

**IN THE HIGH COURT OF SOUTH AFRICA  
(GAUTENG DIVISION, PRETORIA)**

**Case no: 25978/17**

**RIGHT2KNOW CAMPAIGN**

1<sup>st</sup> Applicant

**PRIVACY INTERNATIONAL**

2<sup>nd</sup> Applicant

*(In the application for admission as amici curiae)*

In re

The matter between:

**AMABHUNGANE CENTRE FOR INVESTIGATIVE  
JOURNALISM NPC**

1<sup>st</sup> Applicant

**SOLE STEPHEN PATRIC**

2<sup>nd</sup> Applicant

and

**MINISTER OF JUSTICE AND CORRECTIONAL  
SERVICES**

1<sup>st</sup> Respondent

**MINISTER OF STATE SECURITY**

2<sup>nd</sup> Respondent

**MINISTER OF COMMUNICATIONS**

3<sup>rd</sup> Respondent

**MINISTER OF DEFENCE AND MILITARY VETERANS**

4<sup>th</sup> Respondent

**MINISTER OF POLICE**

5<sup>th</sup> Respondent

**THE OFFICE OF INSPECTOR-GENERAL  
OF INTELLIGENCE**

6<sup>th</sup> Respondent

**THE OFFICE FOR INTERCEPTION CENTRES**

7<sup>th</sup> Respondent

**THE NATIONAL COMMUNICATIONS CENTRE**

8<sup>th</sup> Respondent

**THE JOINT STANDING COMMITTEE ON INTELLIGENCE**

9<sup>th</sup> Respondent

**THE STATE SECURITY AGENCY**

10<sup>th</sup> Respondent

---

**FOUNDING AFFIDAVIT**

---

I, the undersigned

**MURRAY HUNTER**

state under oath as follows:

1. I am an adult male and employed as the Secrecy Organiser of the Right2Know Campaign (**R2K**). R2K's offices are at 1st Floor Community House, 41 Salt River Road, Salt River, Cape Town, 7925.
2. I am duly authorised to depose to this affidavit on R2K's behalf.
3. This application is also brought by the Second Applicant, Privacy International (**PI**). A confirmatory affidavit of Scarlet Kim, Legal Officer at PI will be filed as part of this application.
4. The facts contained herein are to the best of my knowledge true and correct and, unless otherwise stated or indicated in the context, are within my personal knowledge. Where I make legal submissions, I do so on the advice of the applicants' legal representatives.

   
 MH

## I NATURE OF THE APPLICATION

5. This is an application in terms of Rule 16A of the Uniform Rules of the Court for the admission of R2K and PI as *amici curiae* in the matters instituted under case number 25978/17.
6. The main application concerns the constitutionality of the Regulation of Interception of Communications and Provisions of Communication – Related Information Act 70 of 2002 (**RICA or the Act**). The first category consists of flaws regarding the insufficient and unconstitutional manner in which RICA regulates issues that are covered by the Act. The second category of constitutional deficiencies relates to aspects in which RICA is under-inclusive, because it does not regulate the particular issues at all.
7. In light of the extensive work that R2K and PI have engaged in relating to surveillance and the security agencies, they are in a position to assist the court by making submissions particularly in relation to:
  - 7.1 The importance of post-interception notification to the subjects of surveillance as demonstrated in foreign and international jurisprudence;
  - 7.2 The unconstitutionality of the mandatory blanket retention of communication related data (metadata);
  - 7.3 That the designated judge is not sufficiently independent in line with international best practice, that the lack of independence violates the right

to privacy, and that the secrecy under which the judge operates enhances the need for independence; and

7.4 That mass surveillance of “foreign” signals conducted by the National Communications Centre is an unjustifiable limitation of the right to privacy.

8. In what follows, I deal with the following issues:

8.1. R2K and PI’s interest in these proceedings;

8.2. The scope of R2K and PI’s application for admission and the legal submissions they seek to advance; and

8.3. The procedural requirements for admission.

## **II R2K AND PI’S INTEREST IN THE MAIN APPLICATION**

9. In this Part, I describe R2K’s and PI’s interest in the main matter. My statements about PI are confirmed by Scarlet Kim in the confirmatory affidavit.

