
STOP THE SURVEILLANCE!
ACTIVIST GUIDE TO RICA & STATE SURVEILLANCE IN SA
RIGHT2KNOW

Find this report online at r2k.org.za
#StopTheSpies

@r2kcampaign
fb.com/right2know

This handbook was produced by the Right2Know Campaign, drawing on research by the Media Policy & Democracy Project and Right2Know's ongoing activism against 'securitisation'.

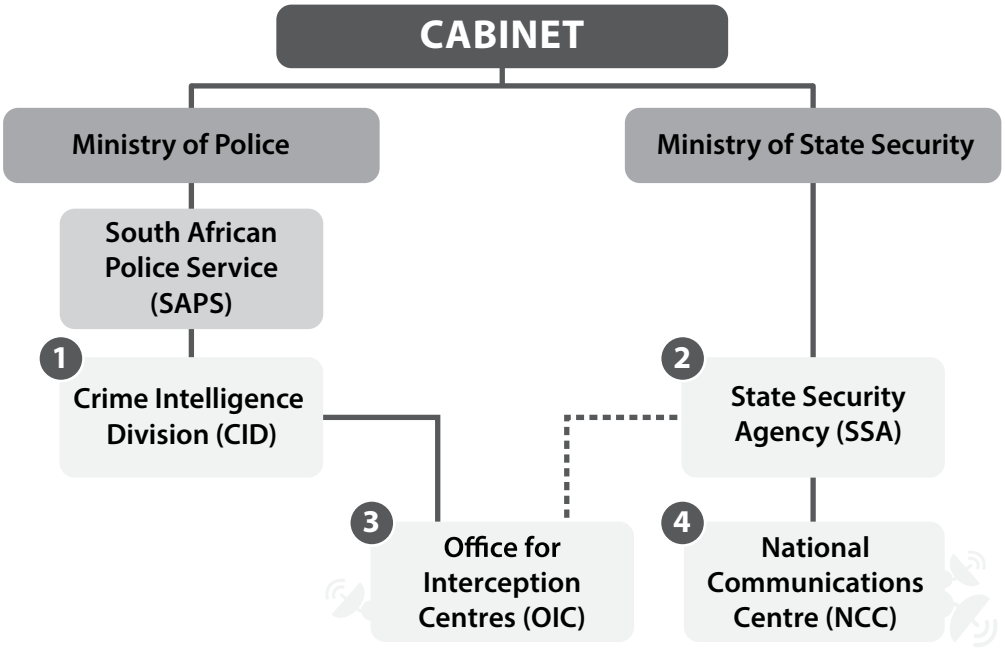
CONTACT US

R2K National: 021 447 1000 | admin@r2k.org.za
R2K Gauteng: 011 339 1533 | gauteng@r2k.org.za
R2K KZN: 031 301 0914 | kzn@r2k.org.za
R2K Western Cape: 021 447 1000 | westerncape@r2k.org.za

Contents

South Africa's intelligence agencies

Intelligence agency: *a government structure that collects, analyses and uses information in support of law enforcement, national security, and foreign policy objectives – usually in secret.*



1 **The Crime Intelligence Division (CID)** is part of the South African Police Service, and falls under the Minister of Police. CID is mainly responsible for supplying intelligence in support of policing, such as organised crime, but also in monitoring potential violence in protests. CID may use communications surveillence as part of its operatons, and relies on the OIC (and possibly the NCC) for support.

2 **The State Security Agency (SSA)** is government's primary intelligence agency. It is responsible for identifying and monitoring a wide range of threats to national security and stability in South Africa. It falls under the Minister of State Security.

The SSA also oversees the surveillance facilities used by all intelligence agencies: the Office for Interception Centres (OIC) and the National Communications Centre (NCC).

3 The **Office for Interception Centres (OIC)** was established in terms of RICA and falls under the Ministry of State Security. The OIC helps the South African government to intercept communications. **See pg 15.**

4 The **National Communication Centre (NCC)** is another surveillance facility that reportedly conducts mass surveillance for the South African government. It falls under the Ministry of State Security. There are serious concerns that its powers may be unlawful and are not properly regulated through RICA. **See pg 15.**

Other intelligence structures include the **Defence Intelligence Division**, which falls under the SA National Defence Force, and the National Intelligence Co-Ordinating Committee (NICOC), which is a joint platform where all SA intelligence agencies share information and coordinate activities.

01 Introduction

What is this booklet about?

Nearly everyone in South Africa knows about a law called "RICA". This is the law that says everyone who buys a SIM card must register their identity to the SIM card: meaning that all of your communications are linked to your identity.

