SPOOKED

SURVEILLANCE OF JOURNALISTS IN SA

RIGHT2KNOW

Find this report online at r2k.org.za/spooked
#StopTheSpies #OngaziMakazi

This handbook was produced by the Right2Know Campaign,
and researched by Murray Hunter and Tymon Smith.

 Published June 2018.

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

Facebook | Twitter | Instagram: @r2kcampaign

Contents

Introduction

Today, many journalists in South Africa are fearful that someone is listening in on their sensitive conversations and spying on their communications. They speak in whispers about the threats they've received, and they joke about it on Twitter too.

Under the apartheid regime, says veteran reporter Max Du Preez, journalists knew their phones were being tapped. "There was no buzzing or beeping," says du Preez, "but we [at Vrye Weekblad] knew because they would produce transcripts later when laying charges. And after 94, people would come confess to you that it was happening."

Fast forward more than two decades later, at the end of the Zuma era: under a constitution that promotes freedom of expression and privacy and limits the powers of the security agencies, we have seen the spooks regain power and influence.

Indeed while R2K has shown significant evidence that surveillance in South Africa affects all members of society, journalists in South Africa have been a particular target for state spying, and more recently, even private-sector spying. This seems to be especially true for journalists who have uncovered corruption, state capture, and abuse of power and in-fighting in agencies like the National Prosecuting Authority (NPA), the State Security Agency (SSA), the Crime Intelligence division of the police, and the Hawks.

This report looks at a range of case studies of surveillance against journalists, to unpack what happened, how it happened, and which parties appear to be responsible. The aim is twofold: to give journalists a better picture of the threats they might face, so that they can better defend themselves, and to rally the broader public to join the campaign to end these surveillance abuses and the bad policies that enable them.

Let's remember that everyone has a right to privacy — nobody's communication should ever be spied on unless they are facing a legitimate investigation for serious criminal activity. But journalists' communications are especially sensitive. This is because as part of their work, members of the media must have confidential discussions with whistleblowers and secret sources who are only able to speak out if their identity is protected. In fact, South Africa's courts have recognised

that protecting the identity of journalists' sources is an "essential" part of media freedom.[1] On top of that, the threat of surveillance can have a hugely intimidating and traumatising effect on journalists — when a journalist fears being spied on, it can have the effect of silencing them from doing the courageous work that is expected of them.

At time of writing, South Africa's main surveillance law, "RICA"[2], faces a constitutional challenge by the AmaBhungane Centre for Investigative Journalism. AmaBhungane launched this court case after learning that one of their journalists, Sam Sole, had been spied on by the National Intelligence Agency (now the SSA). For months, government agents listened to the confidential discussions he had with sources, as well as all of his personal calls with friends and loved ones.

AmaBhungane has told the court that when the government spied on Sam Sole, RICA failed to protect him. They have told the court that RICA is unconstitutional because it fails to protect the rights of journalists and others against surveillance abuses. R2K has joined as a friend of the court to support this position.

This report is the latest in a series of R2K publications looking at surveillance abuses

Big Brother Exposed (2015) documents the testimonies of political activists and unionists who have been harassed or spied on by intelligence structures.

Stop the Surveillance (2017) unpacks some of the main surveillance policies and practices in South Africa, especially the law called RICA.

New Terrains of Privacy in South Africa (2017) is a research study produced with the Media Policy & Democracy Project, exploring biometrics, data collection, SIM card registration and other mass surveillance practices.

Find them at r2k.org.za/publications

1 Bosasa Operation (Pty) Ltd v Basson and Another (09/29700) [2012]

2 Its full name is the Regulation of Interception of Communications and Provision of Communication-Related Information Act

How does communication surveillance work?

The legal framework for surveillance in South Africa is spelt out in the law called RICA.

This Act says that you must link your SIM card, landline and internet account to your identity, so that any communications from that SIM card or account can be traced back to you.

According to RICA, if law enforcement agencies want to intercept your communication, they need to apply for a warrant from a special judge (the 'RICA judge') who is appointed by the President. If the judge approves their application and provides a warrant, this warrant can force any telecommunications company or internet service provider to help the agency intercept the communication of the user.

However, RICA is not the only law that allows for surveillance. Section 205 of the Criminal Procedures Act, South Africa's criminal law, allows law enforcement officials to bypass the RICA judge to get access to your phone records – which shows who you have communicated with, when, and where. According to this provision, any magistrate can issue a warrant that forces telecoms companies to give over a customer's call records and metadata (metadata is all the information about who you contacted, when and from where).

In either situation, the person who has been spied on is never notified that their sensitive information was handed over. In fact, RICA makes it a crime to reveal that the information was handed over, even once the investigation is concluded. This means that if your communications are ever intercepted, even illegally, you never find out about it.

The one difference is that s205 warrants are used much more often than RICA warrants: in 2017 R2K got statistics from MTN, Vodacom, Cell C and Telkom which suggest that law enforcement agencies send them 25,000-50,000 'section 205' warrants every year, as opposed to 500 or 600 'RICA' warrants.[3]

---

3 "Stats reveal that cops are spying on 70,000+ mobile phones every year", 23 August 2017: r2k.org.za/surveillance-stats

Sam Sole

SSA listened to his calls for at least six months

Sam Sole is a director of the ama-Bhungane Centre for Investigative Journalism, and was previously an investigative journalist for the Mail & Guardian. In 2015, it emerged that the National Intelligence Agency (now the SSA) had been tapping his phone while he was reporting on the corruption investigation against Jacob Zuma in 2008.

In a three-decade career as an investigative journalist, Sam Sole has written many articles exposing successive governments' corruption and by his own admission, has become somewhat of a "rather large pimple on the body politic."

In 2008 while reporting on the NPA's investigation of charges of corruption against former president Jacob Zuma, Sole and the amaBhungane team, suspected that their communications might have been monitored.

As Sole recalls, "At the time people from the Zuma camp – who will remain nameless – boasted to us, 'Oh we know you were talking to so and so; we've heard it or we've read the transcripts; or you met with X.'"

However, it was not until 2015 that Sole received evidence of these suspicions when Zuma's lawyers submitted transcripts of conversations between him and NPA prosecutor Billy Downer in the court case for the release of the "Spy Tapes".[4] These transcripts were proof that their calls had been monitored, thought it was not clear whether the monitoring targeted Sole, Downer or both.

---

4 "AmaB challenges snooping law," 20 April 2017: http://amabhungane.co.za/article/2017-04-20-amab-challenges-snooping-law

Sole then made an information request to the State Security Agency (SSA), using the Promotion of Access to Information Act, for confirmation that it had spied on him. Six months later the SSA released a copy of a warrant that had been issued by the RICA judge to tap Sole's phone. This document appeared to be the second warrant the judge had issued, renewing a previous decision to tap Sole's phone, but the SSA said it had no other documents on file. The document provided no reasons for the interception.

Sole then lodged a complaint with the Inspector General of Intelligence, the watchdog on the intelligence services like SSA, to ask for an investigation of how and why Sole had been spied on, and whether any laws had been broken.

