascertain whether there has been any surveillance of their senior officials and allies.

According to the *Mail & Guardian* (2014), academics based at the University of Johannesburg who were at the forefront of research projects focusing on the Marikana massacre, have experienced a series of thefts which have raised the question of whether they were targeted by the State or non-state actors for their investigation of service delivery protests. These academics include Professor Peter Alexander, who is the South African Research Chair in Social Change and Dr Carin Runciman. Another academic, Patrick Bond, of the University of KwaZulu-Natal, had his office broken into and ransacked in 2014. This suggests that academic freedom and critical engagement in South Africa is under siege (*Mail & Guardian*, 2014).

In February 2015, *Al-Jazeera News* reported on the 'Spy Cables' leaked documents which revealed a secret agreement between Zimbabwe's Central intelligence Agency and South Africa's State Security Agency to exchange intelligence and information about 'rogue NGOs' and to 'identify and profile subversive media'. The South African government directly provided public funding to a surveillance technology company, VASTech in 2008 and 2010. According to the *Mail & Guardian*, the South African government continues to fund VASTech. In the mid-2000s, VASTech supplied mass surveillance technologies to the Libyan government of Colonel Gadhafi (*Mail & Guardian*[13], 2013). A leaked report also reveals that sometime in 2005, an Iranian delegation met with the South African government and companies such as VASTech in a bid to obtain surveillance technology (*Mail & Guardian*, 2013).

In a series of investigation newspaper articles on government spying and communications interception and the potential threats these activities pose to personal privacy commissioned by the Media Policy and Democracy Project, Heidi Swart (2015) highlights it is easier for law enforcement agencies in South Africa to obtain meta-data illegally from telecommunications operators. Rather than following the procedure which requires law enforcement officials to apply to a high court judge, a regional court magistrate or a magistrate for a court order, interviewed police officers indicated that they simply approached service providers and requested information related to specific cellphone numbers relevant to their cases. One of the police officers noted that the major reason for circumventing the RICA process is because it is a lengthy process which could hamper case investigation (Swart, 2015). These cases show that it is easy to get access to someone's meta-data without a warrant as outlined in RICA. It also demonstrates that even telecommunication service providers or the RICA judge can be bypassed by the OIC and police crime investigation division when it comes to interception of communications. Although the Inspector General of Intelligence has a mandate to, inter alia, investigate complaints on alleged maladministration, abuse of power, transgressions of the Constitution, laws or policies, corruption or fraud by intelligence services, it is not clear whether the current Inspector General has investigated complaints submitted by NUMSA leaders and other

[13] Mail & Guardian: Millions were handed to an SA company that supplied mass surveillance technology to Libya. Available at: http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spywar

constituencies with regard to the violations of the RICA process.

In a newspaper article titled: *Big Brother is listening on your phone*, Swart (2015) writes that two of her four sources offered detailed explanations about how the OIC in South Africa can intercept communications without the knowledge of telecommunication service providers or the RICA judge. This is despite telecommunication experts in the country arguing that handover interfaces cannot be easily accessed and hacked because inbuilt privacy and security mechanisms such as the use of ghost IP addresses and strict control of the hardware by authorised senior personnel who are vetted (Swart, 2015). Swart (2015) also reports that the SSA and SAPs crime intelligence unit have acquired surveillance equipment like the grabber[14] which enable them to track the whereabouts of a mobile phone and monitors the communications in real time. Reports indicate that there are also private citizens who are using grabbers illegally in South Africa. These are generally used by moneylenders to locate evasive debtors. The use of these surveillance gadgets, which are not regulated by RICA, suggests the violation of law on the part of the police and intelligence agencies. In November 2015, the parliament's Joint Standing Committee on Intelligence (JSCI) expressed concern in a media statement about the illegal use of grabbers, particularly about 'whether at all a member of the crime intelligence unit might have been moonlighting without permission to conduct matters of crime intelligence' with a grabber (Swart, 2015: 8). In the context of mandatory SIM card registration required by RICA, the use of grabbers further undermines citizens' rights to privacy and freedom of expression. As Duncan (2014) observes, it is not clear whether these handover interfaces have been misused in South Africa too, but the point is that potential exists, as it has been architected into the network.

Another issue relates to foreign surveillance of communication between the Legal Resources Centre in South Africa and its clients in the United Kingdom by the GCHQ. This raises fears about the number of organisations and individuals that are being intercepted by foreign intelligence agencies. As Bakir (2015) notes, it is imperative for countries to revise and adopt national surveillance laws and practices that comply with the Principles and to ensure cross-border privacy protections. Given the ubiquitous surveillance in modern societies, it is also essential for South Africa to take necessary steps to investigate and prevent foreign surveillance of its own citizens.

These foregoing illustrative cases of investigative journalists, politicians, trade unionists, lawyers and academics being surveilled by the State demonstrate the corruptible nature of South African interception capabilities. The fact that the Crime Intelligence Division is the biggest user by far of interception directions issued in terms of RICA suggests that abuses of the authorisation procedures and directions are likely to be widespread because, as Swart (2015) observes, security agencies indicated that it is easier to circumvent the RICA process and to obtain information directly from telecommunication service providers.

[14] The grabber, generally installed in the back of a van, consists of a laptop, one or more antennae and a compact base station the size of a shoebox or desktop computer tower, depending on the model. It forces a cellphone to connect to it instead of a real cellphone tower.

3.2 The South Africal Legislative Context

In South Africa, a number of laws have bearing on communications surveillance and cyber-security issues. These laws include: the Electronic Communications and Transactions Act (Act 25 of 2002), Regulation of Interception of Communications and Provision of Communications Related Information Act (Act 70 of 2002), General Intelligence Amendment Act of 2013, Financial Intelligence Central Act of 2001, Films and Publications Act, Intelligence Services Oversight Act, Protection of Personal Information (POPI), State Security Agency Bill and the Cyber-Security and Cyber-Crimes Bill. For the purposes of this report, it is important to look at RICA, Intelligence Services Oversight Act, Cyber-security and cyber-crimes Bill, Protection of Personal Information, Electronic Communications and Transactions Act and the General Intelligence Laws Amendment Act which directly affects communication surveillance in South Africa.

(a) The South African Constitution

South Africa is regarded as having one of the most progressive constitutions in the world which, among other things, provides for the protection of several fundamental human rights. Unlike during the apartheid era, the 1996 Constitution addresses and protects citizens' rights to privacy and personal liberty. Section 14 of the South African Constitution defines 'privacy' 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. Chapter 2 of the Constitution contains the Bill of Rights, a human rights charter that protects the civil, political and socio-economic rights of all people in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom. The Bill of Rights also guarantees 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 as well as the rights to peacefully assemble, demonstrate, picket and present petitions.

Chapter 11 of the South African Constitution, which deals with the mandate of the security services (including the army, police and intelligence services) calls upon them to '…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' (Chapter 11, 199: 5) and that in order to ensure transparency and accountability, 'multi-party parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament' (Chapter 11, 199: 8). Any interference with the right to privacy can only be justified if it is in accordance with the law, has a legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance[15] activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human rights.

[15] This report uses the terms surveillance, interception and bulk data collection interchangeably because it believes these mean one and the same thing. It is matter of semantics to talk about targeted interceptions without falling into the trap of privacy intrusion and violating that qualified right.

Besides outlining an expansive Bill of Rights, the South African Constitution circumscribes the circumstances under which personal privacy may be interfered with. Thus, 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'.

(b) The Electronic and Communications Act (ECTA)

The cryptography services clause in the Electronic and Communications Act (ECTA) creates a regulatory framework for cryptography products and services used in South Africa. It also provides for the establishment and maintenance of a Cryptography Provider Register by the Department of Communications. As a complement to RICA, this clause seeks to assist law enforcement in their investigations in terms of cyber-related crimes. In 2013, the South African government passed the General Intelligence Laws Amendment Act which specifically excludes surveillance of lawful political activity, advocacy, protest and dissent from the mandate of the intelligence agencies.