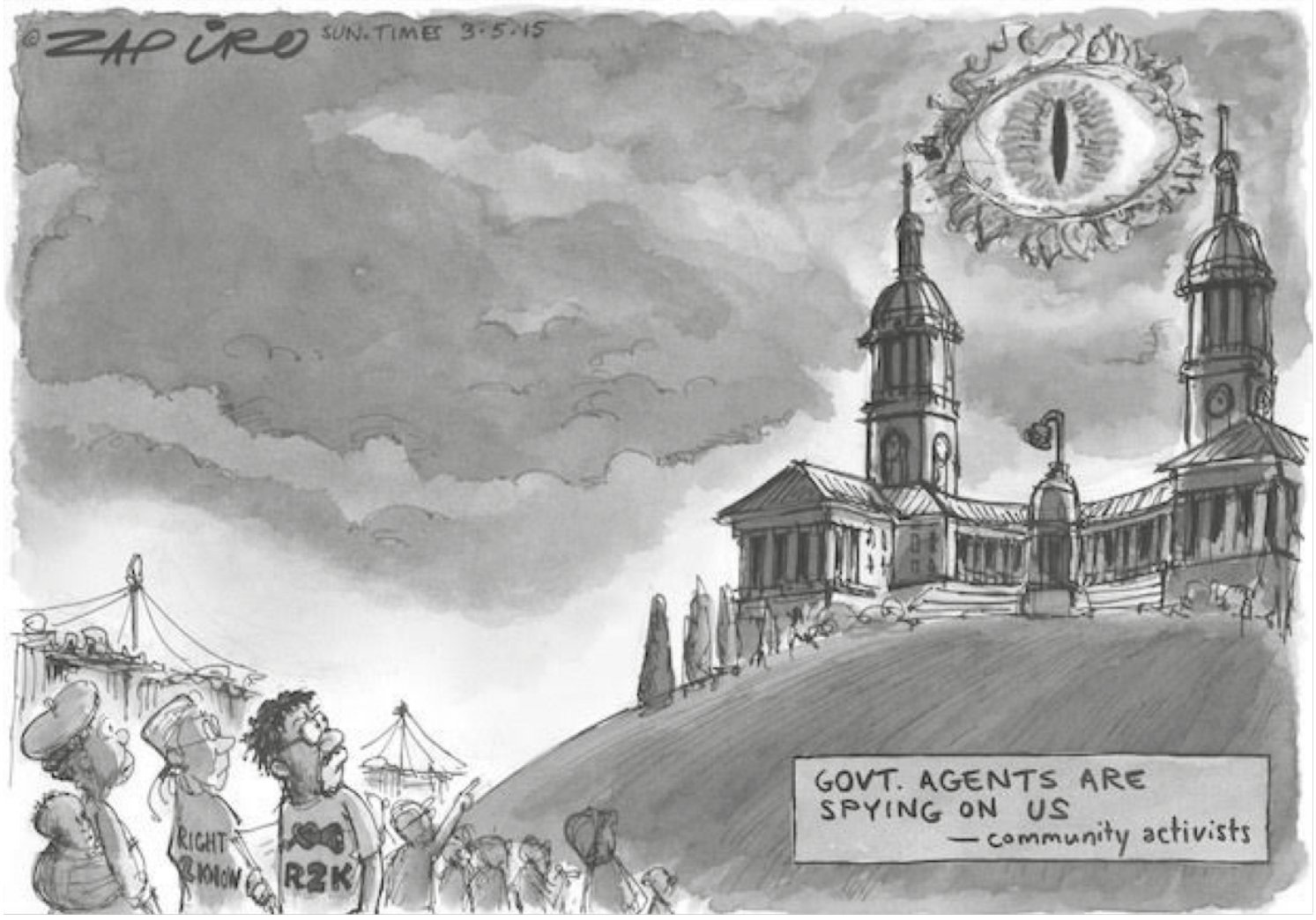
In fact, RICA is South Africa's main **surveillance** law: it is the rulebook that says how and when the South African government can intercept your private communications: your calls, messages, emails, and internet activity. This is what we sometimes call "bugging" or "tapping" of your communications.

Privacy is a basic human right enshrined in section 14 of South Africa's constitution. In South Africa, just like all over the world, there are growing concerns that the government's surveillance capacity – its ability to listen in on people's private communications or gather information on their activities – is being abused. There is evidence in South Africa that surveillance is used to target journalists, political activists, unionists, and to interfere in our politics and public life. There are also broader concerns that this affects not only a few individuals, but millions of ordinary people in South Africa who use communication every day.

This is not only a South African problem; it is a concern around the world. Advancements in technology have brought together many different kinds of communications (calls, e-mails, web searches, online chats, social media) to one device that is both mobile and connected to the internet.

Across the world, communication surveillance is a common tool of repression. Those with power and wealth are afraid of ordinary people, especially when the people are struggling for political freedom and socio-economic justice.

The purpose of this booklet is to unpack some of these issues in a South African context, in order to understand the problems we face and strengthen anti-surveillance activism. Because at the end of the day:- *it's about your rights*!


©ZAPIRO SUN.TIMES 3-5-15
RIGHT TO KNOW
R2K
GOVT. AGENTS ARE SPYING ON US
— community activists

R2K's Pupa Fumba holds the 'spy tapes' at Camp-out at Parliament, 2012

02 Understanding South Africa's surveillance problem

Why should we be worried?

In 2015, the Right2Know Campaign published the stories of activists who have been harassed and monitored by South Africa's security structures, in a handbook called Big Brother Exposed. It showed that some actors in government (and possibly the private sector) are openly monitoring certain activists and organisations, especially those who are engaged in regular protest.

In particular the Crime Intelligence division of the police has taken on a mandate to supply "intelligence" on protest for the Public Order Policing units. Some of these cases have been lodged as complaints to the Inspector General of Intelligence, but none of these have led to prosecution. (The report is available at www.bigbrother.r2k.org.za.)