> *"'Is your phone tapped?' people often ask me. 'I don't know, but I assume it is,' is always my answer."*

In August 2017, more than two years later, the new Inspector General of Intelligence, Setlhomamaru Dintwe, concluded his report. Unlike the other documented cases of surveillance against journalists, Dintwe found that the SSA had not tried to disguise Sole's identity or occupation from the RICA judge: the SSA's request for a warrant "made clear and direct mention of Mr Sole being a journalist and for which media house." In other words, the RICA judge at the time, Judge Khumalo, knowingly signed off on the spying of a journalist.

According to Dintwe's report, the surveillance was part of an operation to identify certain "information peddlers" -- a concept that came to prominence in the 'Secrecy Bill' era of South African politics, to describe individuals who supposedly 'sell' confidential information for profit. It would appear that the intelligence operation was therefore explicitly intended to identify Sole's confidential sources -- although Sole says he has never and would never pay a source for information. Dintwe's investigation determined that Sole was not the only person who was targeted in the operation, although the report did not say if other journalists were among those targeted.

In 2017, amaBhungane launched a legal challenge to RICA's constitutionality[5]. Their challenge aims to address RICA's major flaws (see box). A keystone in their case is the need for RICA to provide notification to users whose communications have been intercepted, even after the fact - Sole says this is needed so that abuses can be acted on.

"Other than this rare case, which came about because of the Zuma tapes, you never get to know that you were monitored and you're never able to challenge the basis and the facts under which that process was done, supposedly legally, and that's a big problem with the system," he says.

"The rule of thumb is that electronic communications are not safe," says Sole. For their recent award-winning work on the so-called 'Gupta Leaks', the team made as little use of electronic communication as possible.

"It's the structure of many intelligence services that while they claim to be protecting the interests of the country, historically and institutionally they're often there to protect the king, or whatever the semi-democratic substitute may be."

5 Ibid

What's wrong with RICA?

These are the main constitutional flaws raised in amaBhungane's case:

- The person targeted for surveillance is never informed of the warrant to intercept their communications – even after the interception has ended and any investigation has been concluded.
- RICA requires that private companies must store a lot of information about who users are and who they communicate with, but it does not provide for any oversight mechanisms.
- RICA is silent about what procedures officials should follow when examining, copying, sharing, and storing the intercepted data. When intercepted data is not relevant to an investigation, there is no prescribed procedure for it to be destroyed.
- RICA does not recognise the need for extra protections for people who have a special legal duty to protect the confidentiality of people they speak to, such as lawyers and journalists.
- The oversight system created by the RICA judge is not sufficient - in particular the process should include a 'public advocate' who should represent the interests of people who have been targeted for surveillance, and to test the reasons for interception which police and intelligence services provide to the RICA judge.
- RICA does not regulate the state's "bulk interception" programmes; this refers to mass surveillance practices which involve collecting and analysing massive flows of data of large groups of people, rather than specific individuals who are under investigation for a serious crime.

Jacques Pauw

SSA recorded his phone calls to identify 'state capture' whistleblowers

Jacques Pauw first came to prominence as an investigative reporter for the anti-apartheid newspaper Vrye Weekblad, where he helped to expose the existence of secret police death squads.

His 2017 book, *The President's Keepers*, exposed a network of corruption and abuse of power surrounding former President Jacob Zuma, especially in three key law enforcement agencies: the South African Revenue Service (SARS), the Hawks and Crime Intelligence divisions of the police, and the State Security Agency.

While *The President's Keepers* has become the best-selling book in South African history, Pauw has faced criminal charges, a police raid, and evidently even been spied on.

Pauw faces one set of charges in terms of the Intelligence Services Act, which makes it a crime for any employee of the SSA to reveal secret information without permission[6]. Another set of charges stems from the Tax Act, which makes it a crime to reveal confidential tax information of any person. (*The President's Keepers* alleges that Zuma owed millions of rands in taxes and that tax officials who tried to get him to pay were forced out of SARS.)

In March of 2018, the Hawks's The Crimes Against the State unit raided Pauw's home and office in Riebeek Kasteel, Western Cape, to search for classified documents.

Pauw says he always expected to face criminal investigations after publishing the book. The week before *The President's Keepers* was published, Pauw says broke off contact

6 While some of Pauw's sources may have been SSA employees, it is not clear how he could be charged under the Act as the secrecy clauses do not seem to apply to civilian.

with all his sources and deleted all records off his computer. "Simply to protect them [my sources], because I knew they were going to listen to my phone," he says.

One of the most explosive revelations in *The President's Keepers* was that Arthur Fraser, then head of the State Security Agency, had faced internal investigations at the SSA that implicated him in massive corruption and illegal intelligence gathering. After the book came out, Pauw received an unexpected second cache of documents, comprising two further investigations against Fraser that had been conducted by the previous Inspector General of Intelligence.

According to Pauw, "That's what drove Arthur Fraser absolutely f***ing mad." The second reports, which were published on The Daily Maverick website[7], confirmed the contents of the SSA's internal investigations and Pauw's book itself. Until then, Fraser had been threatening to sue, but Pauw said they never heard from Fraser after that. However, it is reported that Fraser established a whole task team to investigate the leaks.

> *"I can't do my job as a journalist if my phone and my emails are being monitored. I can't speak to sources, I can't accept any material, I can't do anything."*

In May 2018, the City Press reported that it had transcripts and recordings of a phone call between Jacques Pauw and Setlhomamaru Dintwe, the Inspector General of Intelligence. According to the City Press, on the transcript, Pauw is referred to as "Target".[8]

Dintwe had called Pauw to ask him to give written confirmation that Dintwe had not been the source of leaked documents. At the time, Arthur Fraser had allegedly accused Dintwe of leaking the incriminating reports to Pauw. Pauw agreed to provide a letter.

The existence of the transcript is strong evidence that the State Security Agency was indeed spying on Pauw's private communications – an operation he believes was designed to expose the whistleblowers behind *The President's Keepers*.

---

7 "The Principal Agent Network (PAN) Dossier", 5 December 2017: https://www.dailymaverick.co.za/article/2017-12-05-the-principal-agent-network-pan-dossier-zuma-and-mahlobo-knew-about-arthur-frasers-rogue-intelligence-programme/

8 "Why was intelligence inspector hounded?", 6 May 2018: https://www.news24.com/SouthAfrica/News/why-was-intelligence-inspector-hounded-20180505

"I'm not in possession of any material that jeopardises state security. I am simply in possession of material that shows fraud and corruption at State Security," he says. "It's got fokol to do with state security, it's got to do with protecting Arthur Fraser."

Because of the surveillance on him, Pauw has not been able to do any further investigative reporting. "I can't do my job as a journalist if my phone and probably my emails are being monitored. I can't speak to sources, I can't accept any material, I can't do anything."

When certain people phone him, Pauw immediately advises them not to say anything over the phone.

The similarities between the interception operations against Pauw and Sam Sole (chapter 1) suggest that in Pauw's case, like Sole's, the RICA judge knowingly signed off on a warrant to spy on a journalist in order to identify their sources.

Pauw acknowledges that such a practice is disastrous for the protection of whistleblowers, who usually bring information to the media after other avenues have failed.

"It's become very difficult for whistleblowers in this country, because their protection is not absolutely sure. We need to create conditions where whistleblowers can go to journalists, make their confessions, it gets published, and then there needs to be protections," he says.

Though Pauw was first spied on by the state as a journalist working at the anti-apartheid newspaper Vrye Weekblad, he points out that the pre-94 state was "much more brutal and far harsher" than now. "One of the reasons I'm not scared now is because I've got the Constitution behind me. We didn't have that in 1989 or 1990," he says.

