GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

SOUTH AFRICA

Communications surveillance in South Africa:
The case of the Sunday Times newspaper

Department of Journalism, Film and Television, University of Johannesburg
Jane Duncan
www.uj.ac.za

Introduction

This article discusses the communications surveillance of two investigative journalists from the biggest weekend newspaper in South Africa, the *Sunday Times*. The paper is owned by one of the four largest press groups, Times Media Limited. The journalists, Stephan Hofstätter and Mzilikazi wa Afrika, had their communications intercepted by the Crime Intelligence Division of the South African Police Service (SAPS), in order to disrupt their work as journalists and uncover their sources. This story has been chosen as a case study of just how corruptible South Africa's communications monitoring and interception capacities are, in spite of the government claiming that it offers all the necessary protections for civil liberties.

The revelations by former National Security Agency (NSA) contractor Edward Snowden – that the NSA was conducting mass surveillance of US citizens, as well as political leaders such as German Chancellor Angela Merkel – have created a serious international controversy. Other countries have also been exposed as conducting mass surveillance too, and many people in South African civil society and the media have been concerned that the country's authorities may be doing the same. This report examines one case where clear proof emerged of abuses, and what the case tells us about the state of civil liberties in relation to communications networks.

Policy and political background

South Africa is not a terrorist target, yet growing social protests mean that the temptation is there for less principled members of the security apparatus to abuse the state's surveillance capabilities to advantage the faction currently in control of the ruling African National Congress (ANC) and disadvantage their perceived detractors. South Africa has some excellent investigative journalism teams, and the state could easily misuse its surveillance capabilities to harass them and expose their confidential sources of information, especially if they threaten ruling interests.

South Africa has a law that governs the surveillance of domestic communications on both criminal justice and national security matters, the Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA). RICA forbids the interception of communications without the permission of a designated judge, and sets out the conditions for the granting of interception directions. According to the Act, interception directions should be granted only if there are reasonable grounds to believe that a criminal offence has been or is being or probably will be committed.[1] The Act also requires all South Africans to register their subscriber information management (SIM) cards with their mobile phone providers, so that the state can track the activities of suspected criminals or victims if they need to.[2]

In spite of the fact that RICA attempted to strike the correct balance between the interests of justice and national security on the one hand, and civil liberties on the other, the Act has insufficient guarantees for civil liberties online. It ignores many of the most basic protections set out in the recently released Application of Human Rights Principles to Communications Surveillance, otherwise known as the Necessary and Proportionate Principles.[3]

An added problem is that foreign signals intelligence gathering does not fall under RICA, which means that this practice is unregulated by law. This is particularly worrying as the state's bulk monitoring capacity is held by the interception centre that undertakes foreign signals intelligence; so the state agency with the greatest capacity for mass surveillance is also the one that is least regulated by law.

In 2005, the state's mass surveillance capacity was misused to spy on perceived opponents of the then contender for the presidency, Jacob Zuma. Several politicians and activists have also alleged

1 Section 5(a)(i), Regulation of Interception of Communications and Provision of Communications-Related Information Act, www.justice.gov.za/legislation/acts/2002-070.pdf

2 Section 39, Regulation of Interception of Communications and Provision of Communications-Related Information Act. www.justice.gov.za/legislation/acts/2002-070.pdf

3 en.necessaryandproportionate.org/text

that their communications are being surveilled, although it is difficult to say whether this is the case. Another weekly newspaper, the *Mail & Guardian,* has quoted sources inside the police and State Security Agency (SSA) alleging that security personnel often do not even bother obtaining directions to intercept communications.[4] These incidents and allegations arise from the fact that there are systemic weaknesses in the country's communications surveillance regime, which predispose it to abuse.

The *Sunday Times* case

Hofstätter and wa Afrika are part of an award-winning investigative journalism team at the *Sunday Times*. They have been responsible for some of the most important stories exposing government corruption and malfeasance, and as a result have earned the ire of some government officials who would prefer to keep their dark secrets just that.

The journalists were responsible for a story that saw South Africa's top cop, National Police Commissioner Bheki Cele, being fired by the president in 2012 for dishonesty, unlawfulness and mismanagement in concluding a lease deal for offices for SAPS in the capital city of Pretoria and in Durban. The deal was concluded with businessman Roux Shabangu, who was close to President Jacob Zuma. Their stories exposed how Cele had broken treasury rules to advantage an associate of Zuma's financially.