(c) RICA: Regulating surveillance in South Africa

In South Africa, the law that deals with the surveillance of domestic communications on both criminal justice and national security matters is the RICA, which was promulgated in 2002. According to the law, the interception of domestic communications can only be done after judicial authorisation. This means that any interception of communications without the permission of a designated judge is considered unlawful. RICA also sets out the conditions for the granting of interception directions. According to the Chapter 2, section 5 (2b) of RICA, interception directions should only be granted if there are reasonable grounds to believe that a criminal offence has been, is being or probably will be committed. The Act also requires all South Africans to register their SIM cards with their mobile phone providers, so that the state can track the activities of suspected criminals or victims if necessary (Chapter 7, section 39: 1a). Chapter 5 section 30(1) of RICA makes it illegal to establish communications networks that are not capable of surveillance. It places obligations on communications service providers, including ISPs, to assist the state in the interception of communications (Chapter 5 section 30(1). In spite of the fact that RICA attempted to strike the correct balance between the interests of justice and national security on the one hand and civil liberties on the other, the Act has insufficient guarantees for civil liberties in general (I will look at these inadequacies in the next section). For instance, RICA explicitly outlines the circumstances under which the right to privacy of communications can be violated (I will revisit this issue at length below). In November 2015, the South African parliament's JSCI indicated that it would 'revisit' legislation pertaining to targeted surveillance (namely, RICA) (Swart, 2015). There is a need for civil society organisations to take advantage of this appetite for reform to push for a comprehensive overhaul of RICA to bring it in line with the Necessary and Proportionate Principles.

(d) Cyber-security and cyber-crimes Bill (2015)

Another piece of legislation which will have an effect on communications surveillance is the Cyber-Security and Cyber-Crimes Bill, 2015 (the Bill) which has been tabled in the South African Parliament for debate. The Department of Justice is also in the process of soliciting public comments from various stakeholders. It was released for public comments in August and ran until 30 of November 2015. The Bill is designed to bring South African law into line with international standards and create specific offences for internet-related crime (Duncan, 2015). These include crimes such as fraud, forgery, extortion and terrorism. The Bill amends RICA by adding additional offences. The drafters of the Bill argue that RICA and the Criminal Procedure Act do not contain adequate measures to investigate cyber-crimes. It contains 57 possible criminal offences involving computer usage - many of which are so broad that they could ensnare ordinary computer users. It criminalises acts such as the unlawful interception of and interference with data, as well as computer-related fraud and cyber-terrorism, and regulates foreign co-operation to fight these crimes. It enables the President of South Africa to enter into agreements with foreign States to promote cyber-security, such as Mutual Legal Assistance Treaties.

Clause 2 and 4 of the Bill will affect users' free expression rights by restricting what individuals are allowed to do with their own computers, devices or electronic communication networks (Electronic Frontier Foundation, 2015). The Bill threatens digital rights in significant ways, especially the freedoms of expression and of association and the right to privacy (Duncan, 2015). As Duncan (2015) observes, if the Bill is passed in its current form, the spies will be given additional responsibilities, including the power to interfere unduly in internet governance and content. For instance, it creates a host of institutions co-ordinated by a cyber-security committee under the political control of the state security ministry. In its current state, the Bill will hand over control of the internet to the Ministry of State Security. This may lead to the undue curtailment of online speech on national security grounds. Given the secretive operations of the State Security Agency (SSA) and the current lack of democratic controls, this Bill can be abused to criminalise cyber-dissent by political actors critical of the ruling party. Besides RICA, the Bill provides for some form of targeted surveillance in order to detect cyber-crimes. The Bill also contains an overbroad definition of computer-related terrorist activity and fails to distinguish between cyber-terrorism and cyber-dissent, when people use digital networks for activism and civil disobedience (Duncan, 2015). According to the Bill, a person convicted of this offence could be jailed for up to 25 years.

The Bill shares some features with the controversial Protection of State Information Bill (informally known as the 'Secrecy Bill') and entrenches some of its features. The Bill's definitions of critical data and 'national critical information infrastructure' are overbroad; for instance, the latter includes any government or state communications network. In contrast, the International Telecommunications Union defines critical infrastructure narrowly, as being what is so vital to the country that its incapacity or destruction would have a catastrophic impact (Duncan, 2015). This means that infrastructure could be declared critical to keep information about it away from the public. The government could well use this Bill and the 'Secrecy Bill' to reduce transparency and intensify secrecy. The Cyber-

security and Cyber-crimes Bill may infringe freedom of speech online because its definitions of impermissible speech go beyond those laid down in the constitution (Duncan, 2015). In a way, some of its provisions undermine the country's hard won data protection (the POPI Act). Besides introducing the censorship of online content through the back door, the Bill also creates a parallel procedural system to RICA for investigation, search and seizure of electronic communications/data which provides wider surveillance powers with fewer checks and balances than in RICA. The Bill's grounds for the issuing of a search warrant are even vaguer than RICA's already vague grounds for the issuing of interception directions. Similar to RICA, the Bill doesn't make provision for the user to be notified after a warrant has been issued, in violation of their rights. It also gags people connected to cyber-investigations from speaking about them, which is likely to reduce transparency and increase the scope for abuse.

(e) The Protection of Personal Information Act (POPI)

The Protection of Personal Information Act (POPI) provides for the protection of personal information, regulates the collection of personal information through electronic transactions or electronic communications and grants the necessary authority to the Department to enforce the provisions. This constitutes the data protection policy in the South Africa. It also provides for the Minister of Communications to prescribe minimum standards on how to manage and maintain critical databases. It is aimed at protecting the data privacy of individuals. Sections 50 and 51 of the Electronic Communications and Transactions Act 2002 provide some extremely limited privacy protections for information collected electronically. The Protection of Personal Information Act also establishes an Information Protection Regulator, although the post has not yet been created. This means that data controllers are obliged to notify the Information Protection Regulator of the broad categories of personal data that they collect, as well as the purpose of collecting and processing such personal information.

Data protection is important in the context of surveillance because it has the potential to protect the right to privacy and ensure protection of personal data. This is of particular concern in light of the requirement under RICA for mandatory SIM card registration, the implementation of the Financial Intelligence Central Act by local banks and the introduction in recent years of government-backed schemes to collect personal data of individuals, such as using of biometrics for passports and banking (Privacy International, APC and Right 2 Know Campaign, 2015). Having oversight bodies like the Information Protection Regulator ensures that personal data of users is not arbitrarily collected under the guise of bulk data collection.

4. Summary of Main Findings

How do the South African communications surveillance laws measure up to the Necessary and Proportionate Principles?

As highlighted above, this section analyses how RICA and other related communications surveillance laws fare when assessed in light of the Necessary and Proportionate Principles. It also examines the overlap between the South African legislation on communication surveillance and the Principles and highlights where laws fails to comply with international human rights standards. Findings in this section are organised in terms of principle by principle as outlined on https://es.necessaryandproportionate.org.

NECESSITY, ADEQUACY, PROPORTIONALITY AND LEGITIMATE AIM

RICA requires all citizens to register their mobile phone SIM cards and to identify themselves for internet services. The problem with this clause (Chapter 7, section 39: 1a) is that it significantly limits the ability of mobile phone users to communicate anonymously and facilities the tracking and monitoring of all users easier for law enforcement and security agencies (Privacy International, 2015). This creates serious vulnerabilities in terms of mass surveillance possibilities. The creation of national data banks associated with SIM card registration facilitates mass communication surveillance. This creates serious vulnerabilities where citizens could be arbitrarily surveilled without following the due process. It places individuals at risk of being tracked or targeted and poses risks against the misuse of private information (Privacy International, 2015). In the absence of comprehensive data protection legislation and judicial oversight, SIM users' information can be shared with government departments and matched with other private and public databases, enabling the State to create comprehensive profiles of individual citizens (Privacy International, 2015). The potential for misuse of such information, particularly in countries in situations of political instability and unrest, is enormous. While the aim of the RICA is legitimate (namely interception of communication to prevent bodily harm and interception of communication for the purposes determining location in case of emergency), it fails the test of necessity and proportionality required to justify measures that interfere with the rights to freedom of expression and privacy. Mandatory SIM card registration also fails the test of proportionality requiring that any interference with the right to privacy needs to be the least intrusive; to be authorised on a case-by-case basis and, most importantly, that the measure in question cannot impair the essence of the right.

At a practical level, mandatory SIM card registration can also have discriminatory effects – the poorest individuals (many of whom already find themselves disadvantaged by or excluded from the spread of mobile technology) are often unable to buy or register SIM cards because they do not have identification documents or proof of residence. Public reports from the RICA judge have not demonstrated how SIM card registrations have assisted the Crime Intelligence Division of SAPs in fighting criminal and fraudulent activities. Research (Donovan & Martin, 2014) has shown that SIM card registration fuels the growth of identity-related crime and black markets to service those

wishing to remain anonymous. Instead of using registered SIM cards, criminals have been found to use illicit cloning of third–party SIMs, foreign SIMs on roaming mode and internet and satellite telephony (Donovan & Martin, 2014). This shows that mandatory SIM card registration as a strategy of curbing crime is ineffective in terms of attaining the intended public interest. The problem with the mandatory registration clause is that it assumes that SIM cards are reducible to one user, but to overcome material constraints, shared usage is common on the continent (Nyamnjoh, 2005). Therefore laws such as RICA which demands real-name registration of SIM are not only ineffective but, by their very nature, indiscriminate and disproportionate; they apply to everyone and interfere with everyone's right to privacy. In order to pass the test of necessity, public reports by the RICA judge to the parliamentary committee must show that mandatory SIM card registration is effective; namely, able to achieve the intended, legitimate result.