At the same time, **others have clear evidence that their communications have been illegally intercepted by the state.**

- In 2012 it emerged that the SAPS Crime Intelligence Division (CID) had fraudulently spied on the communications of two Sunday Times investigative journalists, Mzilikazi wa Afrika and Stephan Hofstatter (see pg 17).
- In 2015, it emerged that government agents had spied on the communications of amaBhungane journalist Sam Sole while he was reporting on the corruption investigation of Jacob Zuma. (see page 19)
- Paul Scheepers, a former Crime Intelligence official, is facing charges in a Bellville court of fraudulently using magistrates' warrants to spy on the phone records of senior lawyers and police officers (see pg 18).
- Mpumalanga investigative journalist Tom Nkosi complained that he was under surveillance after Premier David Mabuza boasted that he was receiving intelligence briefings on the movements of Nkosi and other investigative journalists.
- In 2015 the public learned of the existenc of 'Grabber' devices, a portable mass surveillance technology that imitates a cell phone tower in order to 'grab' information from nearby mobile phones (seee pg 18).

So why are these incidents happening?

South Africa's privacy problem in context

In the 1990s, South Africa's new constitution enshrined fundamental human rights, including the right to privacy, and set up a new framework to dismantle the apartheid-era intelligence agencies and create security structures that respect human rights and are accountable.

Yet in the post democratic era, South Africa has continued to be plagued by inequality, crime, social conflict, and political interference in democratic institutions. Among other abuses, this has been fertile ground for the abuse of communications surveillance for the state and

Read more

Big Brother Exposed – testimonies of state surveillance of activists and unionists in South Africa.

bigbrother.r2k.org.za

private sector to push for greater surveillance powers (through existing and new laws) and to use communications surveillance against those who are perceived as political 'threats', competitors for economic power and whistleblowers who expose wrongdoing.

Though surveillance issues have not got much attention in the post-94 South Africa, there have been warning signs for years: such as the Matthews Commission.

The Matthews Commission

In the 2000s, following a series of 'spy' scandals, the former Minister of Intelligence Ronnie Kasrils set up an official inquiry into whether the activities of South Africa's main intelligence structures were in line with the constitution. It was headed by Joe Matthews, an MK veteran. The findings of the Matthews Commission report, which became public in 2008, include:

- Evidence of surveillances abuses and spies taking an inappropriate interest in "lawful political and social activities".
- Lack of transparency and not enough institutional independence in the oversight systems, including the Inspector General of Intelligence and Parliament's intelligence committee.
- The Matthews Commission also revealed that the state has mass surveillance capabilities through the National Communications Centre (**see pg 15**), which now falls under the State Security Agency (SSA). The Commission found that the NCC's conduct is not regulated by any law, and that such surveillance is illegal and unconstitutional.

The Commission's findings told the public a lot about the state of surveillance in South Africa, and continue to guide activism on surveillance today. Unfortunately, the state has refused to engage with the Matthews Commission report at all, because the report was leaked to the public before being tabled in Cabinet – and then, after Mbeki was recalled as President, it was never tabled in Cabinet. Therefore, government officials simpy say the document as "no status".

The report is available at r2k.org.za/matthews-commission!

What did we learn from Snowden?

Edward Snowden is a whistleblower who worked with the United States' National Security Agency (NSA). In 2013, after growing disillusioned with the NSA's surveillance programmes, Snowden took information to the media to expose how the US government and its allies spy on the communications of hundreds of millions of people across the world. His actions taught us important lessons, including:

- New communication technology has made it easier than ever to conduct mass surveillance, on a scale we have never seen before.
- Widespread, untargeted surveillance efforts by one government can violate millions of people in other countries: **so we can't only focus on the local conditions.**
- Surveillance programmes designed for one use (e.g. identifying terrorists) are inevitably extended to other uses (e.g. spying on trade negotiations or profiling activists): **so we can't just 'trust' that powers won't be abused.**
- The private sector often plays a big role in helping governments' surveillance programmes: **so we can't only focus on the state.**
- Our modern communication services generate huge amounts of information about us and our lives, creating major legal and technical challenges to protecting our privacy: **so we need new solutions.**
- Secret intelligence sharing agreements allow governments to share information with each other from their surveillance programmes, and help governments to 'get around' legal restrictions in their own country by relying on information from another government's surveillance programmes: **so we *really* can't only focus on local conditions.**

Snowden's revelations led to some reform of communications laws (in line with the "Necessary and Proportionate" principles: see page 14. In other cases, governments have passed or are considering new laws that give further powers to security agencies to spy on people's communications. ■

International spying on local human rights groups

One of South Africa's oldest public interest law centres, the Legal Resources Centre (LRC), discovered in 2015 that the UK government intelligence agency, GCHQ, had intercepted their emails, as well as those of Amnesty International. Although the details and motives are unclear, it is a chilling reminder of the globalised nature of surveillance.

03 How does communications surveillance work?

Let's unpack some basic concepts

Phone-tapping. Bugging. Spying. These are all words we use when talking about **communications surveillance**. Communications surveillance is the use of surveillance technology to monitor, intercept, collect, and store information that has been communicated over a network. This could refer to a mobile telephone conversation, text message, email, landline call, or the activities of a person browsing the internet. This handbook focuses on government surveillance, and some of the companies that assist, but in the broader sense, users' privacy could also be infringed by private companies or people.

Why is communications surveillance a problem?