At the time of publication, Pauw's legal team was still considering its next steps to challenge the state's spying.

In April 2018, Arthur Fraser was moved out of State Security and is now head of Correctional Services. He faces a range of investigations.

Stephan Hofstatter & Mzi wa Afrika

Crime Intelligence lied to judge to bug their phones after stories about police corruption

In 2010, while journalists Mzilikazi wa Afrika and Stephan Hofstatter were investigating major corruption scandals in the South African Police Service (SAPS), the police's Crime Intelligence Division (CID) tapped their phones.

At the time, wa Afrika and Hofstatter were working for the Sunday Times investigation unit. One of their major exposes related to an irregular leasing deal conducted by then Police Commissioner Bheki Cele which benefitted businessman Roux Shabangu, a friend of Jacob Zuma. Cele would be fired a year later as a result of this expose.

While working on a follow-on investigation in Cato Manor in 2011, a source informed the two journalists that a senior official within the Kwazulu Natal police force wished to meet them to apologise for the tapping of their phones by members of Crime Intelligence during their investigation into Cele.

The meeting never happened but it served to confirm wa Afrika and Hofstatter's suspicion that they had been spied on. They were even given a copy of the RICA warrant by their source, which ordered their phones numbers to be tapped. According to the RICA warrant, the police had told the RICA judge that the numbers belonged to ATM bombing suspects. The warrant authorised the real-time interception of their calls and text messages, as well as of their metadata.

The two approached then Sunday Times Editor Ray Hartley and decided to lay a charge against the police for unlawful interception.

However it may have been more than pressure from the newspaper which lead to the police undertaking an investigation into the interceptions. In a strange twist, the fake intercept order included not only Hofstatter's and wa Afrika's phone number, but Bheki Cele's phone number as well.

Says Hofstatter, "There are various theories as to how his number ended up there…but the most plausible is that his number had been written down on a piece of paper to authorize the intercepts and had accidentally been included in the intercept order."

> *"If you are spying on journalists, understand that this is a criminal offence"*

The prosecutor later told Hofstatter that the bugging of Cele was the real reason there had been a proper investigation into the matter.

During the investigation of the case, Hofstatter says it was never in dispute that they had tapped journalists' phones. Instead, the criminal charge was for giving false information to the RICA judge. Though the investigation determined that senior police officials were involved in the decision to spy on the journalists, only the most junior officer, former Captain Bongani Cele, was ultimately prosecuted. The Pretoria Commercial Crimes Court found him guilty in August 2017 and gave him a three-year suspended sentence.

Hofstatter says that the decision to lay charges was motivated by a desire to send a message to the security services that there can be consequences. "If you are knowingly taking an order from your superiors to spy on journalists, to spy on activists, understand that this is a criminal offence and you can actually go to jail for it," he says.

Both Hofstatter and Wa Afrika say as a result of their experience they tend to use their phones less and prefer to use end-to-end-encryption services for communication with sources. Hofstatter advises that journalists to have meetings with sensitive subjects face-to-face.

Wa Afrika says that his communications continue to be interfered with and believes his Gmail account was hacked as recently as December 2017.

"I confronted someone from intelligence who I suspected was behind it and he admitted he was. So they're still doing it but in a more clandestine way," says Wa Afrika. He has also been the subject of death threats.

"I've received more death threats than birthday presents. You have to take every one seriously and some you pass on to your bosses and some I pass on to friends in intelligence," he says.

The Sunday Times Investigations Unit was disbanded in 2016 but Wa Afrika continues to work as a senior reporter for the paper while Hofstatter now works for Business Day and the Financial Mail.

In February 2018 Bheki Cele was made Minister of Police.

Athandiwe Saba

Spied on by a private investigator while reporting on public corruption

Athandiwe Saba is a reporter for the Mail & Guardian in Johannesburg.

In 2016, she was approached by a source at the Railway Safety Regulator (RSR), the government agency that oversees railway safety across the country. Saba's source had allegations that the RSR's chief executive Nkululeko Poya had tried to mislead investigators from the Public Protector. At the time, the Public Protector was investigating a number of allegations, including that senior executives had used a government vehicle to deliver anti-Magashule t-shirts to the ANC in Welkom.[9]

Saba made contact with the Railway Safety Regulator and put the allegations to them. She met with the RSR's spokesperson and the CEO, Mr Poya, at a hotel in Irene. She recalls that Poya's defence was that the allegations were part of a smear campaign to prevent his contract from being renewed. "He felt people were coming for him and trying to dirty his name."

"I left, I wrote a balanced story, and I don't remember them having any concerns about the story."

A year and a half passed. Saba did not do any further stories on the RSR. But the problems for Mr Poya did not end. In January 2018, the Sunday Times reported that Poya had been suspended and that there was a forensic investigation into his dealings. According to the Sunday Times, the investigation determined that Poya had hired a private investigator to spy on certain members of the board.

---

9 "T-shirt whistleblower may derail the railway regulator as the public protector probes", 16 August 2016: https://mg.co.za/article/2016-08-16-00-t-shirt-whistleblower-may-derail-the-railway-regulator-as-the-public-protector-probes

> *"As a journalist you always think you're being watched, but it's rare that you find evidence"*

Before long, Saba also received a leaked copy of the documents - and they had her name in them. It appeared that Mr Poya's private investigator had snooped on Saba: a copy of his report, dated 2016, had copies of her cell phone records, for both of her cell phone numbers, as well as her phone's unique IMEI number and a credit report.

The report listed all calls between her and some of the board members.

Saba was stunned. "As a journalist you always think that you're being watched or listened to, but it's very rare that you find evidence that somebody went out of their way to try track you. He had my cell phone records so they could find out who I was speaking to, who was the leak," she says.

She says at first she laughed it off. "But when it finally settled in, I started to get really angry. It was such a violation," she says.

Saba went to Khadija Patel and Beauregard Tromp, editor and deputy editor of the M&G, who then went to MTN and Vodacom, the two networks Saba had been using. At the time of this report, Vodacom had yet to report back, but Saba says MTN confirmed that her phone records had been seized in 2016 in terms of a warrant by s205 of the CPA, issued by a judge in KZN. This would mean the private investigator would have needed an accomplice in the police or the NPA. Several people may have committed a crime in accessing Saba's call records.

This would not be the only such incident where individuals in the police have used their position to get cell phone records for private purposes. In Cape Town, a former Crime Intelligence official named Paul Scheepers is facing a host of charges for acquiring warrants fraudulently to get people's phone records.

At time of writing, this incident was still unfolding. But Saba says she intends to take action for the violation of her rights. She and her editors have approached lawyers and are considering their legal options.

Peter Bruce & Rob Rose

Private investigator bribed MTN official for phone records

In 2017 it emerged that a private investigator had illegally accessed the private phone records of business press editors Peter Bruce and Rob Rose, apparently for the benefit of a Gupta-linked propaganda campaign.

Peter Bruce had 17 years experience as editor of the Financial Mail and Business Day, before becoming editor-at-large for Tiso Blackstar, which publishes those titles. In his weekly newspaper columns, Bruce became a vocal critic of the Gupta family and the corrupt influence they had over various government agencies and cabinet ministers. Rob Rose is editor of the Financial Mail, which had reported extensively on the Guptas' business interests.