Added to the concerns associated with SIM card registration and the effect on the privacy of mobile phone users is the growing activity around IMSI Catchers in South Africa. IMSI Catchers (sometimes known as Stingrays or Grabbers) are mobile phone monitoring technology that, at its most basic, collects all identifying data of mobile phone users in a particular area and the most sophisticated units intercept calls as they are taking place. The technology operates by presenting itself as the strongest base station to all the mobile phones in a particular area. Due to the operating features of a mobile network, these phones automatically connect to the IMSI Catcher, which then gathers the IMSI (International Mobile Subscriber Identity), IMEI (International Mobile Equipment Identifier) and a number of other unique identifiers available. Other models of this technology can also intercept or block calls connecting to the IMSI Catcher. In the United States of America, legislation regulating the use of this technology, specifically, has recently come into effect in Washington State16 and a federal bill has also recently been drafted. The Justice Department passed a new law requiring law enforcement agencies to obtain a warrant to deploy cellphone-tracking devices – such as the grabber – in criminal investigations and inform judges when they plan to use them.

The use of this technology is different from an interception direction or any other current form of power available in RICA. The use of IMSI Catchers does not require the cooperation of service providers; they are not targeted surveillance devices either, intercepting information on all users in the area in which they operate. This creates a high degree of collateral intrusion into the private lives of innocent individuals who have done nothing wrong, other than be in the vicinity of the operation of this technology. In South Africa, IMSI Catchers have been in the media due to their purchase and use by private entities. Most recently, a police officer has been arrested using this technology in a private capacity. As it stands, RICA makes no explicit statement regarding the authorisation for or review of the use of this technology. Nothing is said regarding authorisation or review of the operations using this technology, the procedures for dealing with the collection of innocent individuals' information or about specific circumstances in which it would be acceptable to use this technology In November 2015, the JSCI called for the holding of public hearings on the use of IMSI Catchers in South

[16] https://www.washingtonpost.com/world/national-security/justice-department-agencies-will-have-to-obtain-warrant-before-using-cellphone-surveillance-technology/2015/09/03/08e44b70-5255-11e5-933e 7d06c647a395_story.html

Africa, which provided another opportune moment to bring the country's legislation in line with the Necessary and Proportionate Principles.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS

One area where RICA has been criticised for violating the Necessary and Proportionate Principles is its requirement in Chapter 5 section 30(1a) that telecommunication service providers must provide services which have the capability of being intercepted. Section 30 is also very vague. It imposes two broad obligations: (a) provide a telecommunication service which has the capability to be intercepted. Section 30(1a) is very vague in the sense that it simply say 'capability of being intercepted'. It does not specify what it is required by telecommunication service providers. This violates the Necessary and Proportionate Principle on integrity of communications and systems which suggests that 'states should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for state communications surveillance purposes' (https://es.necessaryandproportionate.org).

The provision of interceptable equipment and services provide the state with targeted surveillance capabilities. Swart found that OIC have surveillance capabilities which can bypass telecommunications providers and the RICA judge. Swart (2015) also heard from her informants that the South African OIC has the technology to intercept people's communications at the touch of a button. The centre can intercept voice calls, record the calls, and read and view WhatsApp messages and Skype messages. As Section 4 will show, this report argues for targeted data interception or data preservation orders, which are different and less intrusive than the blanket untargeted data retention orders allowed under RICA. RICA defines meta-data17 as communication-related information. According to the definition, meta-data denotes 'any information relating to an indirect communication which is available in the records of a telecommunication service provider and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system'. The interception, collection and use of meta-data interfere with the right to privacy, as it has been recognised by the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights18. According to the Court of Justice of the European Union, meta-data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained and concluded that the retention of meta-data relating to a

[17] Meta-data can include the length of phone calls, the phone numbers of the caller and the recipient, the serial numbers of the devices used and sometimes the locations of those who made the call. The meta-data includes information about who phone users call, when they call and for how long.

[18] See report of the UN Special Rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

person's private life and communications is, in itself, an interference with the right to privacy. RICA focuses on real time communication in Section 17, thereby referring to content more broadly. There should be a distinction between the definition of content and meta-data (as defined earlier). This is because the current definition of content in RICA is silent on meta-data issues, yet both provide revealing information about user behaviour. As Bakir (2015) observes, there is a distinction between the 'content' of a message (the actual message), the meta-data (such as information about who sent a message to whom and when or where the message was sent), and 'subscriber data' (data regarding the owner of an account involved in a communication).

Another source of controversy in relation to RICA is that the time period for retention of data by telecommunications companies and internet intermediaries is very long than in comparable jurisdictions. Telecommunications service providers and internet intermediaries are required to store communications-related information at their own expense for not less than three years and not more than five years. These long periods of data retention enable the state to capture huge amounts of personal data and presents opportunities for meta-data abuse. This mandatory data retention clause violates the right to privacy and enables mass communications surveillance. South Africa is also out of step with the prevailing theories of other jurisdictions (Privacy International, 2015). For instance, in April 2014, the Court of Justice of the European Union (CJEU) declared invalid the European data retention directive 2006/24, which mandated the retention of data generated or processed in the provision of communications services and networks. In the joined cases brought by Digital Rights Ireland (C-293/12) and Seitlinger and Others (C-594/12), the Grand Chamber of the CEJU found (in paragraph 66) that the data retention directive 'entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary'.

Besides opening up the potential source for data abuse, the requirements also add to the cost of implementing RICA; given that most of the costs of implementation are borne by the service providers, the requirement may prove to be too onerous for small companies, especially ISPs. Although there is a provision (Chapter 6 (38)) within RICA for an Internet Service Providers' Assistance Fund, the fund covers a limited array of the total costs of implementing the Act. Whilst other jurisdictions require targeted data preservation, RICA requires blanket data retention. Unlike in South Africa, in the USA, PRISM data is stored for five years and UPSTREAM data for two years (Simcox, 2015). Furthermore, in terms of internet and telephony communications data, the British Intelligence and Security Committee (ISC) (2015) acknowledge that such data is highly intrusive given that the volume of data produces rich profiles of people. Recognising its intrusive nature, the USA has restricted its surveillance of American citizens' communications data, with the signing into law on 2 June 2015 of the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring [USA FREEDOM] Act (HR 2048). This imposes new limits on bulk collection of communications data on American citizens. It demands the use of more specific selection terms and prohibits bulk collection using broad geographic terms

(such as a state code) or named communications service providers (such as Verizon) (Federation of American Scientists [FAS], 2015). Given these comparative cases, South Africa should embrace targeted data interception or data preservation orders, which are different and less intrusive than the blanket untargeted data retention orders allowed under RICA.

COMPETENT JUDICIAL AUTHORITY

It is important to note that RICA also meets some of the requirements of the Necessary and Proportionate principles with regard to judicial authorisation of interceptions. The Principles also require that the competent judicial authority should be 'conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights' (Access, 2013). In the South African context, given the operations and appointment of the RICA judge, it is difficult to ascertain whether the judge is able to consult with the independent technical and legal experts necessary to fairly decide complicated issues. It is not clear whether the judicial authority is impartial and independent from other arms of the State; for instance, the executive. Furthermore, the granting of directions is an inherently one-sided process, which means that the judge has to take the information that is given to him on trust (Duncan, 2014). No ombudsman is present to represent users' interests; as a result, the process lacks an adversarial component, which also predisposes it to abuse (Duncan, 2014).

According to section 16 (5) of RICA, there are many grounds for issuing interception directions including whether there are 'reasonable grounds to believe' that a serious criminal offence has been, is being or probably will be committed. This clause allows for too low a threshold for interference with an individual's privacy because 'reasonable grounds to believe that a serious offence has been or is being or probably will be committed' can be abused to justify unlawful surveillance practices. Instead of reasonable suspicion as outlined in RICA, the Necessary and Proportionate principles talk of 'high degree of probability'. The term 'probably will be committed' is particularly concerning with regard to RICA. This clause therefore authorises a violation of the constitutional right to privacy. It also leaves room for the use of speculative grounds to justify unlawful interception. It is also possible to use emergency regulations which allow law-enforcement to seek the judge's permission after intercepting the person's communication. Furthermore, directions may also be issued in relation to serious offences that may be committed in future, which may not be constitutional as it allows law enforcement officers to speculate on future acts that have not yet occurred. This clause does not match the standard of the legitimate aim principle, which requires surveillance to be conducted only in the furtherance of a 'predominantly important legal interest that is necessary in a democratic society'.