The team also investigated allegations of corruption against Cele when he was the member of the executive council (MEC) responsible for transport, safety and security in the KwaZulu-Natal province of South Africa. Moreover, they published damning exposés of the serious and violent crimes unit of SAPS in the township of Cato Manor, which they claimed turned rogue by operating a "death squad" and killing suspects. The police members alleged to have been involved still have to stand trial.

As they deal with extremely sensitive stories, Hofstätter and wa Afrika must do their utmost to protect their sources, including those located inside the police. In an attempt to do just that, they carry two phones: one with a SIM card that has been registered in terms of RICA and one with a card that has been registered by someone other than themselves. "Pre-RICA'd" SIM cards – SIM cards that are registered before they are bought – can be bought fairly easily in South Africa, and cannot be traced back to their users as they are not registered in their names. They use the first for non-sensitive communications and the second for sensitive communications with confidential sources, assuming that communications using pre-RICA'd SIM cards will be impossible to trace back to their sources.

Wa Afrika had a sinister run-in with the authorities in 2010, when his communications were intercepted by the police on the pretext that he was suspected of gun running. The journalist had travelled in and out of the country several times on stories, and the police used this as "evidence" that he may well have been involved in crime. The existence of the interception direction was confirmed by the Inspector General of Intelligence, who also confirmed that the direction was lawful.[5] The vague and speculative grounds for the issuing of interception directions worked to the police's advantage, and they used this to pursue an investigation of a non-existent crime.

However, according to Hofstätter and wa Afrika, later in 2010, the police managed to obtain their pre-RICA'd numbers, and slipped them into a larger application for an interception direction for the designated judge, Joshua Khumalo, to approve. The police claimed that the numbers were of suspected members of a criminal syndicate, and the journalists' numbers were included under fictitious names. Oddly enough, the Police Commissioner's number was also included in the application, although Cele's number was subsequently cancelled.

Apparently the police obtained these numbers from one of their sources, who had decided to betray the journalists in return for a promotion.[6] The journalists learned these details from other sources. The bugging of their phones was confirmed by a Pietermaritzburg magistrate, who stated that the KwaZulu-Natal provincial crime intelligence chief had sent him as an emissary to apologise for the bugging. However, the chief has refused to be drawn into a discussion with the journalists directly.[7]

The *Sunday Times* has taken this case to court, and two officers are being charged with having violated RICA. The sanctions for having done so are stiff: any person intercepting communications unlawfully could be imprisoned for up to 10 years or fined up to ZAR 2 million (approximately USD 200,000). The journalists claim that they have not been involved in any crimes, and as a result there is no valid reason for the police to investigate them.[8]

4 Swart, H. (2011, October 14). Secret state: How the government spies on you. *Mail & Guardian*. mg.co.za/article/2011-10-14-secret-state

5 Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 March 2014.

6 Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 March 2014.

7 Affidavit by Stephan Hofstätter, 24 March 2012.

8 Affidavit by Stephan Hofstätter, 24 March 2012.

The only reason why they were placed under surveillance must be that they were being harassed for their investigations into the police, and that the police wanted to uncover their sources so that they could plug the leaks. In fact, in an affidavit for the case, one of the police officers on trial, Brian Padayachee, stated that he was given an instruction by a higher-ranking officer to undertake a covert investigation into the activities of certain journalists that, it was claimed, posed a threat to the organisation. This investigation included the interception and monitoring of their calls.[9] Apparently, the ultimate instruction came from Cele, who was concerned that the journalists were attempting to infiltrate the police with an intention of tarnishing the image of the police; but, in a bizarre twist, this very direction that he had given the instruction for was used against him to place him under surveillance.

These incidents showed just how easy it is to intercept journalists' communications, or indeed the communications of any citizen who asks inconvenient questions about those in authority. There has been growing evidence of South Africa's security cluster – consisting of the police, the intelligence services and the military – becoming increasingly powerful and unaccountable. Unless the state's surveillance capacities are regulated properly, then abuses for political reasons are likely to continue. As Hofstätter noted, "...there is a complete free-for-all for the intelligence services to intercept whatever they want. They just come up with spurious grounds. There is a time-honoured practice to circumvent RICA, and all they do is just slip the numbers in."[10]

Analysis and conclusion

The *Sunday Times* case reveals several systemic weaknesses in the regulation of communications interception in South Africa. One of the most serious weaknesses is that no one is even informed that their communications have been intercepted, even after the investigation is complete. This means that the authorities are given a power that is, to all intents and purposes, hidden from the public eye. This violates the requirement in the Necessary and Proportionate Principles that individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation.[11] Needless to say, this principle should apply only if there is no risk to the purpose of surveillance, in which case *post facto* notification is appropriate.