### **R2K**

10. R2K is a national movement centred on freedom of expression and access to information. It is a democratic, activist-driven campaign that strengthens and unites citizens to raise public awareness, mobilise communities and undertake research and targeted advocacy that aims to ensure the free flow of information necessary to meet people’s social, economic, political and ecological needs and live free from want, in equality and in dignity. In this regard R2K mobilises on four main issues:

- 9.1 To stop secrecy, in particular to ensure that security legislation and the conduct of security agencies are aligned with the Constitution of the Republic of South Africa, 1996 and its underlying values;
  - 9.2 Information access, in particular to ensure that public and private sector information is easily accessible to citizens and that people with information of wrongdoing and/or of the suppression of information in the public interest are free and encouraged to share information with the public;
  - 9.3 Communication rights, in particular to ensure that South Africa enjoys full freedom of expression and a free and diverse range of public, private and non-profit media and affordable access to the open and secure internet and telecommunications. This includes opposition to unconstitutional and unlawful surveillance; and
  - 9.4 Freedom of assembly and the right to protest, in particular to ensure that South Africa has an enabling environment for those who seek to participate in various forms of protest without harassment.
11. R2K has a long track record of opposing the current surveillance regime.
  12. On 30 March 2016, the United Nations Human Rights Committee released its review of South Africa's human rights record, in connection with the International Covenant on Civil and Political Rights. Responding to submissions made jointly by the Right2Know Campaign, PI, and the Association for Progressive Communications (APC), 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, which leaves the most powerful surveillance capacities of the state effectively unregulated. It also noted with concern that the grounds for the issuing of warrants authorising the interception of communications are too vague, and the state's system for interception of communications lacks transparency and accountability. All these problems make it more likely that the surveillance capacities of the state will be abused. I attach copies of the submission made by R2K, PI and APC marked **MH1**. The report of the Committee is attached to the Applicants' papers as annexure **MH2**.

13. In response, led by R2K, 40 civil society and social justice organisations released a joint demand for an end to surveillance abuses. The demand was delivered to Parliament on 26 April 2016. Among these demands were that there should no longer be mandatory SIM card registration or blanket data retention (i.e. communication providers should not be allowed or forced to store the sensitive communications data of their users for years), RICA must be reformed to be more transparent, with more accountability and oversight, and that there should no longer be mass surveillance. I attach a copy of this demand marked **MH3**.
14. R2K and its members have also made numerous public statements and given numerous interviews around surveillance. These can be accessed at <https://www.r2k.org.za/category/security-state/>. It has also prepared publications to provide the public with information about surveillance and their rights under RICA.

15. R2K also has knowledge of and experience in litigating on the right to know more generally:
- 15.1. In *Right2Know Campaign and Another v Minister of Police and Another* [2014] ZAGPJHC 343; [2015] 1 All SA 367 (GJ), R2K brought a successful application to compel the release of the list of national key points;
- 15.2. In *City of Cape Town v South African National Roads Authority Limited and Others* [2015] ZASCA 58; 2015 (3) SA 386 (SCA), R2K was one of several civil society organisations that intervened as *amici curiae* in a matter concerning access to court records; and
- 15.3. The most recent example of R2K's litigation is *Primedia Broadcasting v Speaker of the National Assembly* [2016] ZASCA 142; 2017 (1) SA 572 (SCA) where R2K was one of the successful applicants challenging limits on broadcasting parliamentary proceedings and the use of a signal jamming device in Parliament.
16. The subject-area of this matter falls squarely within R2K's interest. I submit that R2K is well-placed to make legal submissions, and to be of assistance to this Court in the important constitutional and public interest issues that are at stake.
17. In addition to the activity described above, R2K is currently preparing its own challenge to aspects of RICA that have not been directly challenged in this application. It intends to launch that application in 2018. I discuss that application in more detail below when it relates to elements of the present application.