RICA also requires law-enforcement agencies to approach a magistrate or high court judge if they want a user's meta-data. As such, this assumes that the content of communication is more important than the meta-data in terms of higher judicial authorisation. This is a lower form of judicial authorisation because it depends on whether magistrate/high court judges have the necessary understanding of the law (and the technology) to authorise use of meta-data. It is important to highlight that the fact

that judicial authorisation for meta-data in South Africa is quite significant because it is not the case in other jurisdictions. South Africa can also make use of a special public advocate in authorisation proceedings to ensure public interest is defended and checks and balances are embedded in the system.

USER NOTIFICATION

There is also no requirement for individuals, who are subject to surveillance of their communications, to be informed of the existence of interception directions once the investigations are concluded or if the application was rejected by the designated judge. This also violates the Principles' stance on user notifications which calls upon states to ensure that their laws ensure that 'the target should be notified of a search before it is conducted unless a government agent can demonstrate to a judicial authority that a delay is strictly necessary to prevent serious jeopardy to the purpose for which communications surveillance is authorised19'. This entails that the State should notify the target of a decision authorising communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies. They should also have access to the materials presented in support of the application for authorisation. Notification should include information that would enable the target to obtain legal guidance and, if he or she so chooses, to challenge the validity of the court order or the scope of the search, including the court order itself and the application to conduct communications surveillance filed with the judicial authority. In other jurisdictions, such as the USA, the public are informed about interceptions directions related to criminal matters, which fosters transparency in the monitoring process.

In cases where a user notification is delayed for a limited period of time upon request of the government agent, the approval of a request should be subjected to rigorous review process. The Necessary and Proportionate Principles say that under normal circumstances, the delay should only be granted for a well-defined, reasonable amount of time that should generally not exceed 30 days. In order to be granted a delayed notification beyond the initial period, the government agent must seek an extension from the judicial authority by showing that the government agent has: complied with all requirements as enumerated in the court order to conduct communications surveillance; made a good faith effort to gather the necessary information within the time allotted to resolve the circumstances which require a delay in notification and prove a demonstrable need for further extension. This means that delayed notification should only be granted if the government agent demonstrates that a delay is strictly necessary to prevent serious jeopardy to the purpose for which communications surveillance is authorised. The judicial authority should take following considerations into account when granting a delayed notification: clear and present danger to the life or physical safety of an individual; flight from prosecution; evidence tampering or witness intimidation. The target should be notified as soon as possible after the rationale for the delay has expired. In Japan, the Act on the Interception of Communications requires that the subject of intercepted communications must be notified of the interception within 30 days of the surveillance having been completed. Where an

[19] https://es.necessaryandproportionate.org

on-going investigation might be compromised by such notice, a district court judge can extend the period of time within which the subject must be notified. This report recommends that RICA should provide for user notification by the State. It should spell out that any delay in notification is only justified in the following circumstance:

1. Notification would seriously jeopardise the purpose for which the Communications Surveillance is authorised or there is an imminent risk of danger to human life;

2. Authorisation to delay notification is granted by a Competent Judicial Authority;

3. The affected user is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.

Social media companies like Facebook and Twitter are legally required under the DMCA to notify the user and provide information on how to file a counter-notice. Twitter and Facebook commit to inform users about requests for their data, unless the situation is an emergency or the company is legally prohibited to do so (MacKinnon, Hickok, Bar & Lim, 2014).

PUBLIC OVERSIGHT

Although RICA makes provision for both internal and external oversight mechanisms (such as judicial, legislative and executive), it is important to highlight that the safeguards are generally weak and open to abuse. According to the Necessary and Proportionate Principles, true oversight mechanisms should operate independently of the state entity conducting surveillance. The Principles further notes that 'the body issuing authorisations for interception should be independent and that there must be either judicial [oversight] or [oversight] by an independent body over the issuing body's activity'. In South Africa, RICA ensures that the Office of Interception Centres (OICs) that carry out the surveillance report to the Minister of State Security and the Parliamentary Joint Standing Committee on Intelligence[20]. A parliamentary committee oversees both the functions (the work of intelligence services) and the review of those practices (the Office of the Inspector General of Intelligence (OIGI). The Office of the Inspector General was created by the Intelligence Oversight Act. The Office of the Inspector General of Intelligence (OIGI) is charged with monitoring the Civilian Intelligence Services. The OIGI monitors compliance with the Constitution, laws and policies of South Africa. Act 40 of 1994 provides for the establishment of the OIGI. The Inspector General of Intelligence is selected by and reports directly to parliament. He/she is an independent person, appointed by the President to oversee the activities of the Intelligence Services. The candidates are interviewed in an open session by the parliamentary committee. The Inspector-General is functionally accountable to the Joint Standing Committee on Intelligence and administratively accountable to the Minister of State Security. The mandate of the OIGI includes investigating complaints on alleged maladministration,

[20] The Joint Standing Committee on Intelligence (JSCI) is a Parliamentary oversight body composed of members of the six largest political parties. Selection of the committee is based on proportional representation decided on by the percentage of votes received in the last national Election. The JSCI hears complaints from the public, scrutinises the finances and operations of the Intelligence Services and reports on these matters to Parliament.

abuse of power, transgressions of the Constitution, laws or policies and corruption or fraud by intelligence services. It aims to ensure that the Intelligence Services operate within the values of the Constitution of the Republic of South Africa.

In terms of RICA, the designated judge is supposed to furnish the parliamentary Committee with an annual report. The parliamentary committee is also mandated to release the public report on the application of RICA. For instance, insufficient information was provided to explain why there was a huge 231% increase in the number of interception directions granted by the designated judge to SAPS's crime intelligence division between 2009 and 2010 (Duncan, 2014). Information should be explained quantitatively as well as qualitatively, so that any person is able to understand how communications surveillance takes place. Transparency reports by the RICA judge should inform the public about usage of communications surveillance authorities and practices and demonstrate how government agents comply with domestic and international laws. Transparency reports should include:

- the total number of each type of request, broken down by legal authority and requesting State actor, be it an individual, government agency, department or other entity, and the number of requests under emergency procedures;
- the total number and types of responses provided (including the number of requests that were rejected);
- total numbers for each type of information sought; total number of users and accounts targeted;
- total number of users and accounts affected; total number of times delays in notification were requested, the number of times that a delay was granted and the number of times a delay was extended;
- compliance rate, provided as a percentage of total requests received and total requests complied with;
- legal challenge rate, provided as a percentage of total requests received and total challenged;
- the number of investigations into filed complaints and the results of those investigations;
- Remedies ordered and/or actions taken in response to any investigations.

As I will discuss later, another lacuna within the RICA process is the absence of a centralised oversight of public disclosures of statistics on meta-data's collection and use (see Section G dealing with insufficient transparency and democratic accountability). This means that there is a lack of sufficient public oversight on the actual workings of the RICA process. Consequently, the public is provided with too little information to be able to monitor whether the Act is achieving its intended

results; namely, to fight crime and to ward of genuine threats to national security (Duncan, 2014). While the Act compels the RICA judge to make periodic reports to the parliamentary committee on intelligence, extant aggregated data shows that little information is being availed. The problem is compounded by the fact that the Intelligence Services Oversight Act which deals with the oversight of the intelligence services is ambiguous about the content of the parliamentary reports. This is also worsened by the fact that there are unacceptable levels of secrecy surrounding the issuance of interceptions directions, the appointment and operations of the RICA judge in South Africa.

Although on paper the South African oversight system is not very dissimilar to the German system, it differs significantly in terms of practice. The South African system constitutes the RICA judge, parliamentary committee and the Office of the Inspector General, whereas the German federal system consists of internal control, parliamentary oversight, independent oversight and a complaint procedure before an independent body (Bakir, 2015). For instance, only a Federal Minister or the highest authority can order surveillance measures. The minister is required to provide the independent G 10 Commission (*G 10-Komission*) every month with an account of the measures he/she has ordered, before such measures are actually implemented. He/she could, however, order the execution of the measure before having informed the Commission if there is a risk that a delay might frustrate the purpose of the measure. This means that, except in urgent cases, the minister must obtain prior approval of the Commission. Furthermore, an official qualified for judicial office supervised the implementation of the measures ordered. The Parliamentary Supervisory Board (*Parlamentarische Kontrollgremium, PKGr*) performs after-the-fact oversight. The minister has to report to the Board on the application of the G 10 Commission at least once every six months, which enables the Board to oversee the overall performance of the system. The Parliamentary Supervisory Board and the G 10 Commission enjoy sufficient independence of the authorities carrying out the surveillance and are vested with sufficient powers and competences to exercise effective and continuous oversight.

