COMMUNICATIONS SURVEILLANCE AND PRIVACY IN SOUTH AFRICA

RIGHT2KNOW

The Surveillance State: Communications surveillance and privacy in South Africa was produced by the Media Policy and Democracy Project for the Right2Know campaign.

March 2016

Contact the Right2Know
Community House
41 Salt River Road
Salt River, Cape Town
7925, South Africa
Phone (021) 447 1000

Email admin@r2k.org.za
Web www.r2k.org.za
@r2kcampaign
fb.com/right2know

The Media Policy and Democracy Project is a joint collaborative research project between the Department of Communication Science at the University of South Africa (UNISA), and Department of Journalism, Film and Television at the University of Johannesburg which was launched in 2012, and aims to promote participatory media and communications policymaking in the public interest in South Africa.

The project involves three main focus areas:

1. Media diversity and transformation
2. Media accountability and media freedom
3. Communications policy and the public interest

Contact details for the MPDP: jduncan@uj.ac.za, reidjbj@unisa.ac.za, or smiltovc@unisa.ac.za.

The Surveillance State

Communications surveillance and privacy in South Africa

Contents

EXPLANATIONS OF KEY WORDS ARE SET IN RED SQUARES

THE BIG PICTURE

The human race is being watched and listened to more than ever! This is not because governments or corporations have all of a sudden entered into a love affair with democracy. Rather, in most cases it is **because those in and with power and wealth are afraid of ordinary people and more especially those who are struggling for political freedom and socio-economic justice and equality**. It is also because they now have the technological means to engage in a wide range of communications surveillance.

Here **in South Africa activists, whistleblowers and those that have fallen on the wrong side of the ideological, class and/or political 'fence' know this reality all too well. So too do those in government who are prepared to take an honest look at the bigger picture.** For example, members of the 2008 Ministerial Review Commission on Intelligence (the 'Matthews Commission ') who found that the country's intelligence services were engaging "in signals monitoring that is unlawful and unconstitutional" and that "some senior officials believe that it is legitimate to break the rules".

Whether in South Africa or across the world, advancements in digitisation and internet access have led to the **coming together of different forms of communications** (for example – calls, e-mails, web searches, online chats, online shopping) **to one device** that is both mobile and internet-enabled.

This has been coupled to **the increasing commonality of struggles** (of progressive activists and movements across the globe) in response to the parallel universalisation of poverty, inequality and elite-repression (which have been on the rise) as well as intensified political, socio-economic and religion-inspired conflict, most particularly involving core western countries.

In turn, this has led to a wide range of surveillance activity of different kinds of information – for example, the content of communications, meta-data *(see explanation)* and user behaviour. Much of this surveillance is directed at both anti-systemic/political activists and those who are considered as 'terrorists' and/or belonging to movements/groups that are 'enemies' of the state etc. *(see explanation of difference between mass versus targeted surveillance as well as communications surveillance versus interception)*

Meta-Data

Relates to information generated or processed as a consequence of a communication's transmission. It 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 (e.g. mobile phone network or Internet service provider). It 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 is storable, accessible and searchable. Meta-data is a rich source of personal information as it reveals a whole range of information about every electronic communication we make and can provide very detailed information regarding an individual's beliefs, preferences and behaviour

Collection of meta-data

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 (Federation of American Scientists [FAS], 2015).

Mass versus targeted communications surveillance

Mass surveillance: This is the subjection of a population or significant component of a group to indiscriminate monitoring. Any system that generates and collects data without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance and it increasingly involves the generation, collection, and processing of information about large numbers of people.

Targeted surveillance: This is surveillance directed at particular individuals. Targeting methods include the interception of communications and the use of communications data.

Existing legislation and practices in many countries have not been reviewed and updated to address the threats and challenges of communications surveillance, especially on a mass level, in the digital age

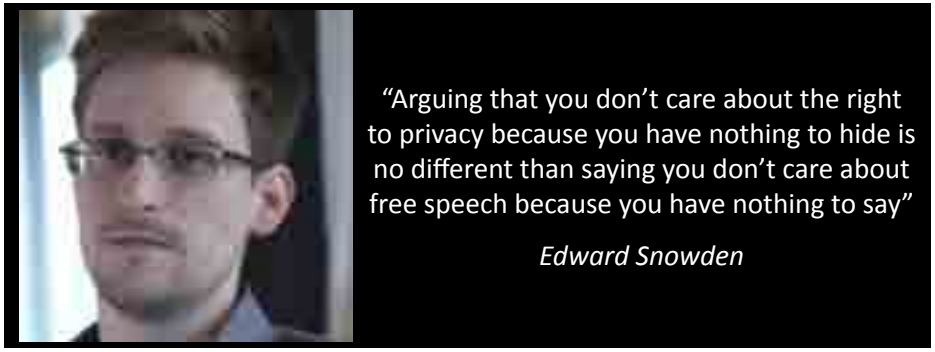
In general, safeguards against unlawful interception of communications that have been put into place – for example to protect personal privacy – are lower for information generated or processed as a consequence of a communication's transmission (called metadata – *see explanation)* **than they are for the actual content of the communication.**

Sharing arrangements between communications service providers and then also between providers and the state, as well as widespread access to communications data by many state/ public bodies, has resulted in **surveillance and ad hoc practices that are beyond the supervision of any independent authority/oversight and take place without judicial authorisation.** For example, in the mid-2000s South African state intelligence's mass surveillance capacity was used to unlawfully intercept the phone calls of leading figures in the Scorpions while they were finalising corruption charges against Jacob Zuma during his ascendency to the Presidency.

Communications interception versus surveillance

Interception: Interception of communications takes two forms: the collection and monitoring of communications data (e.g. records of who contacted whom, when, from where and for how long); and, the acquisition (including listening, viewing and diversion) of the content of the communications themselves, to a person other than the sender or recipient or intended recipient of that communication.

Surveillance: This encompasses a broad range of activity involving (electronic) communications networks. It includes not only the actual reading of private communications by 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.



SNOWDEN'S REVELATIONS

Edward Snowden is probably the best known whistleblower on earth. After years of working at the US Central Intelligence Agency (CIA) and National Security Agency (NSA), Snowden blew the whistle on both the US government's and other Western countries' intelligence services secret mass surveillance programmes and capabilities. His revelations generated unprecedented global attention and debate around the world on privacy intrusions and digital security.

Snowden revealed detailed information about several programmes involving the mass surveillance of communications belonging to individuals both within and outside of the United States

What this showed was the extent, nature, and means of contemporary mass digital surveillance of citizens by their security and intelligence agencies and the role (or lack thereof) of public oversight mechanisms in holding such agencies to account

Further, it revealed the **significant role played by the private sector in the mass surveillance of communications for governments**.