### Privacy International

18. Established in 1990, Privacy International is a non-profit, non-governmental organization based in London, the United Kingdom, which defends the right to privacy around the world. Privacy International conducts research and investigations into government and corporate surveillance activities with a focus on the policies and technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of Colombia, South Korea, the United States, the UK, and Europe, including the Court of Justice of the European Union (**CJEU**) and the European Court of Human Rights (**ECtHR**).
19. Privacy International contributes regularly to the activities of United Nations human rights bodies, such as the UN Human Rights Committee, the Universal Periodic Review, and UN special procedures. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional, and international laws that protect this fundamental right. As a part of this mission, Privacy International works with various partner organizations across the world to identify and address threats to privacy.
20. Privacy International has litigated several cases addressing issues central to the main application. In particular, Privacy International is one of the applicants in *10 Human Rights Organisations v United Kingdom*, a case currently before the ECtHR, challenging two aspects of the UK's surveillance regime: (1) mass interception of internet traffic transiting undersea fibre-optic cables landing in the UK and (2) UK access to the information gathered by the US through its various



mass surveillance programs. Our co-applicants are the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, and Liberty. Privacy International's central claims in this case are that both programs violate arts 8 and 10 of the European Convention on Human Rights, which respectively protect the right to privacy and the right to freedom of expression.

21. Privacy International, together with Open Rights Group, also intervened in the case of *Secretary of State for the Home Department v Tom Watson and Others*, which was decided by the CJEU in 2016 (jointly with *Tele2 Sverige AB v. Post- Och telestyrelsen*). Those cases involved respective challenges to the UK and Swedish national data retention regimes, which mandated telecommunications companies retain the communications data (or metadata) of their users. Its intervention argued that a requirement for the blanket retention of communications data violated arts 7 and 8 of the Charter of Fundamental Rights of the European Union, which respectively protect the right to privacy and the right to data protection. In its decision, the CJEU held that the Charter must be interpreted as precluding "national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication." (*Tele2 Sverige AB v. Post- Och telestyrelsen*; *Secretary of State for the Home Department v. Tom Watson et. al.* (C-698/16) [2016] EUECJ C-203/15 at para 134.)

22. Based on its commitment to privacy and human rights, Privacy International has a strong interest in this matter. Its legal expertise and experience with the subject matter of the main application make Privacy International well-placed to make legal submissions and to assist the Court in understanding the fundamental rights and public interest issues at stake.

### III LEGAL SUBMISSIONS

23. In terms of Rule 16A (6)(b) the *amicus* applicant is required to set out clearly and succinctly the submissions which it will advance should it be admitted as *amicus curiae*. Against this background, R2K and PI intend to advance submissions on the following challenges raised by the Applicants:

- 23.1. Notification of interception;
- 23.2. Mandatory blanket retention of metadata;
- 23.3. The independence of the designated judge; and
- 23.4. Bulk surveillance.

#### **Notification of Interception**

24. The Applicants argue that various provisions of RICA are unconstitutional because they do not provide a default rule that the subjects of interception orders should be notified of the decision. Instead, RICA unconstitutionally creates an absolute rule

of secrecy that subjects will never be notified, even at a point where notification would cause no harm to the investigation.

25. R2K and PI fully support the Applicants' argument. The complete ban on subject notification can never be justified. There are certainly instances where it would be justifiable to delay notification while an investigation is ongoing. However, the state should have to demonstrate to an independent judicial authority that delay is necessary in order not to undermine the purpose of the interception, and the delay should last only for as long as those reasons subsist.

26. R2K and PI seek leave to advance three further submissions:

26.1. The absence of notification violates s 38 of the Constitution;

26.2. Comparative law and practice support the need for appropriate notification;  
and

26.3. International law also supports the need for appropriate notification.

27. First, the Applicants argue that the absence of notification is arbitrary and violates the right to privacy and the right of access to court (and the special rights applicable to lawyers and journalists). We agree. But the absence of notification also violates s 38 of the Constitution. That provision affords all persons "*the right to approach a competent court, alleging that a right in the Bill of Rights has been infringed or threatened, and the court may grant appropriate relief, including a declaration of*

*rights.*" This is what is known in international law as the right to an effective remedy.

28. In the context of interception of communications, this seems to be the most relevant right:

28.1. While s 34 protects the right to approach a court to resolve any legal dispute, s 38 provides special protections for allegations of rights violations.