In June 2017 a website called WMCleaks.com appeared on the internet and started publishing articles about Peter Bruce. The articles were full of false information, such as claims that Bruce was having sex with his daughter's friends when he doesn't have a daughter, or that he was responsible for the invasion of Libya. But some of the articles made it clear that someone had been spying on Bruce.

In one front-page article, WMCleaks.com claimed that Bruce had been cheating on his wife and posted photos of Bruce hugging a woman who was claimed to be

his mistress. As Bruce would explain in the pages of Business Day[10], the photos published on WMCleaks.com appeared to show that he had been followed secretly for at least a week: the photos showed him and his wife walking their dogs, visiting a psychologist's office as he looked for help for a family member, and visiting a business in Parkhurst run by a family friend. (This was the woman who hugged him in the photograph.)

An investigation by the Daily Maverick found that the website and article were linked to a former Gupta employee working in India named Saurab Aggarwal.

Two months later,evidence emerged that Bruce's phone communications had also been spied on and leaked to whoever was behind the website, along with those of Financial Mail editor Rob Rose. In August 2017, WMCleaks.com published an article alleging that Bruce, Rob Rose and former Finance Minister Trevor Manuel were behind an attempt to persuade Baroda Bank to close several Gupta business bank accounts. The article claimed to have records of various phone calls between Bruce and Rose, and Rose and Manuel, alleging that these individuals were communicating with the manager of Baroda Bank via an unnamed middleman in order to force the closure of the Guptas' business accounts.

> *"I have no doubt they [the Guptas] approved and paid for my surveillance"*

Bruce then received a call from someone in the security department at MTN to inform him that an employee had accessed his account illegally and that the phone provider was investigating.

It subsequently emerged that an MTN employee, Primrose Nhlapo had sold Bruce and Rose's phone records to a private investigator named Nico Smith, a former member of the Hawks. Nhlapo was allegedly paid R3,750 for the information.

In terms of RICA, passing on someone's call records is a criminal offence. MTN pressed charges against Nhlapo, and the case is waiting to be heard in the Randburg Magistrate's Court.

---

10 "The price of writing about the Guptas," 29 June 2017: https://www.businesslive.co.za/bd/opinion/columnists/2017-06-29-peter-bruce-the-price-of-writing-about-the-guptas/

When asked how Nhlapo was able to access their phone records, MTN spokesperson Jacqui O'Sullivan said, "As part of her job in our fraud management environment, it was necessary for her to access customer call information in order for her to perform her duties, so it would not be unusual for her to access records for legitimate purposes." Nhlapo subsequently resigned before facing a disciplinary process.

Bruce admits that he was shocked by what happened he still believes that journalists can be protected. "We don't live in a totalitarian country," he says. "I'm sure there are attempts to listen to phone conversations now and again but who do you listen to? If you're paranoid you want to listen to everybody and you can't..."

At this time no other person has been charged for the interception of Bruce and Rose's phone records.

MTN spokesperson Jacqui O'Sullivan says, "MTN has further enhanced its systems by introducing stringent monitoring and review processes."

"Donna"

Evidence that she was targeted in a Crime Intelligence operation

Donna[11] was a reporter for a Johannesburg newspaper who came to believe Crime Intelligence was running an operation against her. This happened while she was working on a series of stories involving former head of police Crime Intelligence Richard Mdluli.

One day in 2012 Donna received a call while working in the newsroom. The caller had an American accent and claimed to have a juicy story. After speaking with her editor, Donna arranged to meet the caller. He claimed to work for the CIA and told her that the Agency was investigating the whereabouts of Gaddafi's millions in South Africa. She asked him to provide proof, which he promised to provide. A week later he called Donna to tell her that he was still collecting documents but he had another story for her. They met; Donna listened to his story and wrote an article after corroborating the information she had been given.

A relationship based on a certain amount of trust had been established. So some time later, Donna agreed to meet him for coffee again. She now remembers signs that he was faking his American accent. "He was quite good at it but I caught him out on certain words – 'robots' instead of 'traffic lights' and 'garage' instead of 'gas station'," she says.

At this meeting her American source mentioned that the CIA "has a fund that helps South Africans, especially those who give them information." Donna did not understand why her source was mentioning this. He then told her, "If ever your son needs anything like soccer boots or whatever, don't hesitate because we're here to help." At the time Donna's son was in primary school and was a keen soccer player. She initially thought nothing of it, although she was a little unnerved because she had never discussed her son or her personal life with her source.

---

11 "Donna" asked to withhold her name

In June 2012, it was Donna's mother's birthday and she was busy making arrangements to travel to her mother's home in another province for the celebrations. She had bought a lot of things to transport with her on the journey. As she was preparing to leave, her source called her to another meeting about a new story. At this meeting the source mentioned in passing that the CIA "often helps journalists because we've got big cars and there's a Jeep available so if you've bought stuff that you want to take home, you can use the Jeep." Donna clicked that the 'source' had information about her personal life. She excused herself from the meeting and reported the incident to her editor. "It was clear that they were tapping my phone and monitoring my movements because how else did they know that I had a lot of stuff I needed to take down to my mother?" says Donna.

She was shaken by the realisation and stopped accepting calls from the source. "My life and my son's life were way more important than any scoop," she says.

> *"We like to believe we're not high profile – until you hit somebody's nerve"*

Donna also contacted some of her sources at Crime Intelligence who told her the 'American' was in fact a counter-intelligence agent of Crime Intelligence, but she was never able to establish his name. The agent kept trying to call Donna and after ignoring a lot of his calls, eventually she answered. He told Donna that he was travelling outside of Johannesburg and needed a favour: He claimed that someone owed him R10 000 and that he wanted them to deliver the money for safekeeping to Donna's office. Donna realised it was a trap. "It was clear they wanted to come with an envelope and catch me taking the money so they could say I had accepted a bribe," she says. Donna told the source never to call her again.

She did not hear from the Crime Intelligence operative again. The following year, 2013, her name and phone number appeared in a fake 'intelligence report' that claimed a group of South African civilians, police officials and journalists was working to topple the South African government. The document was exposed by then Secretary General of Cosatu, Zwelinzima Vavi, who was also named in the report.

Donna discussed the allegations with her editor who tried to persuade her to change her number. As Donna recalls, "I would not change my number and would not change my life to suit them." She had her home and car swept for bugs and improved security at home to protect her son. She says that she never went to the police, because it would be "asking the people who were violating me to investigate themselves."

She later learned that several of her sources within Crime Intelligence were threatened, bugged or targeted with 'dirty tricks' intended to end their careers.

Why did all this happen? Donna believes she was targeted as a result of the stories she was publishing about Richard Mdluli, the former head of Crime Intelligence.

"We all like to believe that we're not high profile and we're just going about our daily stuff and churning out stories until you hit somebody's nerve or the reporting that you do compromises or threatens a person," she says.

Donna continues to work as a journalist in Johannesburg.

In 2018, after being suspended for six years, former head of Crime Intelligence Richard Mdluli was dismissed from SAPS.

"Chris"

Targeted by intelligence officials while reporting on labour disputes

"Chris"[12] was a radio reporter based in Johannesburg who believes his movements were monitored while he was reporting on labour issues in South Africa's platinum belt in the aftermath of the Marikana massacre.