TRANSPARENCY

Given the secrecy shrouding the implementation of RICA, it is important to note that there is insufficient transparency and democratic accountability in the whole process. Section 42 of RICA prohibits the disclosure of any information on the demands of interception. As a result, telecommunications companies are barred from publishing information, including aggregated statistics, both of interception of communications and of meta-data. This is contrary to the transparency principle which suggests that 'States should be transparent about the use and scope of communications surveillance laws, regulations, activities, powers or authorities'. While the parliamentary committee to oversee the work of intelligence services in South Africa is mandated to release public reports on the application of RICA, the information released since 2008 has at most contained bald statistics on the number of interception orders granted. As Duncan (2014) notes, the aggregated data does not provide the number of individuals whose communications are subject to interception (only the number of warrants, that could include any number of individuals.) It does not spell out the details on the reasons these interceptions are carried out or the outcome and effectiveness they may have in preventing or

investigating crimes. Most directions are granted to the State Security Agency. Compared to the South African context, in the US federal system, the publicly available annual reports on 'wiretaps' in relation to criminal matters include information on the number of interception orders, the major offences for which orders were granted, a summary of different types of interception orders, the average costs per order, the types of surveillance used and information about the number of arrests and convictions resulting from intercepts.

As intimated earlier, social media companies like Facebook and Twitter publish data sets known as transparency reports. Facebook's 'Government Request Report' provides much more detail about government requests for user data – including information about compliance rate and request types – than its very basic and incomplete information about content restriction requests (MacKinnon et al., 2014). Since its first transparency reports in 2012, Twitter has disclosed content removal requests. In addition to what Facebook discloses, Twitter's report also includes compliance rate, content withheld as well as copyright takedown notices. Twitter also distinguishes itself from Facebook in transparency about content restriction by publishing copies of the content restriction and takedown requests it receives to the Chilling Effects website (MacKinnon et al., 2014). In terms of government data requests, Twitter also provides details on types of requests and compliance rate, as well as data about information disclosed to authorities during emergencies.

While reports by the RICA judge to the parliamentary committee are in theory commendable in terms of ensuring transparency with regard to government surveillance activities, it is evident from the practice – or lack of practice – that the data released through these reports falls short of acceptable international standards (Duncan, 2014). Transparency reports must contain all relevant information related to the implementation of the RICA process. The reports must contain the following information:

- total number of each type of request, broken down by legal authority, including the total number of requests under emergency procedures;
- total numbers for each type of information sought; total number of users and accounts targeted;
- total number of users and accounts affected; total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended;
- compliance rate, provided as a percentage of total requests received and total requests complied with;
- legal challenge rate, provided as a percentage of total requests received and total challenged;
- Total amount of costs reimbursed to the provider by the State.

In June 2014, Vodafone released 'the most detailed transparency report ever'21, describing the laws governing surveillance and reporting in 29 countries, its own policies and procedures and statistics on government requests. In addition, the company revealed related risks to user privacy and free expression, such as where provider's personnel are employed by government security agencies and where governments enjoy direct access to its networks. In the same vein, RICA should provide for South African telecommunications service providers to issue transparency reports. Guidance regarding what is legitimate for telecommunication service providers to release in transparency reports should also be developed. Service providers should also document and publish responses to requests for search and conduct regular reviews of these responses.

DUE PROCESS

The scope of decryption orders has a bearing on the extent of the interference with the right to privacy (Privacy International, 2015). This is largely due to the fact that decryption orders are particularly invasive of the privacy of individuals' digital communications. One significant concern of the laws regulating decryption orders is the over-broad and discretionary powers vested to the relevant authorities to order or carry out decryption. In South Africa, RICA establishes that a designated judge may issue a decryption order. The order may include requiring the decryption key or providing decryption assistance (defined as the assistance which is necessary to obtain access to the encrypted information specified in that decryption direction or to put that encrypted information in an intelligible form.) This follows that under RICA telecommunications or internet, service providers may be ordered to decrypt communications and/or disclose encryption keys, including pertaining to suspects. Their potential for misuse is extremely high. This is particularly worrying in jurisdictions where failure to comply with such orders is often considered a criminal offence (Privacy International, 2015). In the UK, a person who knowingly fails to comply with the order is punishable with up to two years' imprisonment.

In some jurisdictions, the relevant authorities have power to order decryption or the handing over of decryption keys. In the UK, under the Regulation of Investigatory Powers Act 2000 (RIPA), a decryption order may require the person believed to be in possession of the decryption key to decrypt or, in special circumstances, to provide the decryption key. The grounds for granting such orders are very broad and vague: if decryption is necessary in the interest of national security, crime prevention or detection or the UK's economic well-being. In the UK, data on numbers of decryption requests are provided by the Chief Surveillance Commissioner's Annual Reports. During the 2013–2014 period which was covered in the last annual report, the National Technical Assistance Centre (NTAC) granted 76 approvals from 76 applications. The punishments meted out in cases where people were convicted for not complying with the decryption order are not mentioned in the Commissioner's reports. In view of the foregoing discussion about the UK context, the South African RICA judge should publish information of decryption requests outlining number of applications, approvals and disapprovals.

[21] Peter Micek, Vodafone reports on law enforcement access to user data, worldwide, Access, June 6, 2014, https://www.accessnow.org/ blog/2014/06/06/vodafone-reports-on-law-enforcement-access-to-user-data-worldwide.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS

States should enact legislation criminalising illegal communications surveillance by public and private actors. Besides the Office of Interception Centre (OIC) which is allowed to intercept communications under RICA (Chapter 6, 32 to 37), the National Communications Centre (NCC) which falls under the Ministry of State Security, also carries out electronic communications surveillance. The NCC is currently involved in the interception and collection of electronic signals on behalf of intelligence and security services. As a branch of the State Security Agency (SSA), the NCC conducts mass and targeted surveillance of both foreign and domestic signals. According to the *Mail & Guardian* (2013), the NCC has the capacity to conduct mass monitoring of telecommunications, including conversations, emails, text messages and data, without judicial authorisations or other safeguards. This demonstrates that the NCC is an extra-legal interception institution which exists outside the RICA legal framework. A Ministerial Review Commission on Intelligence in South Africa (also known as the 'Matthews Commission'), set up to review intelligence gathering, also recommended that the NCC should be regulated under RICA. The Commission observed that the agency carries out surveillance (including mass interception of communications) that is unlawful and unconstitutional (Matthews Commission, 2013). This is because mass interception of communications by the NCC does not comply with the legal statutes of RICA (Matthews Commission, 2013). It is therefore *ultra vires* the proportionality, necessity and adequacy principles. Proportionality requires considering government interests in light of the severity of intrusion and sensitivity of information. As will be discussed in Section Four, the definition of interception as outlined in RICA needs to be changed to bring the NCC under the jurisdiction of the RICA process. The point here is that any measure to collect, control, monitor or take custody of communications amounts to an interception thus constituting an interference with privacy that must be justified in accordance with international human rights law. RICA should prohibit unwarranted, unnecessary, disproportionate or extra-legal attempts to conduct communications surveillance by either law enforcement agents or private actors. Users whose information is obtained without proper authorisation and in violation of RICA should be able to seek redress. Potential routes for remedy should include civil legal actions against the state, as well as non-judicial mechanisms, such as independent ombudsmen or national human rights institutions. Although it is the duty of the State to provide remedy, service providers should incorporate the question of remedy into due diligence, implement accessible and secure grievance mechanisms and respond quickly and effectively to user complaints. Service providers should also adopt appropriate procedures to assist users in seeking remedy, such as investigating alleged breaches, preserving evidence, acknowledging and apologising as appropriate and providing compensation as necessary.