28.2. The point of notification is to determine the existence of an *allegation* that a right has been violated. It may be that there is no violation of the right to privacy. Section 38 is about ensuring that those questions are determined by courts. That can only happen if there is notification.

28.3. Section 38 expressly recognises a declaration of rights as an appropriate remedy. As the Applicants acknowledge, in many instances that will be the only available remedy when the interception has been completed at the time of notification.

28.4. International law treats the absence of notification as a necessary safeguard of the right to privacy and one that is closely tied to the right to an effective remedy.

29. For these reasons, R2K and PI will argue that RICA also violates s 38 of the Constitution.

30. Second, R2K and PI have conducted an analysis of various countries' laws on subject notification. The analysis demonstrates that the majority of comparable countries require subject notification. The countries vary in terms of the details of when notification is required, the standard for notification, and how the decision is made. But they share the common themes identified by the Applicants: (a) the subject must be notified either before or after the surveillance unless it will threaten the purpose of interception; and (b) the decision whether to notify or not is overseen by an independent authority.
31. This analysis is important for several reasons:
- 31.1. In interpreting the Bill of Rights, this court may consider foreign law (s 39(1)(c) of the Constitution). In particular, in assessing whether a limitation of a right is justifiable in terms of s 36(1) of the Constitution the court must consider what is reasonable in an "*open and democratic society*". A consideration of what other democratic societies do is obviously useful in that determination.
- 31.2. The First Respondent contends that RICA is in line with other foreign jurisdictions, particularly the United Kingdom, Canada, New Zealand, Australia and the European Union (Minister's AA at paras 49-54). It is not clear why the Minister only relied on these four jurisdictions. However, R2K will demonstrate in legal argument:

31.2.1. That Canada and New Zealand respectively require and permit notification when doing so would no longer threaten the purpose of the investigation;

31.2.2. That the European Court of Justice and the European Court of Human Rights have both recognized notification to constitute a critical safeguard when governments conduct surveillance; and

31.2.3. A broader survey of other countries in Europe, South America and Asia demonstrate a similar pattern. The following countries, for example, all have some notification provision: the Netherlands; Germany; Belgium; Austria; Ireland; the Czech Republic; Switzerland; Slovenia; Montenegro; Hungary; the United States of America; Japan; South Korea; Taiwan; and Chile.

32. Third, international law has increasingly recognised that notification is a fundamental safeguard to protect the right to privacy, the right to an effective remedy and the right to free expression. This position is evidenced by the findings of the UN Human Rights Committee, the UN High Commissioner for Human Rights, and the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. For example, the Special Rapporteur has written:

*"Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might*

*jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath."*

33. This Court is obliged to consider international law by s 39(1)(b) of the Constitution.
34. Fourth, it is noteworthy that the Agency Respondents appear to deliberately mischaracterise the Applicants' claim. They answer it by pointing out, correctly, that notification may undermine the purpose of interception. But the claim is limited precisely to those instances where notification will not have that effect. Moreover, there is no answer to why a default notification regime, with exceptions, would undermine the purpose of interception.
35. The Minister claims that even post-surveillance notification could interfere with investigations. This may be true in some instances. But it is no justification for an absolute prohibition on notification. Importantly, neither the Applicants nor R2K and PI seek to dictate what the notification regime should look like. They argue only that the existing regime prohibiting notification is unconstitutional. Pointing to some cases where even post-surveillance notification may hinder an investigation is no answer to the constitutional challenge. It is difficult to understand why the designated judge should be empowered to determine whether an interception order should be granted, but cannot be trusted to assess whether and when the subject can be notified.

36. Lastly, the Respondents all point to various safeguards in RICA that prevent abuse, and therefore presumably would ameliorate the need to review interception orders. But those arguments miss the point. No safeguards are perfect and there will always be errors or abuse. Prohibiting notification violates the right to approach a court to make the determination of whether or not there was an abuse. The widespread practice of multiple other jurisdictions and international law principles demonstrate that the Minister's concerns are misplaced.