Chris began his job as a radio reporter for a national station in Johannesburg in August 2012. As the new reporter on staff, within weeks he found himself in the midst of an unprotected strike at the Lonmin platinum mine in Marikana in the North West that ended in the Marikana massacre. In the aftermath of the massacre, the platinum belt was a hotbed of labour activity, and Chris found himself making regular trips to the platinum and gold belts covering mining-related stories in Rustenburg and Carletonville.

At this time Chris had little reason to believe that he might have attracted any interest from SSA agents. But by February 2013, he reports noticing a lot more CIDs (undercover operatives working for the Central Intelligence Division of the local police) in Marikana and the neighbouring townships and towns.

In March 2013, Chris and a colleague gave a lift to "two chaps from the community who came out straight and told us they're deployed there as CIDs."

"We weren't driving a marked car but they said they had been told to be on the lookout for journalists and follow us."

At the time, Chris was sharing a house in Johannesburg with a friend who worked for a surveying company which worked on the mines. One day in April 2013, Chris came home from work and his housemate said, "Geez guy, what did you do?"

Chris's housemate said he had received a call from the State Security Agency (SSA) asking him to come to their offices in Centurion for a meeting. At the meeting,

12 "Chris" asked to withhold his name

Chris's housemate was interviewed by two agents who told him that the interview was part of a background check needed because of his involvement with major mining projects. But over the course of the interview, Chris's housemate came to believe that they were more interested in Chris. The housemate was asked lots of questions about who he was living with and what kind of relationship they had and whether they shared information.

Chris says that he was shocked by his housemate's story. "I became hell of a paranoid but I didn't tell anyone what had happened," he says.

Chris also had suspicions that his communications may have been monitored. He says in 2014 he started hearing sounds on the phone which made him suspect that he was being spied on.[13] Later that year while attending an investigative journalism forum, Chris took advantage of a service offered and handed in his laptop and phone for debugging. "They debugged my laptop and found malware that could be used to activate spyware and also on my phone – background apps that were running all the time and they told me to get that off my stuff," he says.

In the years since, Chris has moved on to work for a different news organisation and now takes precautions against interception such as encryption for emails and texts, switching his microphone off on all phones, and restricting which apps have access to his contact list. He also makes sure that interviews with sources take place face to face in busy places or near running water to create background noise that may make it more difficult for a third party to record it. The organisation he works for also conducts regular sweeps of its offices to check for possible bugging devices.

Chris says the risk of being spied on comes hand-in-hand with being a journalist. "We are swimming in the same pond with them so we have to accept that there's a possibility they're monitoring us," he says. At the same time, he cautions that journalists should be aware of the risk of being 'played' by information peddlers in the intelligence structures.

He says, "If they give you a tip off and they're the primary source of the tip off… you know that there might be five other agents who you're not aware of who have been involved in a conversation before you come into contact with the agent who's your source."

---

13 **Note:** It is believed that most conventional forms of phone tapping do not leave an audible trace.

Tom Nkosi

David Mabuza claimed to be getting intelligence briefings on journalists

Tom Nkosi is the founder and publisher of Mpumalanga investigative newspaper *Ziwaphi*. He began his career as a journalist in Mpumalanga in 1987 before going on to work for the ANC in the early 90s and provincial government and then returning to journalism in 2007.

It is no secret that *Ziwaphi* investigations of corruption and criminality in Mpumalanga politics made Nkosi unpopular among some of the province's most powerful politicians.

In January 2015, at a press conference Mpumalanga Premier David Mabuza announced that he was receiving briefings from State Security on the movements of journalists in the province.[1] Mabuza singled out Nkosi as one of those who he said had been having meetings "with his [Mabuza's] enemies" within the ANC.

During the press conference, Mabuza is reported to have said: "It is the duty of the state to inform me every day about meetings that are happening in the evening, I get a report every day."[14]

If State Security agents were monitoring the movements of journalists, it would likely be unlawful so Nkosi filed a complaint to the Inspector General of Intelligence.

As he prepared his complaint, Nkosi started remembering similar instances from the past.

In 2010, he remembers Mabuza had confronted him during a press conference when he announced that he was going to sue some journalists for defaming him. Nkosi says Mabuza accused him of holding meetings with James Nkambule [a Mabuza rival

14 "Mpumalanga Premier said to be getting spy reports on journalists", 10 February 2015: https://www.iol.co.za/sundayindependent/mpumalanga-premier-said-to-be-getting-spy-reports-on-journalists-1815999

who had accused Mabuza of hiring assassins to eliminate his political opponents in the province]. Nkosi says he had been meeting Nkambule but denied having spoken to him recently. Says Nkosi, "He told me he knew I was lying. He joked about how he knew that we were having meetings with his enemies and what furniture was in their houses."

Nkamubule died in 2010, allegedly after being poisoned.

As he drafted his complaint to the IG, Nkosi also remembered having a run-in with David Mahlobo, the man who had become Minister of State Security less than a year before. In 2012, when Mahlobo was in the Mpumalanga provincial government, he and Nkosi had almost come to blows after Ziwaphi reported that Mahlobo was the only head of department in the country who used a blue-light brigade and bodyguards. Mahlobo accused him of "having an agenda and hiding behind journalism".[15]

"I was beginning to connect the dots and so I asked the Inspector General to investigate all these issues," says Nkosi. "I asked whether any of my activities as a journalist could be said to constitute terrorism, sabotage or subversion."

Nkosi filed his complaint in February 2015, asking the Inspector General to investigate whether the SSA had spied on him or his family members, and to determine whether such surveillance was legal or not.

In his complaint he noted that Mabuza's boast had "made it difficult for sources to provide information on the corruption that is going on in the province, and as a result corruption will escalate in the province as they're afraid to blow the whistle when they know that the Premier of Mpumalanga is aware that they're supplying information on corruption in government."

Three years later, Tom Nkosi is still waiting for a finding on this complaint. The new Inspector General, Dr Setlhomamaru Dintwe, had promised to conclude the investigation before the end of 2017 but this has not happened. Another veteran Mpumalanga journalist, Sizwe sama Yende, also submitted a complaint to the IG about Mabuza's claim, but abandoned it in the belief that it was not being taken seriously.

---

15 "Journalist, official clash", 24 July 2012: https://www.sowetanlive.co.za/news/2012-07-24-journalist-official-clash

Since then, Nkosi says he had to change a whole lot of things. "I stopped eating at government functions, I stopped travelling to certain areas and I had to make sure that my family limited their movements. I had to teach my daughter that if she heard noises outside at night she should keep quiet and get on the ground. I started speaking in codes on the phone to my wife. I have to maintain these protocols until I receive communication from the Inspector General," he says.

"It's time for journalists to be trained on security issues – how to secure your gadgets, phones," says Nkosi.

He also reminds journalists to take their role seriously. "If it wasn't for us [journalists] Jacob Zuma or his ex-wife would be president now. We wield power and that power is a threat to people and so we have to realise that. We make enemies and some of those enemies, or those who stand to lose by exposure, work in the state."

> *"Journalist wield power and that power is a threat to people."*

Nkosi continues to publish *Ziwaphi* and is still waiting to hear from the office of the Inspector General of Intelligence regarding his 2015 complaint.

David Mabuza is now deputy president of South Africa. David Mahlobo is now a private citizen.