More specifically, that there **are extensive and indiscriminate surveillance efforts** across the globe and that as a result, there have been (and continue to be) **violations of fundamental rights which, in turn, raise substantial legal and policy questions.**

Snowden's revelations have also sharply raised the issue/question of **the impact of technology on mass surveillance as well as the lack**

of protection for user data associated with communications service providers (for example, cell phone companies).

While all of this has resulted in **some reform of communications and intelligence service legislation** (aligned with *International Principles on the Application of Human Rights to Communications Surveillance* – also known as *'The Principles'*), **in other cases new laws have been passed (or are being considered) in many countries that give further powers to intelligence and security services to spy on people and intercept their communications**.

WHY SHOULD WE BE CONCERNED?

Crucial human rights such as the right to privacy, freedom of expression, freedom of assembly and access to information can be systematically eroded if technologically-driven challenges are not addressed and democratic control exercised over those, both in the public and private sectors who possess substantial political/economic power combined with access to the latest surveillance technology.

Surveillance can have a hugely chilling effect on political activism, protest, debate, investigative journalism and the practice of human rights law and thus the overall character of critical democratic engagement, dissent and the ability of weaker groups to question and challenge those with/in power.

The extent of powers granted to state security agencies, weak oversight bodies and the growing levels of unlawful and mass state surveillance (including within democratic states)**,** all combine to create a societal framework of distrust, fear, division and paranoia.

Metadata gathered through mass surveillance is regularly used by many states in 'terrorism' profiling. This can, and does, lead to a range of rights violations and in some cases, targeted assassinations.

There are numerous, negative **implications posed by large-scale secret monitoring for individual's rights to privacy and the security of their personal data** including the relationship (whether forced or

voluntary) between internet service providers and the state as well as legal requirements for citizens to register their SIM (Subscriber Identity Module) cards – as is the case in South Africa.

Many states continue to have a lack of adequate legislation and/or enforcement as well as weak and ineffectual procedural safeguards. In particular mass surveillance, which should be expressly prohibited, is largely taking place under the legal radar.

Intelligence sharing practices have been used to circumvent national legislation which limit the capacity of security services to collect and examine personal communication and data

There is an overreliance on narrow territorial protection of human rights when communication has become transnational and borderless

Both the (USA) Communication Assistance for Law Enforcement Act (CALEA) of 1994 as well as the European Telecommunications Standards Institute (ETSI) have led to **the development of a handover interface standard – which allows communications to be routed to government interception centres.** Internet service providers are required – as is the case with South Africa's *Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA)* – to use digital switches that have surveillance capabilities built into them.

"We kill people based on meta-data"

General Michael Hayden, former director of the US National Security Agency (NSA) and the Central Intelligence Agency (CIA)

South Africa has, throughout the democratic transition from apartheid, seen intense and widespread **socio-economic as well as racial division/conflict** and has been characterised by **high incidences of social protests and xenophobic violence** against foreign nationals.

Further, in more recent years there has been **intensified political and ideological division and conflict**, within the ruling party (the African National Congress) as well as its Alliance partners (the Congress of South African Trade Unions and the South African Communist Party) as well as within broader society. Added to this volatile mix, are South Africa's **strong traditions of investigative journalism, trade unionism and social movement activism.**

Cumulatively, this **has provided fertile ground for both the state and the private sector to make use of and push for greater surveillance powers** (through existing and new legislation) as well as **engage in communications surveillance** against those who are (or might be) perceived as political 'enemies', competitors for economic power and access as well as exposers of wrong-doing/corruption/mismanagement.

Additionally, it has given added space and reason for less principled members of the state's security apparatus to **abuse and misuse the state's surveillance capabilities for internal party/state factional purposes.**

It is within this macro-context that **we need to ask the question as to how the South African legislation on communication surveillance –** most especially as contained in the *Regulation of Interception of Communications and Provision of Communications Related Information Act* (RICA) which is the main law covering communication surveillance -**measures up to applicable human rights law** (as illustrated in 'The Principles').

Some good framing examples of why such a review is necessary are:

- South Africa adopted the CALEA and European Telecommunications Standards Institute (ETSI) standards in 2005, allowing users' data to be routed to interception centres.
- While the Intelligence Services Amendment Bill was meant to govern the operations of the State Security Agency's (SSA) National Communications Centre (NCC), it has not been passed into law but held over to debates on intelligence policy and the proposed State Security Agency Bill, neither of which has yet taken place. Practically, this means that the mass surveillance capacities of the state are effectively unregulated by a dedicated law which sets out its powers, functions and lines of accountability. Such a situation is hugely problematic and indeed dangerous, as the NCC is the most powerful surveillance tool the state has.
- There is ample evidence to show that state surveillance of communications has been carried out outside of the RICA legal framework in ways that violate the right to privacy *(see explanation)* as enshrined in the Constitution. Accumulated case law and research/evidence (including the government's own investigation in the mid-2000s – the 'Matthews Commission'[1]) confirms that the NCC has indeed engaged in "unlawful and unconstitutional" conduct.
- An international transparency report by Vodafone – which highlights how many times government agencies access customer's voice and data traffic – did not contain any details about requests made to Vodacom (its South African subsidiary) by the South African government because Section 42 of RICA prohibits the disclosure of any demand for lawful interception or communications data that has been issued under the Act.
- The various requirements; under *RICA* for mandatory SIM card registration, under the *Financial Intelligence Central Act (FICA)* for the collection of personal financial data of individuals, and also the more recent use of biometrics for passports and banking are all crucial in the context of surveillance because they have the potential to violate the right to privacy and compromise the protection of personal data.

Right to privacy

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. 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. As with other rights in the Constitution, limitations to the right to privacy 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".