Privacy is a basic right. Communicating is part of what makes us human, and thus communications surveillance is a serious violation of this fundamental need to communicate. People behave differently when they know they are being watched, which can lead to self-censorship or a hesitancy to engage in society. Without the security of knowing that our communications are private, our ability to create safe boundaries and manage our relationships falls apart.

What is 'meta-data'?

Often people think 'communications surveillance' is just when someone secretly reads the contents of a private message or listens in on a private phone call. But a lot of surveillance is focused on collecting meta-data, which is information about a communication, rather than the actual content of the communication. Meta-data includes information such as the identity of the sender and recipient of information, and their locations, the time of the communication, the type of device and network they are using, and many other details. This type of information is more sensitive than many people think: meta-data can be stored for years and analysed to reveal very detailed information about a person's relationships, personal life, beliefs and activities.

What is 'mass surveillance'?

Targeted surveillance is directed at specific people who have been identified as targets. For example, it could involve the tapping of a specific person's phone or analysing a specific person's meta-data. **Mass** surveillance is the much broader, indiscriminate monitoring of a whole population or section of society. Mass surveillance includes any system that collects or stores information about a group of people or users without focusing on well-defined targets (such as a specific person who is under reasonable suspicion of committing a serious crime). In South Africa, one example of mass surveillance is the fact that RICA requires telecommunications companies to store the call records and other meta-data of its users for up to five years.

There are many kinds of surveillance abuses, but mass surveillance is the biggest proble, because it affects many people at once, and because by definition, mass surveillance is not designed to limit how it infringes on people's right to privacy. Any legitimate infringement of a right must be as limited as possible. ■

Read more on how surveillance works:

Privacy International's "Privacy 101" Explainers
https://www.privacyinternational.org/?q=privacy-101

R2Kers launch the Demands to End RICA abuses, Parliament 2016

04 What's wrong with RICA?

What's in South Africa's main communication law – and what's missing?

We all know about the law called RICA because it requires us to register our SIM card to our identity, as well as any landline or internet account that we open. But RICA is actually the most important law when it comes to communications surveillance in South Africa, with much wider provisions. So what does it say?

The stated aim of RICA is to regulate how and when government agencies can intercept a person's communications, as a means to combat serious crime and threats to national security. This could include interception of the content of communications (e.g. what is said in a phone call, text, email) or the meta-data (e.g. who communicates with who, where, when, etc). To make things more confusing, meta-data is called 'communication-related information' in the Act!

When can government agencies intercept communications?

RICA says nobody except law enforcement agencies can intercept your communications without your permission. According to RICA, generally law

enforcement agencies can only intercept a person's communications if they have authorisation of a specific 'designated' judge. For the 'content' of communications or real-time interceptions, they must go to a special judge in the Department of Justice, often called the 'RICA judge'. But for meta-data that is older than 90 days, law enforcement agencies can go to any High Court judge or magistrate.

Such permission can only be granted if police or state-security officials can show reasonable grounds that a "serious offence" has been, is being or will probably be committed, that there is an actual or potential threat to public safety or national security, or for "compelling national economic interests".

If granted, the judge issues the agency with a warrant called an "interception direction". This warrant forces any telecommunications company or internet service provider to help the agency intercept the communication of the user or users. According to RICA, the interception and handover of data is done from the Office for Interception Centres (OIC).

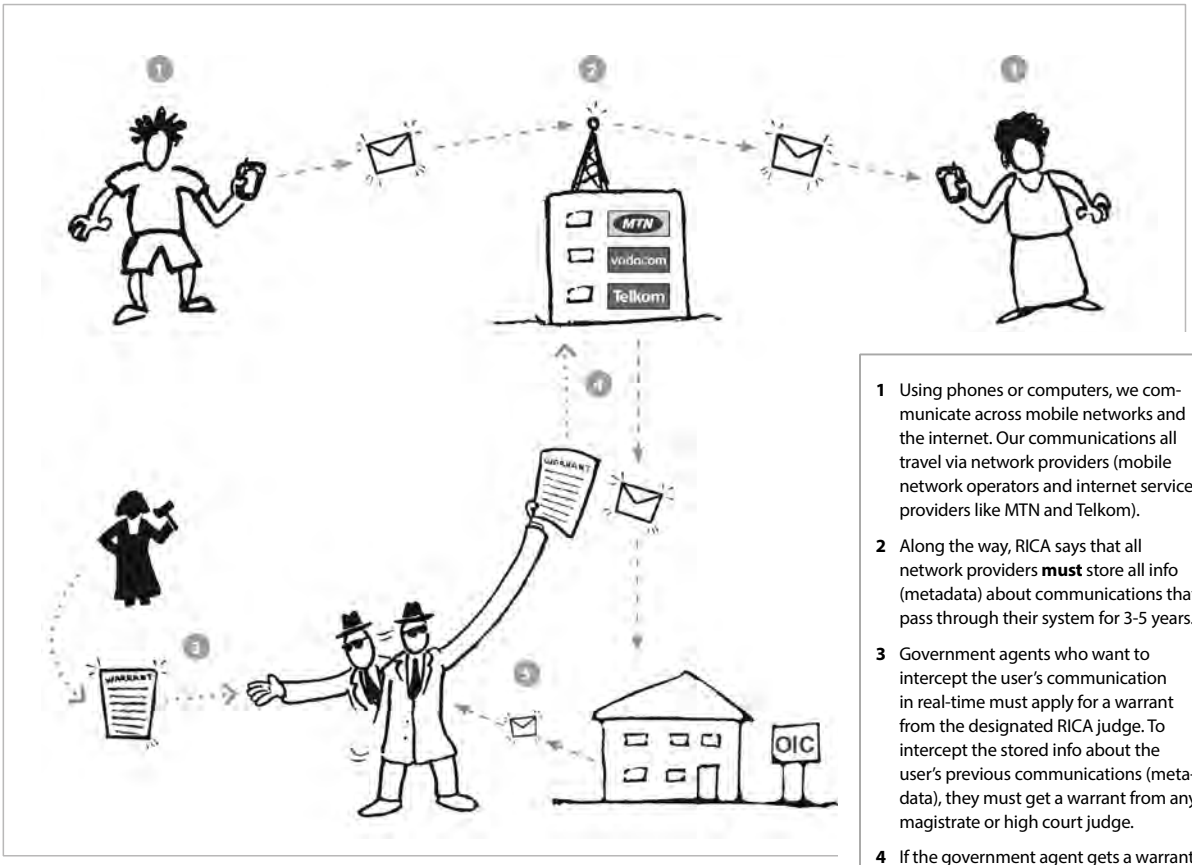
What are some of the problems?