In the United States' system, in order to protect the rights of the people under surveillance in criminal matters, within 90 days of the termination of the court order the judge must ensure that the person whose communications were intercepted is informed about the order.[12] The fact that a similar provision does not exist in RICA lays it wide open to abuse, as the authorities can rest assured that their abuses will most probably never come to light. The only reason why the *Sunday Times* learned of the abuse was because they have extensive contacts within the police; sources of information that would generally not be available to ordinary citizens.[13]

Another problem this case highlights is the speculative nature of the grounds for issuing interception directions using RICA. Privacy International has argued that the grounds are too vague, and that the higher standard of "probable cause" or a similar level of finding is generally required for a judge to issue an interception direction.[14] Directions may also be issued in relation to serious offences that may be committed in future, which may not be constitutional as it allows law enforcement officers to speculate on future acts that have not yet occurred.[15]

Furthermore, the granting of directions is an inherently one-sided process, which means that the judge has to take the information that is given to him on trust. No ombudsman is present to represent users' interests; as a result, the process lacks an adversarial component, which also predisposes it to abuse.

The level of information provided by the designated judge that is eventually released is inadequate. The annual report provides bare details about the number of applications for interception directions, the state agency that made the applications and the number that were granted or refused.

9 Affidavit by Brian Padayachee, 14 March 2012.

10 Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 March 2014.

11 International Principles on the Application of Human Rights to Communications Surveillance. en.necessaryandproportionate.org/text

12 US Code § 2518 - Procedure for interception of wire, oral, or electronic communications. www.law.cornell.edu/uscode/text/18/2518

13 Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 May 2014.

14 Privacy International. (2001). Submission to the Parliamentary Committee on Justice and Constitutional Development, 14 August.

15 Bawa, N. (2006). The Regulation of Interception of Communications and Provision of Communications Related Information Act. In L. Thornton, Y. Carrim, P. Mthsaulana, & P. Reburn (Eds.), *Telecommunications Law in South Africa*. www.wits.ac.za/academic/clm/link/publications/22988/telecommunications_law_in_south_africa.html

The judge may also include some general comments on trends. No information is available in these reports on the number of interceptions that actually result in arrests and convictions. For instance, insufficient information was provided to understand why there was a huge 231% increase in the number of interception directions granted by the designated judge to Crime Intelligence between 2009 and 2010, the year that Hofstätter and wa Afrika's communications were intercepted.[16]

Furthermore, other democracies have established independent commissions to oversee all monitoring and interception activities. Such commissions undertake full and public reporting processes, with the most sensitive areas being removed. Yet in South Africa, the parliamentary reports are written by the very judge who took the decisions, which is not healthy as the judge is unlikely to reflect adequately on the weaknesses of his or her own decisions.

South Africa's Act also does not recognise the right of journalists to protect their sources of information, either in the form of express provisions in the Act or in the form of a protocol that law enforcement or intelligence officials are required to adhere to in investigating journalists.

All these problems make for an Act that is not human rights-compliant, and is likely to continue being abused unless safeguards are introduced.

Action steps

In 2014, the Department of State Security will launch a review of intelligence policy, to assess the strengths and weaknesses of all national security-related policies. The Department of Communications has also launched a review of ICT policy and legislation. Civil society needs to present researched alternatives to the existing communications surveillance regimes that enhance respect for basic rights and freedoms. Particular emphasis should be placed on ensuring that the regime conforms to the Necessary and Proportionate Principles and that these principles are domesticated in South African surveillance policy and practice.

These advocacy efforts should focus particularly on the following areas:

- Strengthening the grounds for the issuing of interception directions in RICA.
- Increasing transparency in reporting levels on communications surveillance practices.
- Ensuring that a user-notification provision is inserted into RICA.
- Ensuring independent oversight over the process of issuing interception directions.
- Implementing a protocol with respect to the surveillance of journalists' communications, setting out the circumstances in which such interceptions can take place, and the procedures.
- Including a provision in RICA for an ombudsman to represent users and the public interest when applications for interception directions are made.

16 Khumalo, J. A. M. (2010). Statistical briefing by designated judge for the period 1 April 2009 to 31 April 2010, p. 3-4.