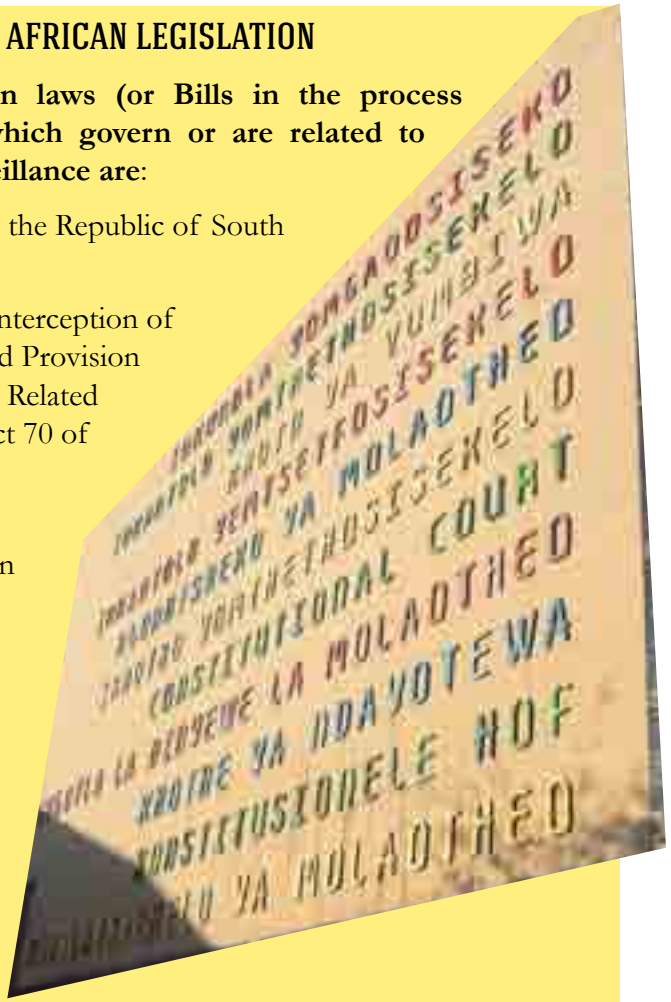
[1] The 'Ministerial Review Commission on Intelligence' (but popularly known as the 'Matthews Commission, so-named after its Chairperson, Joe Matthews) was appointed by then-Minister of Intelligence Ronnie Kasrils to review the operations of all intelligence entities (excepting crime and defence intelligence) with the aim, "to strengthen mechanisms of control of the civilian intelligence structures in order to ensure full compliance and alignment with the Constitution, constitutional principles and the rule of law, and particularly to minimise the potential for illegal conduct and abuse of power."

"The intelligence organisations have not shed sufficiently the apartheid-era security obsession with secrecy. Their emphasis is on secrecy with some exceptions when it should be on openness with some exceptions."

Ministerial Review Commission on Intelligence (chaired by Joe Matthews, pictured here) - 'Intelligence in a Constitutional Democracy'

SOUTH AFRICAN LEGISLATION

The South African laws (or Bills in the process of becoming law) which govern or are related to communication surveillance are:



- The Constitution of the Republic of South Africa (1996)
- The Regulation of Interception of Communications and Provision of Communications Related Information Act (Act 70 of 2002) (**RICA**);
- The Protection of Personal Information Act (Act 4 of 2013) **(POPI)**
- The Financial Intelligence Central Act of (Act 38 of 2001) **(FICA);**
- The Intelligence Services Oversight Act (Act 40 of 1994) **(ISOA)**
- The CyberCrimes and CyberSecurity Bill (2015) **(CAC)**
- The Electronic Communications and Transactions Act (Act 25 of 2002) **(ECTA)**;
- The General Intelligence Laws Amendment Act (act 11 of 2013) **(GILAB)**;
- The Criminal Procedure Act (Act 51 of 1977) **(CPA)**
- The Films and Publications Act (Act 65 of 1996) **(FPA)**

WHAT OUR LAWS SAY

THE CONSTITUTION: Our rights: Section 14 provides every citizen with the 'right to privacy' as well as 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.

Mandate of the security services (army, police and intelligence): All security services are required to "act … in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic". In order to ensure transparency and accountability of these services, "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." Surveillance 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.

RICA: The most crucial piece of legislation when it comes to communications surveillance is RICA. The stated aim of RICA is to regulate the interception of communications and associated processes such as applications for and authorisation of interception of communications. The law see such regulation primarily as a means to combat criminal and 'terrorist' activities. According to RICA, the interception of domestic communications can only be done after judicial authorisation and only then after meeting certain conditions; namely, if there are reasonable grounds to believe that a criminal offence has been or is being or probably will be committed. However, the law makes no provision for the relevant person/organisations to be notified after a warrant has been issued, in violation of their rights. RICA also requires all South Africans to register

Protection of private data

The Safe Harbour Agreement is a formal agreement made between the EU and the US in 2000 to protect private data collected by internet companies. It is designed to regulate the lawful transfer of personal data by companies between the EU, the USA, and other countries.

their SIM cards with their mobile phone providers, supposedly so the state can track the activities of suspected criminals or victims if needed. RICA also makes it illegal to establish communications networks that are not capable of interception and places obligations on communications service providers, including Internet Service Providers (ISPs), to assist the state in the interception of communications.

POPI: POPI provides for the protection of personal information/data privacy; regulates the collection of personal information through electronic transactions or communications; and, grants the necessary authority to the Department to enforce the provisions. POPI also establishes an Information Protection Regulator and directs that any entity which collects and stores/controls data is obliged to notify the Regulator of the broad categories of personal data that they collect, as well as the purpose of collecting and processing such personal information. However, at the time of writing, the information regulator had not been set up yet, meaning that surveillance was taking place without people being able to enforce their right to privacy through protection of their personal data.

FICA: The principal objective of the Act is to "assist in the identification of the proceeds of unlawful activities and the combating of money laundering activities". The information gathered by the Centre can encompass for example, all information associated with any financial transaction between an individual or a company and a banking institution. Such information must be kept by the institution (or a third party delegated by the institution) for a period of 5 years. Any/all of this information can then be made available to investigating authorities, including the security and intelligence services. It can also exchange such information with bodies in other countries that "have similar objectives regarding money laundering activities, the financing of terrorist and related activities, and other similar activities."

ISOA: The Act provides for the establishment of a Committee of Members of Parliament on Intelligence as well as the appointment of an Office of the Inspector-General of Intelligence (OIGI). These are the two key elements of South Africa's intelligence oversight. In particular, the OIGI is mandated to monitor compliance of the intelligence services with the Constitution as well as applicable laws and relevant policies … to review

the intelligence and counter-intelligence activities of any Service [and] … to receive and investigate complaints from members of the public and members of the Services on alleged maladministration, abuse of power, transgressions of the Constitution, laws and policies". In carrying out this legal mandate, the OIGI has powers to access "any intelligence, information or premises under the control of any Service". However, if "the intelligence or information received" by the OIGI "is subject to any restriction in terms of any law" he/she can only disclose it "after consultation with the President and the Minister responsible for the Service in question" and "to the extent that such disclosure is not detrimental to the national interest."

CAC: Recently tabled in Parliament for debate, the Bill has already been through a process of public comment. It is officially designed to bring South African law into line with international standards and create specific offences for internet-related (cyber) crime such as fraud, forgery, extortion and terrorism. The Bill amends RICA by adding 57 possible criminal offences involving computer usage. Despite it criminalising acts such as the unlawful interception of and interference with data, there are a range of serious concerns.

HOW DO THINGS 'WORK' IN THE REAL WORLD?