No transparency

RICA surveillance has no transparency built into the system. The law does not provide for a person to be notified after a warrant has been issued to intercept their data, meaning that people have no way of knowing if they've been put under surveillance and their rights violated.

It is not uncommon for governments to notify users after intercepting their communications – it is called 'user notification', and is required by law in the USA, Germany, Austria, Japan, South Korea, Taiwan, Chile, Czech Republic.

RICA has a secrecy provision that has gagged network operators and internet service providers from telling their users when their communications have been intercepted, or even telling the public how many warrants it receives each year. (Vodacom's global parent company, Vodaphone does a transparency report to reveal how many times it had helped governments spy on its customers, South Africa was one of only six countries where no information could be given, by law.)



The RICA surveillance system (simplified)

1 Using phones or computers, we communicate across mobile networks and the internet. Our communications all travel via network providers (mobile network operators and internet service providers like MTN and Telkom).

2 Along the way, RICA says that all network providers **must** store all info (metadata) about communications that pass through their system for 3-5 years.

3 Government agents who want to intercept the user's communication in real-time must apply for a warrant from the designated RICA judge. To intercept the stored info about the user's previous communications (meta-data), they must get a warrant from any magistrate or high court judge.

4 If the government agent gets a warrant, the network provider **must** secretly hand over the user's communications in real-time, or the meta-data about previous communications. This reportedly happens via the Office of Interception Centres (OIC), which then transfers the information onwards **(5)**.

Communications providers are forced to store their customers' data for years

RICA makes it illegal to establish communications networks that are not capable of interception and forces network operators and internet service providers to help the state spy on their users. Worst of all, RICA states that these companies must store their users' meta-data for three to five years, in case a government agency wants to intercept the data at a later stage. This means that every single communications user in South Africa is already subject to mass, untargeted surveillance. This kind of data retention was struck down in the EU by the European Court of Justice because it led to a serious interference with fundamental rights.

SIM card registration violates privacy

SIM card registration (when users must register their SIM cards to their identity) may seem normal in South Africa, but many countries do *not require it*. Doing so violates privacy because it limits the ability of citizens to communicate anonymously. It also facilitates the tracking and monitoring of all users by law enforcement and intelligence agencies. We've seen research suggesting that SIM card registration is not a useful measure to combat criminal activity, but actually fuels the growth of identity-related crime and black markets to service those who want to stay anonymous, while subjecting everyone else to surveillance.

The judges' role must be strengthened!

Judges can authorise interception on grounds that have already been criticised for being vague and for allowing law enforcement officials to speculate. The fact that interception sensitive meta-data can be authorised by any magistrate or High Court judge (i.e. not the "Rica" judge) means this data is less protected than it should be. It is not known how many surveillance warrants are authorised at this level.

RICA has serious loopholes!

In 2015 and 2016, investigative journalism by Heidi Swart explored how state spies and law enforcement officials have 'got around' RICA, or exploited its loopholes, to spy on people's communications without safeguards. (Use the QR code to read some of the articles.)

RICA's biggest loophole is that it does not regulate the practice of 'bulk monitoring', a form of mass surveillance where intelligence agencies 'suck up' a wide range of information from communications networks, rather than targeting a particular individual, to analyse them for potential threats. The 2008 Matthews Commission found that the intelligence agencies were doing bulk monitoring through a facility called the National Communications Centre (NCC) without any legal oversight – the NCC continues to operate, apparently outside of the law. This is why R2K has demanded an END to mass surveillance.

The Office for Interception Centres (OIC)

Location: Johannesburg

Function: The OIC oversees the interception of communications in terms of RICA. When a network provider (mobile network operators and internet service providers like MTN and Telkom) gets a warrant from the RICA judge to intercept their customer's communication or data, they must route a copy of that communication or data to the OIC.