#### **Mandatory Blanket Retention of Communication Related Information**

37. It is important to be clear about what is at stake here. The Government asserts that it has the power to mandate all telecommunications companies and internet service providers to store all metadata about most South Africans' phone calls, SMSs, emails, and other messaging services for up to five years. This includes the location from which those communications were made, and may, in some instances, also implicate the content of messages, such as the subject lines of emails. It also asserts the power to mandate internet service providers to capture and store metadata about South Africans' internet activity at all times, for no reason whatsoever.
38. This is a massive and systemic violation of the rights of all South Africans who use phones and computers.

39. In this section:



- 39.1. I explain how R2K and PI's position differs from the Applicants' and why it is relevant to this application; and
- 39.2. I set out the provisions of RICA that give rise to this extremely broad power; and
- 39.3. I explain why the mandatory retention of metadata is an unjustifiable violation of the right to privacy.

#### R2K's Position in this Litigation

40. R2K and PI take a stronger stance on the mandatory retention of metadata than the Applicants. The Applicants' attack is limited in two ways:

40.1. First, it is directed at s 30(2)(a)(iii) of RICA. Section 30(2)(a)(iii) is the provision that obliges the Minister to issue a directive to an electronic communication service provider. It assumes the validity of mandatory blanket retention of metadata, and regulates the details of how that will occur. The attack is not directed at s 30(1)(b) and the other provisions of RICA that create the obligation for mandatory blanket retention of communication-related information.

40.2. Second, the Applicants appear implicitly to challenge mandatory blanket retention of metadata. But the real focus of their attack appears to be:

40.2.1. The length of time for which metadata is stored;

40.2.2. The absence of oversight mechanisms for the stored metadata;  
and

40.2.3. The risk to journalists and legal professionals posed by  
mandatory blanket retention of metadata.

41. R2K and PI support the challenge on all three grounds. But we argue that, even if RICA limited the duration, provided oversight, and contained safeguards for lawyers and journalists, the mandatory blanket retention of metadata unjustifiably limits the right to privacy. Moreover, RICA is unconstitutional to the extent that it permits prosecutors to access archived communication-related information without any of the protections built-in to s 19 of RICA.

42. However, R2K and PI accept that, given that the Applicants' attack is limited to s 30(2)(a)(iii), it is not possible for this Court to grant the broader relief that R2K submits the Constitution requires. R2K is therefore preparing a separate application where it will challenge – amongst other unconstitutional elements of RICA – mandatory blanket retention of metadata.

43. For the purposes of this application, R2K's submission is limited to:

43.1. Providing the necessary background, absent from the current application,  
to show why the mandatory blanket retention of metadata is a violation of  
the right to privacy; and

43.2. Contending that, in deciding the narrow challenge, this Court should not decide it in a manner that closes the door for the broader challenge that R2K intends to bring.

The Nature of Mandatory Retention

44. The Applicants focus on the obligation in s 30(2)(a)(iii) of RICA concerning the directive that the Minister must issue about the retention of metadata. But to understand the impact of that power, it is necessary to consider various provisions of RICA.

45. The core obligation lies in s 30(1)(b), which obliges "*telecommunication service providers*" to store "*communication-related information*". Each of those terms is defined.

46. "Communication-related information" is metadata – it is all information available to an electronic communication service provider about a communication other than its content. It is defined as:

*"any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system".*

47. To appreciate the full breadth of the definition, it is necessary to look at the definition of "*indirect communication*":

*"the transfer of information, including a message or any part of a message, whether-*

*(a) in the form of-*

*(i) speech, music or other sounds;*

*(ii) data;*

*(iii) text;*

*(iv) visual images, whether animated or not;*

*(v) signals; or*

*(vi) radio frequency spectrum; or*

*(b) in any other form or in any combination of forms,*

*that is transmitted in whole or in part by means of a postal service or a telecommunication system"*

48. With regard to whom the obligation rests on, RICA is somewhat confusing. In 2006, an amendment removed the definition of "*telecommunication service provider*" and replaced it with a definition of "*electronic communication service*

*provider*", without amending the references to the former in the body of the Act, including in s 30. The term "*electronic communication service provider*" is defined with reference to the Electronic Communications Act 36 of 2005, as:

(a) *person who provides an electronic communication service under and in accordance with an electronic communication service licence issued to such person under Chapter 3 of the Electronic Communications Act, and includes any person who provides-*

(i) *a local access communication service, public pay-telephone service, value-added network service or private electronic communication network as defined in the Electronic Communications Act; or*

(ii) *any other electronic communication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act; and*

(b) *Internet service provider;*

49. In essence, it includes all phone operators and all internet service providers. The latter term is broadly defined as "*any person who provides access to, or any other service related to, the Internet to another person*". This potentially includes all hotels, cafes, and workplaces that offer internet connections.