Sipho Masondo

Warned he was spied on by Crime Intelligence

In 2017, Sipho Masondo had been working on a series of investigations that the City Press called 'WaterGate', which exposed corruption in South Africa's water delivery projects under the stewardship of former water minister Nomvula Mokonyane.

In January 2017, Masondo says he received an anonymous SMS that he should stop driving his car as he was being followed.

"Clearly it came from someone who knows me," says Masondo. The SMS included the model and registration of his car.

A few months later, in June, a source in Crime Intelligence warned Masondo that somebody was listening to his calls.

Masondo says he believes the spying may still be happening to this day.

Around that time, Masondo and another colleague received further tip-offs that Crime Intelligence had marked them for surveillance.

The City Press wrote a letter to police leadership to complain and as Masondo describes it, "ask them to get off our backs." No response has ever been received.

As in several other cases in this report, the issue of surveillance was overshadowed by other serious threats to Masondo's safety.

While he was reporting on the 'WaterGate' series, Masondo was approached several times by individuals offering him money to drop the story – including, he says, by senior Crime Intelligence representatives. At one point he was offered R3-million and a high-paying job to drop his investigation.

When he refused, City Press was told by a source that Mokonyane's special adviser allegedly met with senior SAPS officials to discuss "what to do with Masondo" – including speculation that he should be "dealt with". According to this source, some pushed for "Masondo's disappearance". Following this threat, Masondo's employers at Media24 took steps to beef up his security.

In addition to this, Masondo says he tries to stick to encrypted communication platforms.

While his work continues, Masondo has expressed a concern of heightened threats to journalists, from corrupt officials to fake Twitter bots. If the environment doesn't change, he says, "we will get a situation where journalists are being shot in this country."

In June 2017, he was awarded the Nat Nakasa Award for courageous reporting. Mokonyane is now Minister of Communications.

SABC 8

Suspect they were spied on as part of a dirty-tricks campaign

The SABC 8 are a group of journalists and editors at the public broadcaster who captured the public imagination when they spoke out against censorship and managerial interference under former SABC boss Hlaudi Motsoeneng in 2016. The eight (Busisiwe Ntuli, Foeta Krige, Jacques Steenkamp, Krivani Pillay, Lukhanyo Calata, Suna Venter, Thandeka Gqubule, and Vuyo Mvoko) were suspended, then fired, and later reinstated[16] after a public support campaign and a court ruling. Parliament's decision to set up a committee to investigate the crisis at the SABC drew them back into the public eye as several members appeared before the committee to testify about their experiences.

But both during their dismissal and even after their reinstatement, the SABC 8 were targeted in an escalating campaign of threats, harassment, abuse and eventually violence -– especially Suna Venter. Several members of the SABC 8 believe that their communications were being intercepted as part of this campaign.

16 Mvoko was the only member not reinstated, as he did not have the same labour protections as a contract worker. However he has since been appointed a news anchor at eNCA.

History of surveillance at the SABC

In the final years of Hlaudi Motsoeneng's tenure at the SABC, several signs emerged of State Security involvement at the public broadcaster which raised surveillance concerns:

- **January 2014:** then SABC chairperson Zandile Ellen Tshabalala reportedly warned staff in an editorial meeting that due to information leaks about conditions at the SABC, their communications may be intercepted by intelligence services.
- **August 2015:** SABC Durban staff complained to their union (Bemawu) that SSA officials had "instructed employees to leave their offices whereafter operators spent between two and three hours per office for a purpose unknown to the employees." According to the initial complaint, employees were threatened against discussing or reporting the incident. To date there has been no explanation of this incident.
- **December 2016:** Parliament's inquiry into the SABC learns that the SSA was hauled in to interrogate various senior staff after information about the SABC's financial crisis was reported in the media.
- **January 2017:** R2K reported to Parliament that recent changes to SABC manager-level contracts had added a 'surveillance' clause, whereby the employee was required to consent to the SABC intercepting their phone calls, emails and stored files.

The SABC's status as a public body and national key point has been invoked as the reason for State Security oversight in its security matters, including vetting of staff.

Intimidation and attacks

At the core of this was a constant stream of anonymous threatening SMSes which started during the SABC 8's court challenge and which continued throughout Parliament's inquiry. According to Foeta Krige, the timing of these messages suspiciously coincided with or seemed to respond to private discussions among the SABC 8 or behind-the-scenes events – leading to suspicions that their private communications were not secure.

For example, after Venter emailed the SABC 8's lawyers saying that Motsoeneng and former head of news Simon Tebele may have lied to Parliament, within two days she received an SMS that read: "GO WORK FOR FREEDOM FRONT AND SOLIDARITY. YOU ALREADY DO. YOU ARE POISON."

In another incident on 5 September 2016, the SABC 8's legal advisers sent the group an email advising them on what they needed to proceed with their Constitutional Court case. The same day Krige received an SMS telling him: "IF YOU GO AHEAD TOMORROW IT WILL BE YOUR LAST WARNING. YOU AND THE LITTLE GIRL ARE FOOLS. GOOD LUCK YOU'LL NEVER SEE…IT WILL BE TOO LATE. PASS ALICE LANE." Only later did Krige realise that 'Alice Lane' was the office address of the group's attorney Aslam Mosajee, suggesting that the sender was privy to their discussions.

The messages continued, and were eventually joined by suspicious break-ins and violent attacks. In October 2016, Venter's flat was broken into and trashed. On the same weekend there were also break-ins at the house of fellow SABC 8 member Busisiwe Ntuli, and at a property in Auckland Park belonging to Krige and registered in his wife's name.

At one point, on her way home after meeting with another journalist about the SABC 8 case, she was shot at from behind a fence on the side of the road while stopped at an intersection. A week after the incident Venter received a message saying: NEXT TIME WE WON'T MISS.

In January 2017, Venter sent a document to Krige for checking – it was a submission to Parliament's SABC inquiry. As Krige recounts, "She sent it to me on a Saturday afternoon to check and two hours later she was shot in the face while she was on her way to a party in Sandton." The metal pellets had to be removed through surgery.

In perhaps the most horrifying incident, Venter was abducted by an unknown man who threatened to kill her and left her tied to a tree in Melville Koppies after setting the veld around her on fire. She managed to use her phone to contact Krige at around 4am, who came to her aid. According to Krige, police forensics found no fingerprints or other evidence on the scene.

Understandably, at this point Krige says Venter was under huge emotional strain. "Suna was part of our family towards the end – she would stay over if she was afraid or scared and she was also a good friend of my daughter," says Krige.

In the end Parliament's inquiry concluded its investigation and recommended most of the changes the SABC 8 had asked for. The group withdrew their court case and released a statement. Krige says they received their last message: "WHAT THE F**K? YOU LOST. STILL SCHEMING LIKE HEROES." After that the messages stopped.

Who was behind the campaign?

The police investigations into the intimidating messages yielded few results. While the police traced the messages, Krige says that "[whoever was responsible] were using 6 or 7 cellphones but by the time the police had gotten permission to trace, they had moved on to new phones. Initially I thought it was people at the SABC who wanted to protect Hlaudi but the more I think about it, it seems very professional." However he still suspects that pro-Motsoeneng elements within the SABC were responsible for passing information on to the perpetrators of the intimidation tactics.