SAFEGUARDS FOR INTERNATIONAL COOPERATION

Unlike in other jurisdictions, RICA does not cover foreign signals intelligence. As it stands, the NCC is responsible for intercepting foreign signals intelligence. This creates friction with the law because under RICA all interception should be carried out by the Office of Interception Centre (OIC). The OIC controls powerful equipment that enables branches of the government's State Security Agency (SSA) to monitor the telecommunications of individuals suspected of criminal or terror activities — telecommunications that include landline calls, faxes, cellular calls, SMSes and MMSes, internet activity, social network usage, emails and messenger services such as WhatsApp and Skype (Swart, 2015). The centre can also monitor meta-data including the time of calls, the numbers called and a caller's location. Foreign signal interceptions are therefore not regulated by RICA, which raises the issue of the constitutionality of its operations, especially in the absence of real checks on executive authority. This is important given that the OIC is the only constitutional entity mandated to carry out all kinds of interception in South Africa. The NCC which is currently performing foreign signal intelligence is not regulated. This means that these signals can be intercepted without a warrant as envisaged under RICA – a major lacuna in the law that has been criticised for creating space for violations of the right to privacy on national security grounds. In light of the ambiguity in the law, activists, investigative journalists and ordinary citizens can be put under surveillance outside of the law and without a judge's direction; that is, if the communication involves a party in a foreign country. Given that a huge chunk of internet traffic originates outside the country, the interception of this information can take place without judicial oversight, which is wide open to abuse. Although the Snowden leaks revealed high incidences of warrantless surveillance, the US law prescribes that the collection of foreign intelligence should be approved by a special secret court.

5. Recommendations for Reform to Ensure Compliance with International Human Rights Law and Standards

In view of the analysis presented above, this section offers a set of legal and policy recommendations in terms of reforming existing laws and devising checks and balances with which human rights are respected in South Africa.

GOVERNMENT

The following recommendations are made for parliament and government:

- Parliament should amend RICA to ensure that people whose communications have been intercepted are informed after the completion of investigations, or if the designated judge refuses to grant an interception direction.
- There is need for RICA to be reformed to include targeted data interception or data preservation orders, which are different and less intrusive than the blanket untargeted data retention.
- Mandatory SIM card registrations should be scrapped from RICA. They violate citizens' rights to privacy and make it difficult for people to communicate anonymously. As Privacy International (2015) notes, anonymity and encryption protect privacy; without effective protection of the right to privacy, the right of individuals to communicate anonymously and without fear of their communications being unlawfully detected cannot be guaranteed.
- The reform process should ensure that a user-notification provision is inserted into RICA. This should provide for user notification after the fact, not during the investigation, so that a challenge can be made if the individual feels that it was an unlawful.
- There is need to strengthen the grounds for the issuing of interception directions in RICA so that it explicitly focuses on 'high degree of probability' rather than 'reasonable suspicion' as outlined in the law.

There is need to define some key terms in the RICA:

- Parliament should define 'national security' in RICA so that the Act is not open to arbitrary abuse by the ruling elite. As it stands, South Africa uses a broad definition of 'national security' which is taken from the human security centred notion as outlined in the 1996 Constitution.
- Parliament should also amend the definition of 'interception' in RICA. According to RICA, 'interception' means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of

the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes:

(a) monitoring any communication by means of a monitoring device;

(b) viewing, examining or inspecting the contents of an indirect communication;

(c) diverting any indirect communication from its intended destination to any other destination

An amendment is long overdue in order to clarify that it covers any measure to collect, control, monitor or take custody of communications (content and meta-data). Mass surveillance falls under the definition of 'intercept' in RICA.

Regulation of the National Communications Centre

- The NCC should be covered by RICA because it seeks to conduct surveillance (Chapter 1 (2) (a)). The current unregulated interception of foreign signals intelligence is unconstitutional and therefore the activities of the NCC should be covered by RICA. The reform of RICA must ensure that the regulation of the NCC goes through white and green paper processes of the parliament.

Disclosure of surveillance activities

- The various arms of government must come clean with regard to the deployment of the grabber. This is a technology with the capacity to enable mass communications surveillance. The government should explain how they use these programmes and which laws govern their deployment. The government should publicly disclose details of the scope and scale of its surveillance activity at the level of clarity and granularity espoused by the Necessary and Proportionate Principles. It is important for the government to explain its relationship with VASTech and how public money is being used to finance its operations to manufacture surveillance technologies. There should be specific statements in RICA around the use of IMSI Catchers and the deletion of collateral intrusion. Legislation should also be explicit about the regulation of hacking in South Africa.

Accountability and oversight mechanisms within RICA

- Parliament should direct the designated judge to outline in his/her annual report how many directions resulted in arrests and convictions. Transparency reports should include:
    - the total number of each type of request, broken down by legal authority and requesting State actor, be it an individual, government agency, department, or other entity, and the number of requests under emergency procedures;
    - the total number and types of responses provided (including the number of requests that were rejected);

- total numbers for each type of information sought;
- the total number of users and accounts targeted;
- total number of users and accounts affected;
- total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended;
- compliance rate, provided as a percentage of total requests received and total requests complied with;
- legal challenge rate, provided as a percentage of total requests received and total challenged;
- number of investigations into filed complaints and the results of those investigations;
- remedies ordered and/or actions taken in response to any investigations.

- There is need to explicitly separate bodies (Inspector General of Intelligence and the RICA judge) around authorisation and oversight/review/investigation of surveillance authorisations. Working 'hand in glove' risks pushing these two institutions too close together and cancelling the benefits of prior judicial authorisation and separate oversight. The oversight of intelligence services can only be effective if it is independent and granted sufficient powers and resources, both human and financial, to fulfil its mandate (see also UN good practices on oversight institutions below). The Fundamental Rights Agency of the European Union (FRA) (2015) provides some innovative oversight mechanisms for surveillance by intelligence services. The report argues that oversight should be a combination of executive control, parliamentary oversight, judicial review and expert bodies.

FIGURE 2: UN GOOD PRACTICES ON OVERSIGHT INSTITUTIONS

UN good practices on oversight institutions

Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law, the effectiveness and efficiency of their activities, their finances and their administrative practices.

Practice 7. Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations and have full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses and obtaining documentation and other evidence.

UN, Human Rights Council, Scheinin, M. (2010)

- The office of the RICA judge can also be further strengthened through appointment of a special public advocate who reviews interception directives and defends the public interest. There is need to include a provision in RICA for an ombudsman to represent users and the public interest when applications for interception directions are made. An independent oversight of the process of issuing interception directions will go a long way in ensuring due process is followed. As the University of Amsterdam (2015) suggests, where secrecy is necessary, this can be implemented by the appointment of a special advocate who defends the public interest or the interest of affected individuals. Alternatively, if the strengthening of oversight institutions cannot be achieved, then another option is to appoint a Surveillance Commissioner who is well resourced financially and technologically literate. In the same vein, an Interception Commissioner can also be appointed who is then compelled by the law to issue public reports as a way of promoting transparency and accountability.

- Parliament should conduct public hearings on intelligence sharing agreements with external partners. The most recent example of this is the Parliamentary inquiry in Germany, which is on-going. This will enable current South African legislation on communication surveillance to come in line with the Necessary and Proportionate Principles.

- The Intelligence Services Oversight Act should also be amended, setting out the required content for reports of the designated judge under RICA. At the very least, annual reports should include the following information: the number of directions granted, the offences for which orders were granted, a summary of types of interception orders, the average costs per order, the types of surveillance used and information about the resulting arrests and convictions.

- There is a need for legislation to strengthen the Office of the Inspector General of Intelligence with regard to financial and technical resources. Oversight bodies such as OIGI should have sufficient resources to perform effective oversight. This includes the attribution of the necessary equipment and staff, resources in terms of information and technical expertise (University of Amsterdam, 2015). This also contributes to OIGI's independence from the intelligence services and the government.

- The Office of the Inspector General of Intelligence should comply with 10 standards of oversight institutions as outlined by the University of Amsterdam (see Figure 3 for an overview). The Intelligence Services Oversight Act should be reformed in such a way that oversight should encompass all stages of the crime investigation and intelligence cycle, including the collection, storage, selection and analysis of data.

- The Office of the Inspector General of Intelligence should be independent from the intelligence services and the government. Judicial oversight offers the best guarantees of independence. Therefore, it is preferable to involve the judiciary in the oversight on secret surveillance and data collection.

- The Office of the Inspector General of Intelligence should be able to declare a measure unlawful and provide for redress. As the University of Amsterdam (2015) notes, oversight bodies for intelligence services should have the power to prevent or end a measure imposed by intelligence services, and oversight bodies should have the power to declare a measure unlawful after the fact and provide for redress.

- The Office of the Inspector General of Intelligence should be able to receive and access information about surveillance. The Intelligence Services Oversight Act must provide a framework for oversight and support public scrutiny of the surveillance powers.