ACTIVISM & EXAMPLES OF SURVEILLANCE AND INTELLIGENCE ABUSE IN SOUTH AFRICA

Public officials in South Africa have had their communications illegally intercepted by the state. One example is the former Chief of the South African Revenue Service (SARS), Oupa Magashula whose telephone conversation – in which he made an improper offer of employment to a young woman – was secretly recorded as part of a sting operation on the former South African Police Service (SAPS) chief Bheki Cele. While it is clear that what Magashula did was wrong (with a subsequent SARS investigation leading to his resignation), the fact remains that the interception of his communications was illegal and therefore a direct violation of not only his privacy rights but also of the law (RICA).

Applications in 2010 by the Crime Intelligence Division (CID) of the SAPS to tap the communications of two *Sunday Times* investigative journalists were granted under very suspect circumstances. All evidence suggests that the CID took advantage of RICA's low threshold of surveillance to obtain judicial approval to intercept mobile phones by providing fictional names and suggesting such interception was needed to investigate a criminal syndicate.

In February 2015, Al-Jazeera News reports on the international 'Spy Cables' documents obtained by Wikileaks, 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 and (according to the *Mail & Guardia*n) continues to do so. While there is little information about whether VASTech equipment has been used in South Africa, it is highly likely given the fact that several years ago VASTech supplied mass surveillance technologies to the Libyan government of Colonel Gadhafi and a 2005 leaked report also revealed that an Iranian delegation met with

the South African government and companies such as VASTech in a bid to obtain surveillance technology.

"The best weapon of a dictatorship is secrecy, but the best weapon of a democracy should be the weapon of openness"

Niels Bohr (1885-1962) – Danish physicist, Nobel Laureate

Research by Heidi Swart for the *Mail & Guardian* last year (2015) shows that it is easy for law enforcement agencies to obtain metadata illegally from telecommunications operators. Rather than following the law under RICA which requires law enforcement officials to apply for a court order/warrant, police officers who were interviewed indicated that, in direct violation of RICA, they simply approached service providers and requested information and/or meta-data related to specific cell phone numbers relevant to their cases.

Further research by Swart revealed how the Office of Interception Centres (OIC) can intercept communications without the knowledge of either telecommunication service providers or a RICA judge. Both the SSA and CID as well as private corporations and individuals have evidently acquired surveillance equipment, like the grabber, which allows them to track the whereabouts of a mobile phone and monitors the communications in real time. The use of the grabber is not regulated by RICA.

In early 2014, two academics at the University of Johannesburg – with well-known links to community organisations – conducting a multi-year research project on protest activity had their laptops stolen in break-ins at both their offices and homes, after publicising some of the research project findings. Soon thereafter, the project's online data storage facility containing all their interviews was compromised in a cyber-attack. Although there is no direct evidence that such illegal activities were carried out by the state's intelligence services, given the nature of the research it is difficult to imagine that it was the work of disgruntled individuals or ordinary criminals.

Research by the Right2Know Campaign has detailed many examples of political and community activists/organisations that are critical of the state/ruling party and who engage in regular protest, being subject to regular physical surveillance, harassment and threats by security and intelligence services. Evidence gathered shows a clear link between physical and communications surveillance. None of these cases have ever been seriously followed up by either law enforcement/intelligence or oversight structures (including the OIGI) and no one has ever been criminally prosecuted.

In a prime example of how communications surveillance has become globalised and often appears to be linked to close relationships between governments and corporate capital, one of South Africa's oldest and most respected human rights legal NGOs – the Legal Resources Centre (LRC) – was the subject of unlawful surveillance by British intelligence services during 2015. The LRC, which has been at the forefront of representing victims of the Marikana massacre that took place at a mine owned by LONMIN[2], has since indicated that this experience has forced them to become much more cautious with client information and to adopt counter-surveillance practices.

Nkaneng informal settlement outside Lonmin's Marikana mine.

[2] LONMIN is a British-based mining corporation of platinum group metals (which besides platinum include: gold, copper, nickel, chrome and cobalt) whose core operations are in South Africa

A DIFFERENT STANDARD:
THE NECESSARY AND PROPORTIONATE PRINCIPLES

'The Principles' are founded on established international human rights law and jurisprudence. Officially launched at the UN Human Rights Council in Geneva in September 2013 with the final publication occurring in May 2014, they were initially drawn up by a wide range of privacy and security specialists from across the globe. Later, human rights and digital rights campaigners joined the final drafting process. They outline how international human rights law applies in the context of communication surveillance and provide a framework for assessing human rights obligations and duties when conducting communications surveillance. Below is a summary of 'The Principles':

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 an important legal interest 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 be 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.

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.

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

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.

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

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

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

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS: States should enact legislation criminalising illegal communications surveillance by public and private actors.

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.

THE MAIN QUESTIONS

Question 1: How do South African communications surveillance and intelligence laws – mainly RICA – measure up to 'The Principles'?

NECESSITY, ADEQUACY, PROPORTIONALITY & LEGITIMATE AIM

WHAT DOES THE LAW SAY?

- RICA requires that all cell phone users in South Africa register their cell phone SIM cards and identify themselves for internet services. RICA also sets up the OIC.

WHAT'S THE PROBLEM?

- Drastically reduces the ability of cell phone/internet users to communicate anonymously and facilities the tracking and monitoring of all users – including through the collection of meta-data – by law enforcement and security agencies without due process.
- Creates the space for the misuse of personal communications and information for political and factional purposes (for example, the targeting of activists and whistle-blowers) in direct violation of rights to freedom of expression and association.
- Does not prevent the sharing of user communications and information with other government departments as well as private and public databases, which enable the creation of comprehensive personal and life/work profiles of users that violate the right to privacy.
- Discriminates against poor people (many of whom already find themselves disadvantaged by or excluded from the spread of mobile technology) who are often unable to buy or register SIM cards because they do not have identification documents or proof of residence.
- Has no demonstrable and positive impact on achieving its main aim (i.e. to combat criminal activity). Instead, research shows that SIM card registration actually fuels the growth of identity-related crime and black markets to service those wishing to remain anonymous.

KEYWORDS: Indiscriminate; Disproportionate; Ineffective

INTEGRITY OF COMMUNICATIONS & SYSTEMS

WHAT DOES THE LAW SAY?

- RICA requires that communication service providers ensure that their communication networks/ systems have the "capability of being intercepted" and places obligations on service providers to assist the state in the interception of communications.

WHAT'S THE PROBLEM?