The National Communications Centre (NCC)

Location: Pretoria

Function: The NCC is actually not recognised in law, so its exact functions are not spelt out! But according to the Matthews Commission and investigative journalism, the NCC appears to be responsible for "bulk interception" and storage of communications - mass surveillance. The Matthews Commission found that the NCC's facilities were used to spy on at least 13 people illegally during a rogue intelligence operation linked to the Zuma-Mbeki leadership battle. Not only is the NCC operating outside of the law - R2K believes the NCC's mass surveillance activities should be shut down entirely!
Photo credits: Madelene Cronje, Mail&Guardian

Looking beyond RICA

International best practice: the "Necessary & Proportionate" Principles

In 2014, a group of international human rights organisations launched 13 international principles to design laws that protect against surveillance abuses. These are called the "Necessary and Proportionate" Principles. Any surveillance law should follow these principles - and laws, like RICA, which don't follow them should be reformed urgently. Find the principles at **necessaryandproportionate.org**

Trouble for internet freedom? SA's Cybercrimes Bill

The Cybercrimes and Cybersecurity Bill was tabled in Parliament in late 2016. The Bill 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. Though it has been revised after a public outcry (see r2k.org.za/cybercrimesbill), there are concerns that the Bill expands the state's interception powers in RICA, and puts the state security structures in charge of internet governance for South Africa. Despite criminalising acts such as the unlawful interception of and interference with data, there are a range of serious concerns that need to be dealt with at the time this handbook was produced.

A source of hope? SA's new data protection law

The Protection of Personal Information Act (POPI) is South Africa's data protection law, passed in 2013. It provides for the protection of personal information and regulates how information can or cannot be collected through electronic transactions or communications. POPI also establishes an Information Regulator (a kind of 'Public Protector' of your data). The Information Regulator, chaired by former IEC chair Pansy Tlakula, was only established at the end of 2016. It remains to be seen whether this body will be a fierce watchdog against surveillance. ■

Sunday Times journalists join R2K's anti-surveillance picket at the court

05 Stories of surveillance

Let's look at some key case studies of how RICA has been abused.

CASE STUDY *Sunday Times journalists bugged*

Mzilikazi wa Afrika and Stephan Hofstatter are investigative journalists at the Sunday Times. In 2010, when they were investigating major corruption scandals in the South African Police Service, the SAPS Crime Intelligence Division (CID) spied on their phone communication.

It has since emerged that officials got a warrant to monitor these phone numbers by lying to the RICA judge – they told the judge these phone numbers belonged to individuals who were part of a criminal syndicate that was under investigation.

Under RICA, it is an offence to supply false information to the RICA judge.

continued on p 17...

...continued from p 16

A single Crime Intelligence official, former Captain Bongani Cele, is now being prosecuted in the Pretoria commercial crimes court for misleading the judge. Though nobody else has been charged, there is evidence that other more senior officials were involved. Ironically, nobody has been prosecuted for actually ordering that journalists' phones be tapped.

As a result, a warrant was issued to collect Afrika and Hofstatter's meta-data – a record of who they called and exchanged messages with, and their locations.

This would be a serious violation of their rights as journalists and would potentially expose the identities of their sources.

At the time that this publication was printed, the trial was still going on. But the allegations are a clear reminder of some of the loopholes in RICA that R2K has complained about. Only through urgent reforms can we prevent these abuses from happening in the first place.

- The low threshold for issuing a warrant allows rogue cops to mislead judges when requesting a warrant, and it has also been reported that intelligence structures can intercept communications without getting a warrant.
- The fact that RICA forbids users from being notified when their communications are intercepted means that when these abuses happen, the victims have no way of ever finding out about them. (Afrika and Hofstatter were warned by sources that they had been bugged.)
- The fact that RICA requires everyone to register their identity to a SIM card makes it almost impossible for citizens to communicate anonymously. With mounting evidence of surveillance abuses, it is absolutely necessary for journalists for example to be able to speak to confidential sources without compromising their identity. ■

CASE STUDY *Crooks with Grabbers*

The 'Grabber' is a local nickname for a kind of technology that is also sometimes called an "IMSI Catcher" (pronounced 'Imzee'). These devices, which can be as small as a car battery, are capable of sucking up data from thousands of mobile phones in a radius of up to several kilometres, and identify each user by their SIM card. While they are acquired in secret for "national security" purposes, in other countries cops have been accused of using them to investigate petty crime and to identify participants at protests. In a number of countries, human rights groups have submitted complaints or legal challenges to their use.

In 2015, the public learned that these devices were available in South Africa after police arrested a group of individuals alleged to have been in possession of a privately owned grabber device. These men are now facing prosecution in the Pretoria Commercial Crimes Court.

Meanwhile, it has emerged that police and security agencies also possess and use these grabbers in utmost secrecy, raising serious questions about legality.

Even when used in 'normal' criminal investigations, there are concerns that these devices may be inherently unlawful. This is because they can 'grab' the phone information of everyone in a certain radius, not just of the person that is being targeted by police. Therefore, even if a judge has authorised the surveillance of one particular person, when the device is used this way, it may violate thousands of other people's privacy too. It is not clear how this can be lawful in terms of the RICA system, let alone section 14 of the Constitution, which protects the right to privacy.