- RICA should be amended to enable telecommunications or internet service providers to publish aggregate information on surveillance orders they receive. Transparency reports will enable telecommunication service providers to disclose aggregate information publicly about orders they receive directing them to provide information to the government. They should be able to make more detailed/confidential information available to oversight bodies (such as parliament, the judiciary and a specialised (non-parliamentary, independent) commission).

Regulation of foreign signals intelligence

- RICA should also be made applicable to foreign signals intelligence unlike the current situation where foreign signals are intercepted by the NCC. These signals should ordinarily be intercepted by the Office of Interception Centres as envisaged under RICA.

FIGURE 3: STANDARDS FOR OVERSIGHT AND TRANSPARENCY OF NATIONAL INTELLIGENCE SERVICES

Standard 1: Intelligence services need to be subject to oversight that is complete. This means it should be complete in terms of: a) the oversight body: the government, parliament, the judiciary, and a specialised (non-parliamentary, independent) commission should all play a role in oversight; b) the moment of oversight: prior oversight, on-going oversight, and after-the-fact oversight, and c) the mandate of oversight bodies: reviews of lawfulness and effectiveness.

Standard 2: Oversight should encompass all stages of the intelligence cycle. Surveillance involves different stages, including the collection, storage, selection and analysis of data. As all these stages amount to an interference with the right to privacy, these separate stages should be subject to oversight.

Standard 3: Oversight of the intelligence services should be independent. In this context, this means independence from the intelligence services and the government. Judicial oversight offers the best guarantees of independence. Therefore, it is preferable to involve the judiciary in the oversight on secret surveillance and data collection.

Standard 4: Oversight should take place prior to the imposition of a measure. In the field of secret surveillance of communications, especially by means of sophisticated technologies now associated with untargeted surveillance, the risk of abuse is high and abuse can have harmful consequences, not only for individual rights but also for democratic society as a whole. Therefore, prior independent oversight on the application of surveillance and collection

Standard 5: Oversight bodies should be able to declare a measure unlawful and provide for redress. Prior and on-going oversight bodies for intelligence services should have the power to prevent or end a measure imposed by intelligence services and oversight bodies should have the power to declare a measure unlawful after the fact and provide for redress.

Standard 6: Oversight should incorporate the adversary principle. The 'adversary principle' is a basic rule of law principle. Where secrecy is necessary, this can be implemented by the appointment of a special advocate who defends the public interest (or the interest of affected individuals). As a result, some form of adversarial proceedings would be introduced without the secrecy of measures to be imposed being jeopardised.

Standard 7: Oversight bodies should have sufficient resources to perform effective oversight. This standard includes the attribution of the necessary equipment and staff, resources in terms of information and technical expertise. This also contributes to their independence from the intelligence services and the government.

Standard 8: Intelligence services and their oversight bodies should provide layered transparency. This means that: a) the individual concerned, the oversight bodies, and civil society are informed; b) there is an adequate level of openness about intelligence activities prior to, during and after the fact and c) notification, aggregate statistics, working methods, classified and detailed information about operations, and general information about what will remain secret under all circumstances is provided.

Standard 9: Oversight bodies, civil society and individuals should be able to receive and access information about surveillance. This standard more or less mirrors the previous one. Clear legislation on receiving and accessing information about surveillance must provide a framework for oversight and support public scrutiny of the surveillance powers.

Standard 10: Companies and other private legal entities should be able to publish aggregate information on surveillance orders they receive. Organisations should be able to disclose aggregate information publicly about orders they receive directing them to provide information to the government. They should be able to make more detailed/ confidential information available to oversight bodies.

Source: University of Amsterdam, Institute for Information Law, 2015: pp. i-ii.

CIVIL SOCIETY

The following recommendations are made for civil society:

- A coalition of existing organisations around internet rights and surveillance should be formed. Instead of reinventing the wheel, organisations such as the Right2Know Campaign, Media Monitoring Africa, FXI and the SOS: Support Public Broadcasting Coalition can begin exploratory discussions on rolling out an anti-surveillance project. The organisation can then rope in other players in the private sector, academia, journalists, trade unionists and community activists interested in communications surveillance issues. It can advocate for the reform of RICA and the Intelligence Oversight Service Act. The envisaged coalition should also make the general public conscious of the violations of the right to privacy (amongst others) associated with mass communications surveillance in South Africa. The coalition can also focus on training its constituencies on various tools available which enable them to circumvent the dangers of mass surveillance.

- Qualitative baseline research should be conducted to ascertain the prevalence of surveillance amongst key constituencies, such as student activists, trade unionists, lawyers, opposition political parties, journalists and civic activists. Similar to the '*Big Brother Exposed'* released by the Right2Know Campaign, this information will form the basis for advocacy and campaigns around the prevalence of mass communications surveillance in South Africa. Research findings should be released publicly to build public awareness of the extent of mass communications surveillance.

- Monitoring of the public reports by the National Assembly's Joint Standing Committee on Intelligence should be conducted on a regular basis. Pressure should be exerted on the committee to direct the RICA judge to publish more information on the implementation of the law.

6. Conclusions

It is clear from the foregoing that mass communications surveillance is not only an issue confronting authoritarian regimes. The South African case has demonstrated that the government conducts both mass and targeted communication surveillance. This is because intelligence and law enforcement agencies are violating the dictates of the RICA legal framework through engaging extra-legal communications surveillance, as evidenced by the creation of the National Communications Centre. This shows that as it stands South African legislation and practice on communications surveillance violates the Necessary and Proportionate Principles. This report has noted that, although the country has laws governing communications surveillance, these are generally inadequate, leaving significant regulatory gaps and providing weak safeguards, oversight and remedies against unlawful interference with the right to privacy, including mass surveillance. For instance, RICA has several clauses which violate the Necessary and Proportionate Principles. These include mandatory SIM card registration, prohibition of disclosure, mandatory installation of telecommunication services and products which are interceptable, long periods of meta-data retention and weak oversight mechanisms. These clauses violate the right to privacy as enshrined in the 1996 Constitution. They also facilitate mass communications surveillance which is not necessary, proportionate and legitimate in a democratic order. The report has also highlighted areas where RICA and the Intelligence Oversight Services Act need to be reformed to conform to the Necessary and Proportionate Principles template.

Bibliography

Access. 2013. Universal Implementation Guide for the International principles on the Application of human rights to communications surveillance. Retrieved from www.accessnow.org. [Accessed September 10, 2015]

Alexander, P. (2012, April 13). A massive rebellion of the poor. *Mail and Guardian*. mg.co.za/article/2012-04-13-a-massive-rebellion-of-the-poor.

Andrejevic, M. (2007). iSpy: Surveillance and power in the interactive era. Kansas: University of Kansas Press.

Bakir, V. (2015). 'Veillant Panoptic Assemblage': Mutual Watching and Resistance to Mass Surveillance after Snowden. *Media and Communication* (ISSN: 2183-2439) 2015, Volume 3, Issue 3, Pages 12-25.

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

Caluya, G. 2010. The post-panoptic society? Reassessing Foucault in surveillance studies, *Social Identities*. 16:5, 621-633

Deleuze, G. (1992). Postscript on the societies of control. October, 59, 3-7.

Duncan, J., Finlay, A., Groome, A., Comninos, A. and Esterhuysen. A. (2014). Mapping the ICT policy environment in South Africa, Association for Progressive Communications (APC) May 2014. Retrieved from www.apc.org.za/APC_PolicyMapping_SouthFrica_20140509. [Accessed October 5, 2015].

Duncan, J. (2014). Monitoring and defending freedom of expression and privacy on the internet in South Africa. Retrieved from https://www.apc.org/en/system/files/SouthAfrica_GISW11_UP_web.pdf. [Accessed August 23, 2014]

Duncan, J. (2011). 'Another View: Time to Oversee the Officials Who Spy on Us', Sunday Times, 30 October 2011, www.timeslive.co.za/opinion/commentary/2011/10/30/another-view-time-to-oversee-the-officials-who-spy-on-us. [Accessed September 17, 2015]

Donovan, P. and Martin, A.K. (2014). The rise of African SIM registration: The emerging dynamics of regulatory change. *First Monday*, 19(2-3). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820 doi: http://dx.doi.org/10.5210/fm.v19i2.4351. [Accessed September 12, 2015]

Electronic Frontier Foundation. (2014). Necessary & Proportionate International Principles On the Application Of Human Rights Law To Communications Surveillance: Background and Supporting International Legal Analysis May 2014. Retrieved from www.eff.org. [Accessed October 5, 2015]

Electronic Communications and Transactions Act 25 of 2002, Chapter XI. Retrieved from www.info.gov.za/view/DownloadFileAction?id=68060. [Accessed August 15, 2015]

FAS. (2015). CRS Legal Sidebar. USA Freedom Act reinstates expired USA PATRIOT Act provisions but limits bulk collection. FAS. Congressional Research Service Reports on Intelligence and Related Topics. Retrieved from www.fas.org/sgp/crs/intel/usaf-rein.pdf. [Accessed November 2, 2015]

FISA Order. (2013). Verizon forced to hand over telephone data—Full court ruling. The Guardian. Retrieved from http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order. [Accessed October 10, 2015]

The Fundamental Rights Agency of the European Union (FRA). (2015). Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks. Vienna: European Union Agency for Fundamental Rights.