50. Section 30(1)(b) is stated in broad terms. The details of the obligation to store metadata are meant to be set out in directives issued by the Minister under

s 30(2)(a)(iii). The Minister has exercised that power with regard to phone operators. She has not issued a directive to deal with internet service providers. In the absence of a directive, it is not clear whether and in what manner internet service providers are complying with their obligation to store metadata.

51. Once the information is stored, it is regarded as "*archived communication-related information*". Section 12 of RICA prohibits the electronic communication service provider from disclosing this information to anyone but the customer.
52. However, it can be accessed by the government using a direction issued in terms of s 19 of RICA. This has the limitations and safeguards described by the Applicant:
  - 52.1. It can only be obtained to investigate certain types of serious offences, and threats to national security;
  - 52.2. The application can be made only by specified senior officials within the definition of "*applicant*" in RICA; and
  - 52.3. The application must include the detailed information set out in s 17(2) (with the necessary changes based on the context).
53. However, archived communication-related information can also be accessed outside of s 19 of RICA. In fact, all this metadata can be accessed at any time, by virtually any prosecutor for an investigation into any crime without having to make out any case at all.

54. This flows from s 15 of RICA read with s 205 of the Criminal Procedure Act 51 of 1977 (**CPA**). Section 15 of RICA provides:

"(1) *Subject to subsection (2), the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in sections 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act.*

(2) *Any real-time or archived communication-related information which is obtained in terms of such other Act may not be obtained on an ongoing basis."*

55. Section 205(1) of the CPA is one such procedure. The provision reads:

"(1) *A judge of a High Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection (4) and section 15 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, upon the request of a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the Director of Public Prosecutions, require the attendance before him or her or any other judge, regional court magistrate or magistrate, for examination by the Director of Public Prosecutions or the public prosecutor authorized thereto in writing by the Director of Public Prosecutions, of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the*

*Director of Public Prosecutions or public prosecutor concerned prior to the date on which he or she is required to appear before a judge, regional court magistrate or magistrate, he or she shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.” (emphasis added)*

56. Section 205 is clearly intended to be used to obtain archived communications related information. Yet s 205 contains none of the safeguards in s 19 of RICA:

56.1. A request under s 205 can be made to investigate any offence;

56.2. The applications can be made by a far wider swathe of prosecutors;

56.3. Section 205 does not require the same detailed information to be placed before the judge or magistrate; and

56.4. Judicial officers dealing with s 205 applications are not subject to any reporting requirements, unlike the Designated Judge who under s 3 of the Strategic Intelligence Oversight Act is required to report certain information to Parliament – an issue we return to below.

57. In practice, s 205 warrants are often extremely easy to obtain. Indeed, the vast majority of metadata requests are not made in terms of s 19, but in terms of s 205. The applications are generally determined on paper, in chambers by any magistrate or judge.



58. The cumulative impact of these provisions is as follows:

58.1. All phone companies must maintain a record of the who, when, how and where of every single phone call and SMS of their users.

58.2. All ISPs must maintain a record of every website any person visits, and the who, when, how and where of every electronic message sent, including emails, Whatsapp, Facebook messages or any other form of electronic communication. That includes telecommunication service providers who operate as ISPs when consumers use their phones to access the internet. In the case of emails, the communication-related information includes the subject of the email.

58.3. That information must be stored in accordance with a directive issued by the Minister, for up to five years.

58.4. The information can be accessed either under s 19 of RICA, or s 205 of the CPA. That means it can be accessed to investigate any offence, without the procedural safeguards in s 19 (which are in any event inadequate to safeguard the right to privacy).