Krige says one possible reason why Venter was subjected to so much more abuse than her colleagues was because she was the youngest and that she acted as a liaison between the SABC 8 and their lawyers. "If anyone were intercepting our communications it would look like she was the main means of communication," says Krige. "When they held the portfolio committee hearings she was the one who would go and get the Hansards [Parliamentary transcripts] and sit on weekends transcribing everything to get evidence related to our case – she was just that sort of person."

Suna's death

On 29 June 2017 Suna Venter was found dead in her flat. Media reports noted her cause of death as "broken heart syndrome" -- it is presumed her condition was exacerbated by the stress of the preceding year. She was 32 years old.

While Krige continues to work for the SABC he is bitter about Venter's death. "She died for f**k-all," he says. But he does emphasise that things changed at the SABC. "Make no mistake – the toxic environment of fear has gone and people debate and differ and in that sense the SABC 8 did a tremendous job and Suna was part of that," says Krige.

Under a new board, Hlaudi Motsoeneng has been dismissed along with a number of other senior executives. In September 2017, the Labour Court ordered Motsoeneng along with former head of news Simon Tebele to pay the SABC 8's legal costs.

To date nobody has admitted involvement in the attacks on the SABC 8.

The Inspector General of Intelligence, Dr Dintwe, is investigating whether any intelligence structures were involved in surveillance or illegal operations against the SABC 8. At the time of this report (May 2018), the outcome of that investigation is still pending.

Recommendations

The case studies in this publication offer a snapshot of some of the major *detected* surveillance threats that journalists face. There are likely other spying practices that have not been documented in here. However, based on the experiences of the journalists here, a few basic recommendations present themselves.

1. Reforms to RICA

It is clear that South Africa's surveillance law, RICA, has failed in several ways to protect journalists' communications - along with the communications of the general public. In April 2016, Right2Know tabled a set of demands for surveillance reform with the Department of Justice and Constitutional Development that was co-signed by 40 civil society organisations[17]. Several of these demands are of special importance to addressing the weaknesses in RICA that have put the journalists in this publication at risk:

- **Greater transparency within RICA, including 'user notification'** (whereby anyone who has been targeted for surveillance is eventually notified once any investigation against them is concluded). In all the case studies documented here, the journalist who was spied on only found out about it through accident, coincidence or via a confidential source – without which it would be impossible to get any recourse.
- **An end to the mandatory storing of users' metadata** (records of who you communicated with, your location, etc, which by law is currently stored for up to five years by service providers). This system creates a huge vulnerability for journalists and their sources.
- **An end to SIM card registration** (RICAing your SIM card and communication channels to your identity). SIM card registration prevents anonymous communication but is easily circumvented by criminals, so it is mainly law-abiding citizens who are subject to RICA data collection and storage. There is no convincing evidence that this policy has improved the state's crime-fighting capacity.

---

17 "Memorandum to Department of Justice: Demands to Stand Against Surveillance and Fix RICA", 26 April 2016: https://r2k.org.za/rica-memo

- **Closing the section 205 'loophole'** (which allows law enforcement to bypass the RICA judge and go to any magistrate if the intercept is for call records and metadata rather than the content of messages and calls themselves). This has created a parallel process for surveillance with even less oversight and protections than RICA.
- **An end to mass surveillance** (the bulk collection of communication/signals that is not targeted to specific individuals who are under investigation). The activities of the National Communications Centre must be strictly regulated through RICA and all mass surveillance must end.

2. Fixing the spooks

It is beyond urgent that South Africa essentially rebuilds its intelligence structures from the ground up, in particular the State Security Agency and the police's Crime Intelligence Division.

In May 2018, President Cyril Ramaphosa announced a panel to review the structures and activities of the intelligence structures.

A roadmap for this already exists, in the report of the Matthews Commission – an official inquiry set up in the mid 2000s by former Minister of Intelligence Ronnie Kasrils to investigate the activities and legal mandate of South Africa's main intelligence structures. The Commission's report, completed in 2008, found far-reaching problems with the intelligence structures and made comprehensive recommendations to address them. Unfortunately, the state has refused to engage with the Matthews Commission report on a technicality – Kasrils stepped down when Mbeki was recalled as President, and the report was never tabled in Cabinet. Therefore, government officials simply refuse to recognise its findings, saying the document has "no status"[18].

The recommendations of the Matthews Commission report, which became public in 2008, include:

- Narrowing the spooks' mandate to prevent them from taking an inappropriate interest in "lawful political and social activities".

---

18 The Matthews Commission Report, 2008: https://www.r2k.org.za/matthews-commission

- Laying down mandatory transparency measures in the intelligence structures, which operate with secrecy that goes far beyond what is necessary or justifiable to protect legitimate national-security secrets.
- Strengthening the transparency and institutional independence of the oversight systems, including the Inspector General of Intelligence and Parliament's intelligence committee.
- Urgent legal reforms to curtail the intelligence agencies' spying abuses, including its unregulated mass-surveillance programme at the National Communications Centre (NCC) – which the Commission found to be 'unlawful and unconstitutional'.

In particular, it is clear that in at least several cases, the intelligence structures have targeted journalists for surveillance in order to identify their sources. In the case of Sam Sole, and possibly Jacques Pauw, this appears to have been the declared objective of the operation, which the RICA judge has signed off on knowingly. This practice is a serious abuse of power and has grave implications for the protection of whistleblowers. It must end immediately.

It is clear that journalists will always be at risk of being spied on until state security structures stop thinking that spying on them is part of the job.

3. Protection for SABC workers

Journalists at the public broadcaster face a unique threat to their privacy, in that they are also civil servants working for a public institution. While other journalists may face 'external' threats, at the SABC it appears that the state intelligence structures were essentially invited in by management, as part of the SSA's mandate to offer various support services to other organs of state – especially to do 'vetting' of staff and contractors.

In terms of the National Strategic Intelligence Act, this includes gathering "departmental intelligence" for any state department, and vetting of all staff at any government department, and staff and contractors at national key points. During a 'security vetting', SSA operatives can interview the subject's family and acquaintances, access their bank statements, and even subject them to a polygraph test or intercept their communication (as long as the interception is in line with RICA). Such invasive measures are surely a threat to any journalist's sources.

The full range of the SSA's activities at the SABC have yet to be revealed, but we at least know that in the past the SSA was brought in to investigate 'leaks' to other media about the crisis at the SABC, that the SABC management asserted its legal right to intercept employees' communications, and that the SABC management regularly invoked the institution's special status under the National Key Points Act to justify invasive measures against its employees.

The risk of abuse of 'vetting' processes, and institutions' repeated abuse of their 'National Key Points' status, are a general point of concern. However, when it comes to the SABC in particular, it is clear that urgent measures are needed specifically to protect journalists from harassment, intimidation and interception.

- The SABC management must table a clear policy on vetting that protects editorial staff or any non-security staff member from vetting.
- Parliament should draft protections against abusive vetting into law. In a joint submission to Parliament on legislation to replace the National Key Points, SANEF and the SOS public broadcasting coalition called for the law to give explicit protection from vetting to SABC editorial staff.[19]

4. Newsroom protections

There may sometimes be a tendency for journalists and their organisations to downplay the threat of spying as an occupational nuisance rather than a legitimate threat. While individual journalists do often take steps to protect their privacy (for example, by adopting better digital security) the collective response of media organisations has sometimes been slow and inconsistent.