R2K used the Promotion of Access to Information Act to demand proof that the RICA judge had even been notified of the use of Grabbers: government agencies refused to provide the information. ■

Read more

"How Cops and Crooks Can Grab your Cell Phone", Mail & Guardian, 27 Nov 2015

CASE STUDY *"Rogue Spook" Paul Scheepers*

Former Crime Intelligence official Paul Scheepers faces prosecution in the Bellville Special Commercial Crimes Court for a range of offences, including contravening RICA. Scheepers is accused of running a private security firm on the side of his police duties, and supplying falsified affidavits to a magistrate in order to get meta-data records of lawyers, senior cops, an individual from the financial services regulator, and other individuals.

He is also accused of acting as a vendor for a UK based company called Forensic Telecommunications Services Ltd (FTS), helping sell an IMSI Catcher on behalf of FTS to a local cash-in-transit security firm (who, according to court documents, had been assured it would be legal to acquire the device). At time of going to print, the trial was scheduled for May 2017. ■

CASE STUDY *amaBhungane journalist bugged*

In 2015, it emerged that unknown government spies had spied on the communications of amaBhungane journalist Sam Sole while he was reporting on the corruption investigation against Jacob Zuma. Though it had previously been reported that he suspected he was under surveillance, it was verified after transcripts of Sole's phone conversations with a source were submitted as evidence in the ongoing court battle over President Zuma's corruption charges. This revealed that state resources had been used to spy illegally on Sole as a journalist, and had then leaked the contents of his communications, illegally, to a private citizen (the transcript was submitted by Zuma's legal team). ■

06 Watchdog bodies

Who gives oversight to the security agencies?

Parliament's Joint Standing Committee of Intelligence

The Joint Standing Committee on Intelligence (JSCI) is a committee constituted by Parliament to deal with matters relating to intelligence. It has special rules allowing it to meet behind closed doors (the public and media are not allowed to attend the meetings).

The current chairperson of the JSCI is Hon. Charles Nkaqula.

Office of the Inspector General of Intelligence

The Inspector General is like the Public Protector, but focused on the intelligence structures. The Inspector General is mandated to ensure South Africa's intelligence agencies comply with the Constitution and other laws, and to investigate complaints from members of the public and members of the intelligence services on any maladministration, abuse of power, or criminal activity by the intelligence structures (including illegal surveillance). While this has the potential to be a powerful watchdog for the public, in reality the Inspector General has often lacked transparency and independence, and can only disclose information to the public after consulting the President and the Minister of State Security or Police. In December 2016, Parliament nominated Dr Setlhomamaru Dintwe as the next Inspector General, after a nearly two-year vacancy.

The nominated Inspector General Dr Setlhomamaru Dintwe.

RICA judges

RICA puts certain designated judges in charge of authorising (or not authorising) requests by law enforcement for warrants to intercept people's communications. There is a single 'RICA judge' to consider requests for direct interceptions, who is appointed by the President and reports to Parliament's intelligence committee. However, any High Court judge or magistrate can authorise requests to intercept meta-data that is more than 90 days old. Some of the problems with this oversight are explored on pages 8-11. In 2016, Judge George Maluleke became the main 'RICA' judge.

Picketing the court where a former intelligence official is charged with tapping journalists' phones

06 Let's take action against surveillance!

It's time to demand an end to surveillance abuses!

Let's challenging RICA!

On 30 March 2016, the United Nations Human Rights Committee released its review of South Africa's human rights record, in connection to the International Covenant on Civil and Political Rights.

Responding to submissions made by the Right2Know Campaign, the UN Human Rights Committee was very critical of South Africa's surveillance policies, and RICA in particular. The Committee expressed concern that mass surveillance takes place outside the law in South Africa. It also noted with concern that the grounds

for the issuing of warrants authorising spying on someone's communications are too vague, and the state's system for interception of communications is not transparent or accountable. All these problems make it more likely that the surveillance capacities of the state will be abused.

In response, led by the Right2Know Campaign, 40 civil society and social justice organisations released a joint demand for an end to surveillance abuses. Among these demands:

- No more SIM card registration – we want the right to communicate anonymously!
- No more data retention – communication providers shouldn't be allowed or forced to store our sensitive communications data for years!
- RICA must be reformed to be more transparent, with more accountability and oversight
- No more mass surveillance!

The full list of demands can be downloaded at www.r2k.org.za/rica-demands.

You cannot fix a political problem with legal reforms alone. But when existing legal loopholes exist to perpetuate and deepen a problem, no solution can be possible without legal reforms.

We must push the Department of Justice to fix RICA now and end surveillance abuses.

Demanding surveillance oversight

1. Inspector General must act

From 2015 to 2016, there was no Inspector General of Intelligence. All complaints and investigations of surveillance abuses ground to a halt. R2K activists spent a lot of energy in Parliament to ensure an Inspector General is appointed. Now we must get the Inspector General to act on all complaints tabled before him, and ensure that the Inspector General acts in a transparent and independent way.

This may require reforms to the Intelligence Services Oversight Act, which does not provide for enough transparency or independence of the Inspector General, or provide for a deputy Inspector General to avoid any future vacancies.

2. Parliament must stand up against the securocrats!

We must campaign to make Parliament more independent and fearless in tackling state-security abuses, including surveillance. The public must continue to pressure Parliament's intelligence committee to be more transparent and provide more public oversight on surveillance issues, rather than meeting behind closed doors.

3. RICA judges must provide more information to the public

The RICA judge's annual report must be made public promptly and must be more detailed and conform to a minimum standard. (Previous reports have only been released months or years after being tabled in Parliament and lack important details.) Most importantly, *all* High Court judges and Magistrates must report annually on how many warrants they have signed to authorise the interception of people's meta-data and call records.