- Opens the door for unknown and unregulated monitoring, surveillance and retention equipment to be built into networks/systems because the law does not specify what kind of "capability" (for interception) is required by communications service providers. When users are left completely in the dark, the user system loses its integrity.
- Does not deal adequately with the interception, collection and use of communications meta-data. While the provision of interceptable equipment by service providers does give the state targeted surveillance capabilities over communications content, RICA's definition of content is silent when it comes to meta-data. There is more than enough evidence to confirm that the OIC have the technology to bypass such equipment and thus possess the capability to engage in parallel, untargeted and again unknown and unregulated, interception, collection and use of communications meta-data. Without any specific right to privacy lines drawn, there can be no trust.

- Sets mandatory periods for the blanket retention of data by telecommunications companies and internet intermediaries which violate the right to privacy and enables mass communications surveillance. The lengthy periods for data retention – not less than three years and not more than five years – enables the state to capture huge amounts of personal data and presents opportunities for meta-data abuses.
- The requirements favour large, corporate communications and internet service providers because they add to the already significant costs of implementing RICA – most of which have to be carried by the service providers themselves. In turn, this negatively impacts on the affordability of services for the majority of South Africans who are poor.

KEYWORDS: Unregulated; Blanket Retention; Discriminatory

COMPETENT JUDICIAL AUTHORITY

WHAT DOES THE LAW SAY?

- RICA requires that any application for the issuing of an "interception direction" of communication "in the course of its occurrence or transmission" be made to a judge specifically designated by the Minister of Justice to hear such applications. However, when it comes to meta-data access, law enforcement agencies/personnel are required to approach a sitting magistrate or high court judge.
- RICA provides several grounds for issuing interception directions including if there are "reasonable grounds to believe" that a serious criminal offence has been or is being or probably will be committed. Further, RICA allows law-enforcement agencies/personnel to seek a designated judge's permission after intercepting the person's communication as well as in relation to serious offences that may be committed in future.

WHAT'S THE PROBLEM?

- Given that RICA's "designated judges" are chosen directly by the Minister there arise serious concerns about whether the judge is impartial and independent from other arms of the state such as the Executive and also

whether the judge is able to consult with the independent technical and legal experts necessary to fairly decide complicated issues.

- Does not allow for the position of a relevant Ombudsman who could represent users' interests in the applications to grant interceptions. As such, the proceedings will inevitably be one-sided, lack any adversarial component and be predisposed to abuse.
- Allows for a lower level of judicial authorisation for access to and use of, a user's meta-data – through the Magistrate's or High Court – that raises concerns about whether these judges have the necessary understanding of the law and the technology to make judgements authorising the access to and the use of, meta-data
- Establishes an extremely low threshold for interference in an individual's privacy by allowing several shaky grounds for issuing interception directions, including; if there are "reasonable grounds to believe" that a serious criminal offence has been or is being or probably will be committed. Such grounds leaves much room for speculation and guesswork (on acts that have not yet even occurred) as the basis for justifying surveillance practices that would constitute a violation of the right to privacy and be potentially illegal.

KEYWORDS: Bias; Expertise; Speculation

USER NOTIFICATION

WHAT DOES THE LAW SAY?

- RICA has nothing to say about user notification. In other words, there is no requirement for individuals and/or organisations subject to surveillance of their communications to be informed of the existence of interception directions either before the 'investigation' begins or once the 'investigation' is concluded. Further, there is no requirement to notify the targeted individual and/or organisation if the application for an 'interception direction' was initially rejected by the designated judge.

User Notification:

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 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.

WHAT'S THE PROBLEM?

- Without any notification requirements, the targeted individual and/or organisation have absolutely no way of challenging – whether legally or by seeking other remedies – the court order authorising surveillance and/or the content and scope of the surveillance. This is in conflict with the right to just administrative action and equality before the law.
- Those subject to surveillance will have no idea why they are being targeted and will have no recourse to challenge an application, because they will have no access to whatever materials are presented in support of the application. This directly violates the right of access to information as well as just administrative action.

KEYWORDS: Non-notification; Unjust

PUBLIC OVERSIGHT

WHAT DOES THE LAW SAY?

- RICA contains general provisions for both internal and external oversight mechanisms. These include the judicial, legislative and executive branches of government.
- More specifically, the designated RICA judge is mandated to furnish the responsible Parliamentary Committee – which is the Joint Standing Committee on Intelligence (JSCI) – with an annual report. The JSCI, which oversees both the functions and the reviews of the intelligence services, is then also mandated to release a public report on the application of RICA.
- The Office of the Inspector General of Intelligence (OIGI) – a position created by the ISOA – is charged with monitoring the civilian intelligence services and ensuring compliance with the Constitution, laws and policies as well as investigating complaints about the intelligence services. He/she is selected by and reports to, Parliament, although is ultimately appointed by the President and is administratively accountable to the Minister of State Security.
- RICA requires that the Office of Interception Centres (OICs) which carry out communications surveillance, reports to the Minister of State Security as well as the JSCI.

Oversight

Oversight refers to the various ways of holding the intelligence services accountable before the public and the government. For example: internal oversight by the responsible minister, parliamentary oversight, judicial oversight and external independent oversight. 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.

WHAT'S THE PROBLEM?

- Even though there are oversight mechanisms in the laws, they are generally weak, too secretive and subject to abuse. There is a lack of both operational and political independence as well as transparency and this leaves the public largely in the dark when it comes to exercising democratic oversight and accountability.
- All of the oversight bodies are, in one way or another, tied to the state itself and thus also to the dominant/ruling party of the day. This makes them susceptible to personal as well as political pressure and manipulation.
- Two prime examples are:

  a) There is no independent oversight body that can check and review the decisions and reports of a RICA judge. The designated oversight body – the JSCI – generally holds hearings and discussions without public access/participation and often releases highly selective and redacted reports and information that provide insufficient information for the public to understand for example, why during 2009-2010, there was a huge 231% increase in the number of interception directions granted by the designated judge to SAPS's crime intelligence division.

  b) Both the OIC and the OIGI are administratively accountable to the very Ministry (State Security) that is ultimately responsible for communications surveillance and which generally operates in a state of secrecy. Further, they are functionally accountable to a JSCI which is controlled by members of the same political party as that of the State Security Minister and which also operates in a climate of generalised secrecy.
- There is no central and independent oversight body related to public disclosures of statistics on the collection and use of meta-data which has become a large part of the 'world' of communications surveillance. As a result, individuals as well as the public in general have no means to determine the reliability or practical effectiveness of the people and bodies legally responsible for oversight.

KEYWORDS: Secretive; Unaccountable; Non-independent

TRANSPARENCY

WHAT DOES THE LAW SAY?

- RICA explicitly prohibits the public disclosure of any information on the demands – issued under the Act – for lawful interception of communications and meta-data. While the JSCI is mandated by RICA to release public reports on the application of RICA, there are no specific requirements laid out in terms of what those reports should contain.