- **Security:** Newsrooms should undergo organisational processes to strengthen information security, including network security. These processes need buy-in at every level of the organisation, from reporters up to management.
- **Complaints procedures:** When there is evidence or a reasonable suspicion of abuse on the part of intelligence structures, this should form the basis of a complaint to the Inspector General of Intelligence. Where a case exists for criminal charges, a charge should be laid with the police.

---

19 "Written Submission on the Critical Infrastructure Protection Bill", 13 March 2018: https://pmg.org.za/files/180314SANEF_SOS_and_MMA.pdf

- **Fundraising for digital and legal defences:** To become resilient to surveillance takes time and money. In the same way that many media organisations have sought to raise funds for investigative capacity, they may also need to marshal more resources to protect against these abuses.

5. Service providers

Mobile network providers such as MTN, Vodacom, Cell C, and Telkom, as well as internet service providers, have allowed themselves to be caught in a legal trap where they must cooperate with a system of surveillance that they know is being abused. These companies are legally bound to assist in state surveillance of their customers (on provision of a warrant). However, there are steps that service providers can take to push back against abusive surveillance

- **Transparency:** While RICA forbids service providers from notifying a user if they have been targeted for interception, there is no ban on disclosing general statistics on interceptions. Service providers should publish annual transparency reports disclosing the number of interceptions on their networks.
- **RICA reforms:** Service providers should be actively lobbying for legislative reforms to RICA that will protect their customers' privacy.
- **Resisting abusive surveillance:** In the US and Europe, certain tech companies and service providers have shown that they are willing to use the courts to protect their customers' privacy against invasive government surveillance. South African companies have yet to show such willingness. Yet there is sufficient evidence of abuse that companies need to closely scrutinise law enforcement requests for interception assistance. Where there is a risk of abusive surveillance, the company should be willing to go to court rather than be forced to comply with a dodgy surveillance request.
- **Protect journalists:** Given that the companies know that certain customers such as journalists are being targeted unlawfully through RICA, they should be willing to fight for the right to disclose to such customers that their communication has been intercepted. This is especially true of the 'section 2015' warrants: While RICA forbids the service providers from telling a customer if there is a RICA warrant against them, this provision

does not extend to section 205 warrants. Every service provider should have an established channel of communication with SANEF through which journalists can request confirmation of whether or not their data has been intercepted over the network.

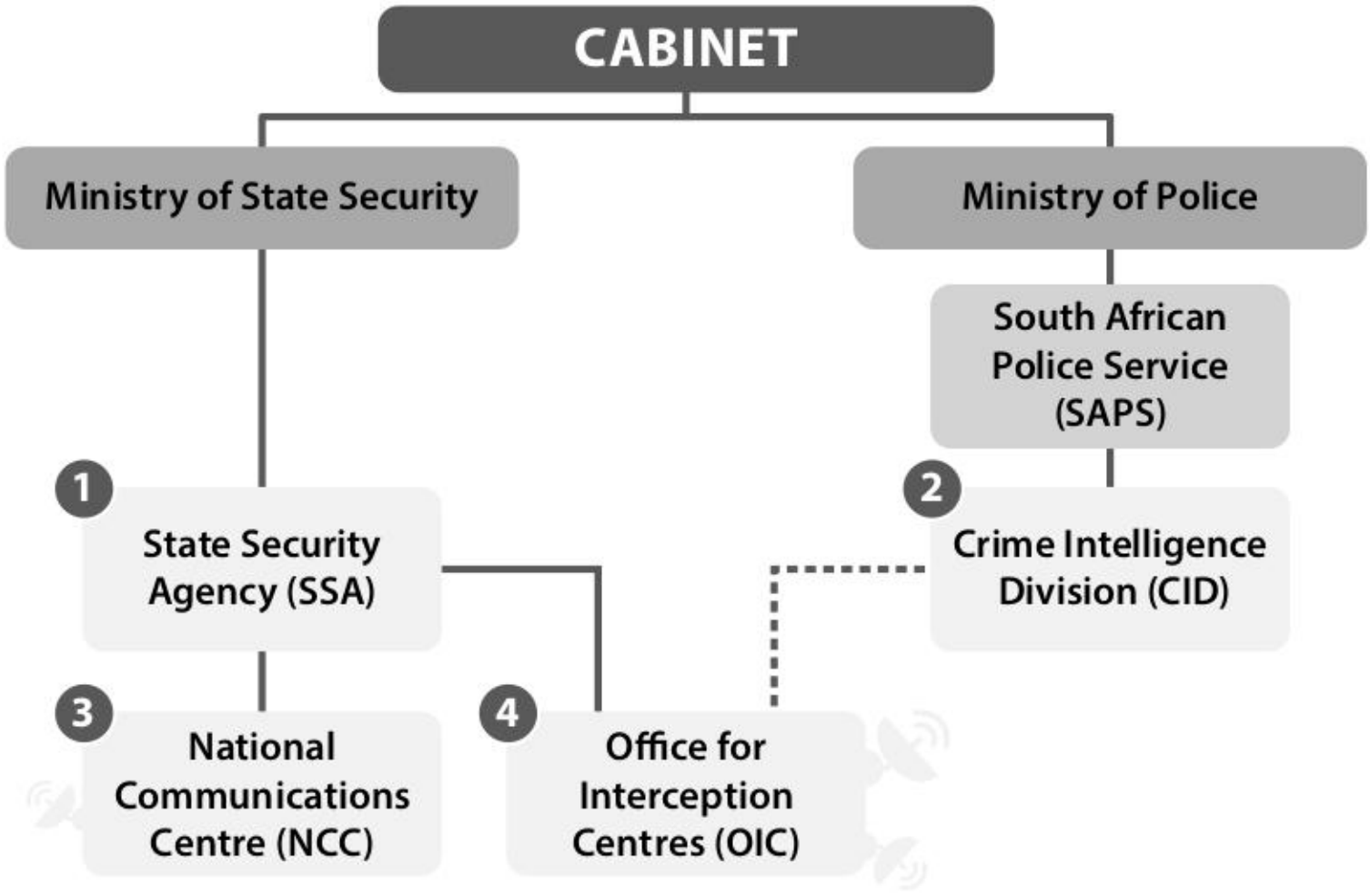
- **Coming clean:** Cases like those of Peter Bruce and Rob Rose (where an MTN employee assisted in illegal surveillance) underscore that companies themselves do not have sufficient internal protections against abuse. The service providers should disclose what security measures are in place to protect people's personal information such as their metadata, how many people have access to that information, and what protections there are against misuse of that information.

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

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 State Security Agency (SSA)** is government's primary intelligence agency. It is responsible for identifying and monitoring a wide range of threats to national 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).

2 **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.

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.

3 The **National Communication Centre (NCC)** is an additional surveilalnce facility that reportedly conducts mass or bulk 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 not properly regulated by RICA.

4 The **Office for Interception Centres (OIC)** was established in terms of RICA and reports to the Minister for State Security. The OIC is tasked with providing communications interception for law enforcement agencies.

This is a report by the Right2Know Campaign on surveillance of journalists in South Africa.

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. 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!

Follow R2K on social media and help spread the word:

Facebook | Twitter | Instagram: @r2kcampaign

#StopTheSpies #OngaziMakazi

Find this report online at r2k.org.za/spooked

WWW.R2K.ORG.ZA