4. Push for more transparency from the state on surveillance activities

In the short term, while we campaign for new laws and regulation to end surveillance abuses, the security agencies, especially the SSA, must publicly disclose details of the scope and scale of surveillance activities carried out by the state.

The state must also disclose its intelligence sharing agreements with foreign countries (using the present Parliamentary Inquiry in Germany as a 'best practice'). Not only will such hearings strengthen public oversight and accountability but they will also help ongoing efforts to bring South Africa's surveillance laws in line with international human rights law.

5. Tackling the private sector's role in surveillance

The communication service providers in South Africa – MTN, Vodacom, Telkom, and others – have assisted the state in spying on its customers without any pushback. We must call on them to be more transparent and more independent

and defend their customers' right to privacy. At the very least, these companies must publish annual transparency reports to disclose how many times a year they help the government spy on their customers.

6. Using the courts to challenge surveillance!

All of the examples above are campaigning opportunities to challenge surveillance and RICA abuses through policy processes and political action. But we must also use the courts to enforce our rights and challenge laws which violate our rights. R2K should support strategic court cases to challenge surveillance abuses.

7. Protect your communications and practice digital security!

Protecting your own communications is an important step in challenging surveillance abuses. There is no 'one-size fits all' solution for digital security, but they could include switching from voice calls and text messages to encrypted data calls and messages. One excellent resource is the Surveillance Self-Defence Guide (see below).

Protect your communications

For tutorials on digital security and securing your data, see the Electronic Frontier Foundation's Surveillance Self- Defence Guide: https://ssd.eff.org

08 More resources

R2K activist handbook:

- *Big brother exposed: stories of South Africa's intelligence structures monitoring and harassing activist movements*

Available at: bigbrother.r2k.org.za

MPDP research papers on communications surveillance in South Africa:

- Heidi Swart, 'Communications surveillance by the South African Intelligence Services'.
- Admire Mare, 'An analysis of the communications surveillance legislative framework in South Africa'.
- Admire Mare, 'A qualitative analysis of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa'.

Available at: mediaanddemocracy.com/communication-surveillance.html

MPDP investigative journalism series on surveillance:

- Heidi Swart, 'Big Brother is listening – on your phone', Mail& Guardian, 13 November 2015
- Heidi Swart, 'How cops and crooks can "grab" your cellphone – and you', Mail& Guardian, 27 November 2015
- Heidi Swart, 'Say nothing – the spooks are listening', Mail& Guardian, 18 December 2015
- Heidi Swart, 'You always feel like somebody's watching you? They probably are', Daily Maverick, 03 June 2016
- Heidi Swart, 'Missed call: Rica registration 'useless' for crime prevention purposes', Daily Maverick, 10 November 2016

Available at: mediaanddemocracy.com/communication-surveillance.html

MPDP & R2K research monograph:

- Dale McKinley, 'New Terrains of Privacy in South Africa'

Available at: r2k.org.za/privacy-monograph

09 Glossary

CID: Crime Intelligence Division of the Police (p 4)

GCHQ: UK Government Communications Headquarters, a surveillance agency for the United Kingdom (p 8)

Grabber: a mobile surveillance device (p 19)

I**MSI Catcher:** see 'Grabber'

Information Regulator: South Africa's new data protection watchdog (p 16)

Intelligence: the gathering of information, especially secret information, often by the state

Intelligence agency: a government structure that collects, analyses and uses information and intelligence in support of law enforcement, national security, and foreign policy objectives – usually in secret (p ii)

JSCI: Parliament's joint standing committee on intelligence (p 21)

Mass surveillance: (p 11)

Matthews Commission: (p 8)

Meta-data: (p 11)

NCC: National Communications Centre (p 14)

NICOC: National Intelligence Co-Ordinating Committee (p ii)

NSA: National Security Agency, a surveillance agency for the United States government (p 9)

OIC: Office for Interception Centres (p 14)

OIGI: Office of the Inspector General of Intelligence, a watchdog of the intelligence agencies (p 21)

POPI: Protection of Personal Information Act (p 15)

RICA: Regulation of Interception of Communications and Provision of Communications Related Information Act(p 12)

SAPS: South African Police Service (p ii)

SSA: State Security Agency (p ii)

Join us!

R2K is pushing for an end to surveillance abuses in South Africa!

Here are some practical steps to fight back:

- Know your rights and equip yourself with knowledge of the intelligence structures. Share this handbook with others!
- Challenge surveillance and state-security abuses, and make this part of daily struggles to build democracy!
- Demand laws and policies that protect our rights!
- Demand that Parliament and the Inspector General of Intelligence act as watchdogs against surveillance abuses!
- Join the Right2Know Campaign and volunteer at the monthly working group meetings!

Contact us:

- R2K National: 021 447 1000 | admin@r2k.org.za
- R2K Gauteng: 011 339 1533 | gauteng@r2k.org.za
- R2K KZN: 031 301 0914 | kzn@r2k.org.za
- R2K Western Cape: 021 447 1000 | westerncape@r2k.org.za

Follow R2K on social media and help spread the word:

Twitter: @r2kcampaign | Facebook: right2know

WWW.R2K.ORG.ZA