WHAT'S THE PROBLEM?

- Ensures that there is insufficient transparency and democratic accountability in specific relation to how RICA is applied and whether it is actually achieving its stated goal/purpose. For example, because telecommunications companies are barred from publishing information, including aggregated statistics, both of interception of communications and of meta-data, there is simply no way for the public to know how the law is being implemented.
- Allows for very limited information to be released as part of the public reports from the JSCI, most of which is in the form of generalised statistics on the number of interception orders granted. As such, the only publicly available information on RICA implementation contains nothing on, for example: the number of individuals whose communications are subject to interception; the reasons these interceptions are carried out; or, the outcome and effectiveness they may have in preventing or investigating crimes.
- Formalises a secretive approach to the workings of government surveillance of communications. Unlike many foreign-based social media companies, the South African state does not even attempt to provide 'transparency' reports nor does RICA itself require South African telecommunications companies to issue such reports. The result is a circle of secrecy around communications surveillance.

KEYWORDS: Non-transparent; Unaccountable; Misleading

Due process

This is a fundamental principle of fairness in all legal matters, both civil and criminal, especially in the courts. All legal procedures set by statute and court practice, including notice of rights, must be followed for each individual so that no prejudicial or unequal treatment will result. In the specific case of South African law, there are three parts of the 'Bill of Rights' in the Constitution that speak directly to due process:

a) that "everyone is equal before the law and has the right to equal protection and benefit of the law";

b) that "everyone has the right to freedom and security of the person, which includes the right not to be deprived of freedom arbitrarily or without just cause [and] not to be detained without trial"; and

c) that "everyone has the right to administrative action that is lawful, reasonable and procedurally fair".

DUE PROCESS

WHAT DOES THE LAW SAY?

- Cumulatively the laws that deal with communications surveillance set out a formal body of law that is available to the public. In different ways, these laws provide the government with formal, legal sanction to interfere with the human rights of citizens when such interference meets particular standards, rules or 'common good ' (e.g., 'national security').
- One key example involves decryption RICA allows for a designated judge to issue a decryption order which may include requiring (telecommunications companies) the decryption key or providing decryption assistance (defined as the assistance which is necessary to obtain access or to put the encrypted information in an intelligible form.) On the other side of the 'due process' coin, ECTA creates a regulatory framework for cryptography products and services used and provides for the establishment

Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

and maintenance of a Cryptography Provider Register by the Department of Communications.

- Another key example is that ECTA allows for Department of Communications-chosen "cyber-inspectors" (upon the issuing of a warrant by "any judge") to "enter any premises or access an information system that has a bearing on an investigation … at any reasonable time [and] without prior notice …"
- Further, according to ECTA, the Minister of Communications can "declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data". Such "critical data" is then subject to registration with terms of access set by the Minister, the violation of which can be a criminal offence.

WHAT'S THE PROBLEM?

- Despite all the relevant laws being publicly available, the sections that impact on due process are, for the ordinary citizen, often complex and difficult to find. For those who do not have easy access to legal help, the application of the laws governing communications surveillance can become a one-way street in which due process is practically impossible.
- More specifically, decryption orders (as under RICA) threaten the right to privacy since they are particularly invasive of the privacy of individuals' digital communications. This is made worse because RICA does not require a designated judge to publish information of decryption requests that, for example, outline the number of applications, approvals and disapprovals.
- Further, the broader goals/standards (such as 'national security' or the "economic and social well-being of citizens") for legally justifying decryption orders and the search and seizure of databases are clearly too vague and give excessive discretionary powers to the relevant government leaders/authorities. This is especially the case when failure to cooperate and comply with the respective 'order' is considered a criminal offence. The potential for abuse – and thus also of the violation of due process – is not only obvious, it is extremely high.

KEYWORDS: Unfair; Abuse; Arbitrary

25 Tambach Road, Sunninghill, Sandton: address of the Office of Interception Centres (OIC). Pic: Google Maps

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS

WHAT DOES THE LAW SAY?

- RICA establishes the Office of Interception Centre (OIC) as the only entity that is legally allowed to intercept communications. There is no other law that provides for any other legal interception entity.
- Overall operational and managerial responsibility for the OIC rests with the Minister of State Security. This includes appointing the Director of the OIC who is accountable to the Minister and who must take responsibility for all the functions and workings of the OIC, including record-keeping and the provision of any reports to other arms of government.
- Allows for "any law enforcement officer' to intercept "any communication" (without going to a designated judge) if he/she "is satisfied that there are reasonable grounds to believe that a party to the communication has caused, or may cause the infliction of serious bodily harm to another person … or him/herself" and if "he or she is of the opinion that because of the urgency…it is not reasonably practicable to make an application".

WHAT'S THE PROBLEM?

- There is no specific legislation (outside what little RICA provides) that criminalises illegal communications surveillance by both the public and private sectors.
- Leaves the fox guarding the chicken coop. The OIC (as the only legal government interception entity) falls under the direct operational control of the very Ministry (SSA) that conducts and/or oversees the vast majority of communications surveillance in South Africa. Since SSA has shown itself to be actively opposed to strict legal and procedural oversight and public accountability as well as more than willing to engage in illegitimate surveillance, the law is simply inadequate to safeguard against illegitimate access by the entity it sets up for that very purpose.
- The law does not cover the National Communications Centre (NCC) which is housed within the SSA and involved in mass and targeted surveillance of both foreign and domestic signals *(see explanations – both of mass versus targeted surveillance as well as foreign signals intelligence)* on behalf of intelligence and security services. Given that the NCC has the capacity to conduct mass monitoring of telecommunications across a wide range of platforms without judicial authorisations or other safeguards, the NCC is effectively an unregulated, extra-legal interception institution existing outside the law that governs communications surveillance.

Foreign Signals Intelligence

According to the General Intelligence Laws Amendment Bill, this term means: "intelligence derived from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals, and includes any communication that emanates from outside the borders of the Republic, or passes through or ends in the Republic" [Section 1(c) of GILAB].

- The lack of specific legal measures to prohibit and criminalise illegitimate access carried out by the government or private service providers, leaves users completely vulnerable to gross interference with their right to privacy as well as lacking in avenues of legal and procedural redress that must be justified in accordance with international human rights law.

KEYWORDS: Conflict of Interest; Illegal; Criminalisation

SAFEGUARDS FOR INTERNATIONAL COOPERATION

WHAT DOES THE LAW SAY?

- Although the South African government has signed numerous multi-lateral International Treaties as well as 'Mutual Legal Assistance treaties' with various countries, some of which most likely contain provisions related to human rights and international communications surveillance, none of the communication/information laws in South Africa explicitly make reference to such Treaties in respect of their content or applicability.
- RICA simply states that any communications interception or information request (related to organised crime or terrorism) from or provision to, "the competent authorities of a country or territory outside the Republic", must be "in accordance with an international mutual assistance agreement".