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA and the US surveillance state. New York: Metropolitan Books.

Greenwald, G. (2014). 'NSA collecting phone records of millions of Verizon customers daily'. Guardian, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [Accessed July 14, 2014].

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

Hayden, M. (2014). The price of privacy: Re-evaluating the NSA. John Hopkins Foreign Affairs Symposium. Retrieved from: https://www.youtube.com/watch ?v=kV2HDM86XgI. [Accessed October 10, 2015]

Hayden, M. (2015). Getting past the zero-sum game online. Washington Post. Retrieved from: http://www.washingtonpost.com/opinions/dont-let-america-be-boxed-in-by-its-own-computers/2015/04/02/30742192-cc04-11e4-8a46-b1dc9be5a8f f_story.html. [Accessed September 25, 2015]

Hintz, A. (6 October 2015). The Next Snowden Casualty: U.S. no 'Safe Harbour' for EU data). Retrieved from http://www.jomec.co.uk/blog/the-next-snowden-casualty-u-s-no-safe-harbour-for-eu-data/. [Accessed October 3, 2015]

Human Rights Watch. (2014). With Liberty to Monitor all: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy. Washington DC: Human Rights Watch.

Intelligence and Security Committee. (2015). *Privacy and Security: A Modern and Transparent Legal Framework*. House of Commons [12 March]. 2015: 36).

Khumalo, J.A.M. (2010). Statistical briefing by designated judge for the period 1 April 2009 to 31 March 2010. Report to the National Assembly of the Joint Standing Committee on Intelligence.

Kuner, C. (2015). Safe Harbor before the EU Court of Jus-tice. Cambridge Journal and Comparative Law Journal. Retrieved from http://cjicl.org.uk/2015/04/13/safe-harbour-before-the-eu-court-of-justice. [Accessed October 23, 2015]

Kuner, C., Cate, F.H., Millard, C., Svantesson, D.B. and Lynskey, O. (2015). Internet Balkanization gathers pace: Is privacy the real driver? *International Data Privacy Law*, 5(1), 1-2.

La Rue, F. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/ HRC/17/27 (Geneva: United Nations General Assembly, Human Rights Council, 2011), 12, Retrieved from www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. [Accessed August 13, 2015]

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*, Minneapolis: University of Minnesota Press.

Lyon, D. (2003). *Surveillance after September 11*. Cambridge: Polity.

Lyon, D. (ed.) (2006). *Theorizing Surveillance: The Panopticon and Beyond*. Devon, UK: Willan Publishing.

Lyon, D. (2014). Surveillance, Snowden, and big data: capacities, consequences, critique. *Big Data & Society*, July–December, 1-13.

Lyon, D. (2015). The Snowden stakes: challenges for understanding surveillance today. *Surveillance & Society*, 13(2), 139-152.

Mail & Guardian, (2013). Spy wars: South Africa is not innocent, (21 June 2013). http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent. [Accessed September 27, 2015]

Mail & Guardian, (2013). Millions were handed to an SA company that supplied mass surveillance technology to Libya. Retrieved from http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware. [Accessed August 28, 2015]

Mail & Guardian, (2013). DTI 'funded Gaddafi spyware', (22 November 2013). Retrieved from http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware. [Accessed October 12, 2015]

Mathiesen, T. (1997). 'The Viewer Society: Michel Foucault's "Panopticon" Revisited', *Theoretical Criminology* 1(2): 215–33.

Ministerial Review Commission in Intelligence, (2008). 'Intelligence in a Constitutional Democracy/\', Final report to the Minister for Intelligence Services, the Honourable Mr. Ronnie Kasrils MP,

Ni Loideain, N. (2011). Implications of the EC Data Retention Directive for data protection and privacy. In C. M. Akrivopoulou & A. Psygkas (Eds.), *Personal data privacy and protection in a surveillance era: Technologies and practices* (256-272). Pennsylvania: Information Science Reference.

Ni Loideain, N. (2014). Surveillance of communications data and Article 8 of the European Convention on Human Rights. In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reloading data protection: Multidisciplinary insights and contemporary challenges* (pp.183-209). London, UK: Springer.

Ni Loideain, N. (2014b). Is the EU really about to outlaw mass metadata surveillance? Wired. Retrieved from http://www.wired.co.uk/news/archive/2014-04/28/mass-metadata-surveillance-eu. [Accessed September 11, 2015]

Ni Loideain, N. (2015). EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, 3(2): 53-62.

Nyamnjoh, F. B. (2005). *Africa's Media: Democracy and the Politics of Belonging*, London/New York: Zed Books.

Orwell, G. 1949 Nineteen Eighty-Four, New York: Penguin.

Privacy International, (2012). Towards International Principles on Communications Surveillance, Referencing a meeting of experts in Brussels In October 2012, 21 November 2012, Retrieved from https://www.privacyinternational.org/. [Accessed September 5, 2015]

Privacy International, Association of Progressive Communications and Right 2 Know Campaign. (2015). Suggestions for right to privacy-related questions to be included in the list of issues on South Africa, Human Rights Committee, 114th session, June-July 2015 April 2015.

Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002, S. 30(2)(a).

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2013.

Report of the UN Special Rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

Right2Know Campaign, (2015). 'Big Brother Exposed: How South Africa's intelligence structures monitor and harass our movements, unions and activists'. Johannesburg: Right2Know Campaign.

Right2Know Campaign, (2014). Big Brother Exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements: Activist Handbook. Johannesburg: Right2Know Campaign. Retrieved from www.bigbrother.r2k.org.za. [Accessed June 15, 2015]

Rose, R., Hofstatter, S. and Wa Afrika, M. (2012). 'Bugging: How Cops Lied'. Sunday Times. (19 May 2012). Retrieved from www.timeslive.co.za/sundaytimes/2012/05/19/bugging-how-cops-lied. [Accessed August 22, 2015]

Stepanovich, A., Mitnick, D. and Robinson, K. (2014). The Necessary and Proportionate Principles and the US government. Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos). Global Information Society Watch 2014 Communications surveillance in the digital age.

Swart, H. (2011). 'Secret State: How the Government Spies on You', *Mail and Guardian*, 14 October 2011, www.mg.co.za/article/2011-10-14-secret-state. [Accessed October 12, 2015]

Swart, H. (2015). Big Brother is listening on your phone. *Mail and Guardian,* November 13-19. pp: 9-11.

Swart, H. (2015). How cops and crooks can 'grab' your cellphone and you. *Mail & Guardian* November 27 to December 3 2015, pp: 8-9.

University of Amsterdam. (2015). Ten standards for oversight and transparency of national intelligence services IViR (Institute for Information Law) Sarah Eskens, Ot van Daalen & Nico van Eijk. Institute for Information Law.

UN (United Nations), General Assembly (GA) (2014a), Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age. A/RES/68/167, 21 January 2014.

UN, GA (2014b) Resolution on the Right to Privacy in the digital age. Doc. A/RES/69/166, 18 December 2014.

UN, GA (2014c). The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. Doc. A/69/276, 7 August 2014.

UN, Office of the High Commissioner for Human Rights (OHCHR) (2014). The right to privacy in the digital age, A/HRC/27/37, 30 June 2014.

UN, Human Rights Council (2015), Resolution on the right to privacy in the digital age. Doc. A/HRC/RES/28/16, 30 March 2015.

UN, Human Rights Council, Scheinin, M. (2010), Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, Doc. A/HRC/14/46, 17 May 2010.

Wicker, S. B. (2013). *Cellular convergence and the death of privacy*. Oxford, UK: Oxford University Press.

Young, J. M. (2004). Surfing while Muslim: Privacy, freedom of expression and the unintended consequences of cybercrime legislation. *Yale Journal of Law and Technology*, 7: 346-421.