WHAT'S THE PROBLEM?

- There is presently no law that explicitly addresses and provides for, adequate safeguards related to the interception of communications that are 'extra-territorial' (i.e. communications that emanate from outside the borders of South Africa, or that pass through or end in South Africa). The present situation is one in which, practically and legally, users are left defenceless against such surveillance; and their right to privacy as well as recourse to the legal system, can be violated at will.
- The unregulated and unmonitored NCC – and thus also the SSA – has been effectively given *carte blanche* to do as it pleases. This gives the SSA complete and arguably unconstitutional discretion and power to engage in 'extra territorial' surveillance outside of the law and opens the door to wide scale and politicised abuse in the name of 'national security' and self-constructed notions of South Africa's "intelligence priorities".
- Given that large amounts of electronic communications traffic emanate from outside the country, especially when it comes to the work of political and social activists as well as investigative journalists, the present situation virtually ensures that such communications can and will be targeted for surveillance.

Question 2: What is required of the South African government, specifically in terms of amending RICA, to respect and protect human rights when conducting communication surveillance and in order to match 'The Principles'?

Specific amendments to RICA

Re-definition of key terms

- The term "national security" must be tightly defined and centred on respect for and protection of, constitutional rights so that the Act is not open to politicised manipulation and arbitrary abuse by the securocrats and/or ruling elite.
- The definition of "interception" should be amended to clarify that it covers any measure to collect, control, monitor or take custody of both communications content and meta-data, of both targeted and mass communications surveillance *(see explanation)*.

User notification

- People whose communications have been intercepted must be informed after the completion of investigations, or if the designated judge refuses to grant an interception direction.
- A user-notification provision needs to be included. 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.

Mass surveillance

The practice of mass surveillance should be expressly prohibited and criminalised.

Transparency on surveillance:

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.

Data retention

Replace the present blanket and untargeted data retention approach with targeted data interception and/or data preservation orders

Data retention periods:

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."

SIM card registration

Mandatory SIM card registration should be scrapped.

Interception directions

Tighten the grounds for the issuing of interception directions to a "high degree of probability" rather than "reasonable grounds to believe", as is presently the case.

Regulation of the National Communications Centre (NCC)

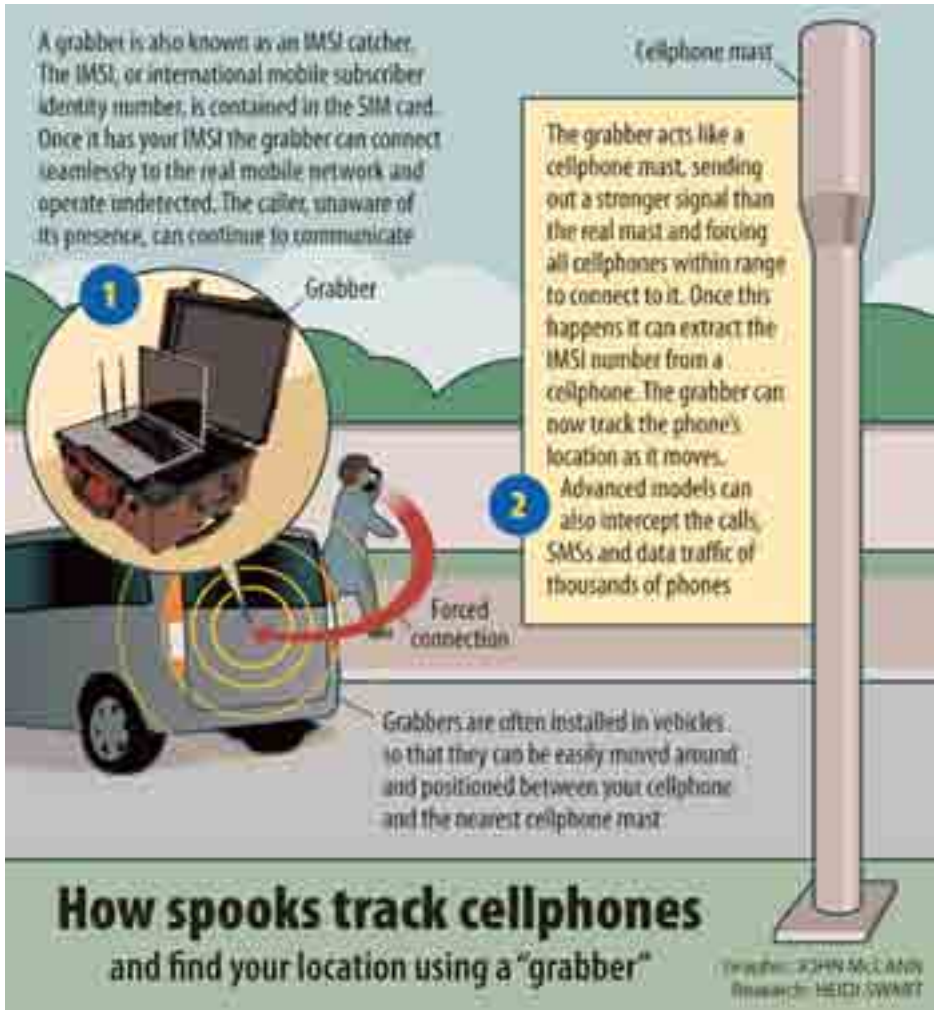
The NCC must be specifically covered by new regulations in RICA. The regulatory content should take on board the recommendations of the Matthews Commission and be informed by white and green paper processes of Parliament.

Regulation of foreign signals intelligence (see explanation)

Foreign signals intelligence should be covered by new regulations in RICA that provide clarity on the scope and character of such surveillance and place sole authority to carry out this kind of surveillance with the OIC.

Regulation of cell phone tracking technology

In the USA, legislation regulating the use of this technology, specifically, has recently come into effect in Washington State 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 cell phone-tracking devices (such as the grabber) in criminal investigations and inform judges when they plan to use them.



Regulation of grabber technology

There should be regulatory clauses added to RICA that set out specific and strict conditions/rules for the purchase, sale and use/deployment of grabber technology.

Transparency reports by service providers

Include new clauses that both require and enable telecommunications or internet service providers to publish aggregate information on surveillance/information orders they receive. These transparency reports must be

publicly available while more detailed and confidential information should be made available to oversight bodies such as Parliament, the Judiciary, and a specialised (non-parliamentary) independent commission.

Creation of a Special Public Advocate/Ombudsman

A new position should be created in RICA for a Special Public Advocate/Ombudsman to represent users and the public interest when applications for interception directions are made. An independent advocacy role focusing on the process of issuing interception directives will go a long way in ensuring due process is followed.

Alternatively, if the establishment of a Public Advocate/Ombudsman cannot be achieved, then another option is to strengthen independent oversight by appointing 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.

Accountability and oversight mechanisms

Annual transparency report from designated RICA judge

Either through an amendment to the Intelligence Services Oversight Act (ISOA) or through a directive of Parliament, the designated RICA judge should be required to provide an annual report which, at the very least, must include the following:

- Number of interception directions granted
- The offences for which orders were granted
- The average costs per order
- How many and which interception directions resulted in arrests and convictions as well as base information about arrests and convictions.
- The types of surveillance used
- Number of each type of interception request, broken down by type of information, legal authority and requesting state actor of whatever origin
- Number of interception requests under emergency procedures

- Number and types of responses provided to requests, including the number of requests rejected
- Number of users and accounts targeted as well as those affected
- Number of times delays in notification were requested, granted and extended
- The compliance rate, provided as a percentage of total requests received and complied with
- The legal challenge rate, provided as a percentage of total requests received and challenged
- Number of investigations into complaints filed, the results and the remedies ordered and/or actions taken in response to any investigations.

Disclosure of surveillance activities

In the shorter-term, pending legislative reform, the various arms of government but more especially the SSA, must publicly disclose details – in line with 'The Principles' – of the scope and scale of surveillance activities carried out by the state. In particular, this must include full information about the deployment and use of as well as relevant laws pertaining to, grabber technology.

Government relationship with VAStech

With immediate effect, the government must fully explain to the South African public the nature, scope and character of its relationship with VAStech and more specifically, how public money has been and/or continues to be, used to finance its manufacturing of surveillance technologies. Going forward, if

VASTech

"VASTech (Pty) Ltd is an independent South African company, created in 1999, with international subsidiaries in the Middle East and Europe.

We offer sophisticated hardware and software telecommunications solutions to national governments and the law enforcement community, that are not under any sanctions, in the fight against cross-border and international crime."

http://vastech.co.za/about

the proposed amendment to RICA outlawing mass surveillance is adopted then this relationship, as well as VAStech, will thankfully become redundant given that VAStech's specialty is the manufacture of mass surveillance equipment.

Public Hearings on Intelligence Sharing Agreements

As soon as possible, Parliament should conduct public hearings on any past and ongoing intelligence sharing agreements with foreign countries (using the present Parliamentary Inquiry in Germany as a 'best practice' reference – *(see inset)*. Not only will such hearings strengthen public oversight and accountability but will also assist in ongoing efforts to bring current South African legislation on communication surveillance in line with 'The Principles'.

Public Oversight:

The Germany federal system consists of internal control, parliamentary oversight, independent oversight, and a complaint procedure before an independent body. For instance, only a Federal Minister or the highest authority can order surveillance measures. The minister is required to provide the independent Commission every month with an account of the measures he/she has ordered, before such measures are actually implemented. Except in urgent cases, the minister must obtain prior approval of the Commission. Furthermore, an official qualified for judicial office supervises the implementation of the measures ordered. The Parliamentary Supervisory Board performs after-the-fact oversight. The minister has to report to the Board on the applications to the Commission at least once every six months.

Question 3: What should civil society in South Africa do to strengthen and expand the struggle for a more human rights-centred and democratically controlled communications surveillance regime?

Form an internet rights and surveillance coalition

A coalition of existing organisations around internet rights and surveillance should be formed. Instead of reinventing the wheel, organisations such as the Right2Know Campaign (R2K), Media Monitoring Africa (MMA), the Freedom of Expression Institute (FXI) and the Support Public Broadcasting Coalition (SOS) can begin exploratory discussions on rolling out a collaborative anti-surveillance project. The organisations can then rope in other players in the private sector, academia, journalists, trade unionists and community activists interested in and affected by, communications surveillance issues.

The coalition should advocate for the specific reform of RICA and ISOA as outlined above as well as conscientise the general public on the violations of the right to privacy, due process and freedom of expression (amongst others) associated with communications surveillance in South Africa. Further, the coalition can also focus on training its constituencies on various tools available which enable them to protect their privacy and practically circumvent the dangers of mass surveillance.

Baseline surveillance research

Qualitative baseline research should be conducted to ascertain the prevalence of surveillance amongst key constituencies like student activists, trade unionists, human rights/public interest 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 communications surveillance in South Africa. Research findings should be released publicly to build public awareness of the extent of communications surveillance.

Consistent monitoring and Pressure on JSCI

Monitoring of the public reports by the National Assembly's Joint Standing Committee on Intelligence (JSCI) 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.

SOURCES

Access, 2013

Bakir, 2015

Brown, 2013

Constitution of the Republic of South Africa, 1996

Donovan & Martin, 2014

Duncan, 2014 & 2015

Electronic Frontier Foundation, 2015

La Rue, 2013

Lyon, 2014

Mail & Guardian, 2013

Matthews Commission, 2013

Ministerial Review Commission on Intelligence (Mathews Commission Report), 2008

Nathan, 2012

Ni Loideain, 2015

OHCHR, 2014

Privacy International, 2015

Right2Know Campaign, 2013, 2014 & 2015

Sunday Times, 2014

Swart, 2015

UN General Assembly, 2013/2014

University of Amsterdam, 2015

Young, 2004

https://es.necessaryandproportionate.org

http://www.htxt.co.za/2014/06/06/sa-phone-companies-may-be-used-for-spying-but-cant-tell-you-when/

USEFUL CONTACTS

Centre for Applied Legal Studies (CALS)

DJ du Plessis Building, West Campus Wits University, Braamfontein, Johannesburg

Tel: 011-7178600; Fax: 011-7171702; Email: gina.snyman@wits.ac.za

Freedom of Expression Institute (FXI)

1st Floor, Richmond Forum Building, 18 Cedar Avenue, Richmond, Johannesburg

Tel: 011-4821913; Fax: 011-4821906; E-mail: fxi@fxi.org.za

ProBono.Org

1 Kotze Street, Old Women's Jail, West Wing Constitution Hill, Braamfontein, Johannesburg

Tel: 011-3396080; Fax: 011-3396077; Email: erica@probono.org.za

Right2Know Campaign

1st Floor Community House, 41 Salt River Road, Slat River, Cape Town

Tel: 021-4471000; Fax: 0865518879; Email: admin@r2k.org.za

Socio-Economic Rights Institute of South Africa (SERI)

6th Floor, Aspern House, 54, De Korte Street, Braamfontein, Johannesburg

Tel: 011-3565860; Fax: 011-3395950; Email: sanele@seri-sa.org