#### Unjustified Limitation of Privacy

59. For those people who have cellphones the information that phone operators and ISPs are mandated to store is incredibly personal. It is information about when, where, how and with whom we communicate. It is information about what internet

sites we visit. For those with cellphones – and particularly those who own smartphones – the metadata will literally track their movements minute by minute. Every time the phone makes a connection with the network – whether to make a call, check for emails, update an app, or any other purpose – the service provider will be obliged to record the user's location.

60. While cellphones allow the greatest intrusion into our private lives, it still applies to users of landlines, computers, or any other device that connects to the internet or a telecommunication network – smartwatches, tablets, smart TVs and so on. Information about our use of all of these devices is captured and stored.
61. This information is incredibly sensitive, and its collection is extremely invasive of the right to privacy. The only available information that is left untouched is the actual content of the messages. But the metadata on its own – especially when looked at systematically over a period of time – can tell the government a huge amount about a person's private life. Governments use this information not only to obtain evidence for prosecution of particular offences, but to build detailed profiles of people – who they interact with, where they move, what their interests are.
62. To appreciate just how invasive this power is, it is worth imagining what it would mean in the pre-digital age. The government would be able to maintain a record of every single letter that was sent, of who sent it to whom, and from where it was posted and received. The Government would be entitled to know who called who when and from where. It would be entitled to know what newspapers, books and

magazines we read. And it would have a record of where most people are every minute of the day. As the European Court of Justice has aptly explained, the mandatory and untargeted retention of metadata *"is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."* (*Digital Rights Ireland (Judgment of the Court)* [2014] EUECJ C-293/12. See also *Tele2 Sverige AB v. Post- Och telestyrelsen*; *Secretary of State for the Home Department v. Tom Watson et. al.* (C-698/16) [2016] EUECJ C-203/15)

63. The type of information s 30 of RICA requires companies to store is fundamentally personal information, particularly when it is aggregated over a period of time:

*"Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."* (*Digital Rights Ireland* at para 27. See also *Tele2 Sverige* at para 99).

64. Obliging companies to retain metadata – for any length of time and with even the most stringent safeguards – limits the right to privacy. The interference arises both from the fact that it is stored by a private company at the behest of the government, and from the fact that the government can access that data, with little or no safeguards, for the investigation of any crime.

MH

H

65. This is plainly a limitation of privacy. But it also limits the right to free expression. Even though the content of the communication is not recorded, the mandatory, blanket retention of metadata may prevent people from freely communicating with others because of the knowledge that the private information revealed by their metadata is available to the state. Chilling how people communicate because of the ever-present threat of government surveillance is a clear limitation of the right to free expression.
66. The Government seeks to justify this power because one day it might need the information in serious criminal investigations, and to combat threats to national security. This temptation is understandable. When crimes are committed we naturally want to be able to use all means available to identify and prosecute the wrongdoers. Seeking to investigate, punish and prevent those crimes is plainly a legitimate government objective.
67. But there are three reasons this can never justify the scheme created by RICA.
68. First, individualized reasonable suspicion is a well-established and fundamental safeguard to protecting the right to privacy. There must be some reason to suspect a particular person of wrongdoing in order to justify limiting their privacy.
69. Under RICA, everybody's metadata is retained, regardless of whether they are suspected of having committed a crime or not. As the European Court of Justice has explained when it set aside a comparable directive, such a mandate “*covers, in a generalised manner, all persons and all means of electronic communication*”

*as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. ... It ... applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."* (Digital Rights Ireland at paras 57-8) This is incompatible with the right to privacy.

70. Second, the same purpose could be achieved through a less restrictive, more targeted regime for the retention of metadata. The onus is on the state to show that a targeted retention regime would not serve the goals of crime-fighting as well as the boundless retention of every single person's metadata.
71. Third, under s 205 of the CPA, the state can access the metadata to investigate any crime, not only serious crimes and threats to national security.
72. Accordingly, the scheme for the mandatory retention of metadata is inherently unconstitutional. In this application, this Court is limited to particular limited aspects of that scheme. It should declare those aspects unconstitutional, but leave the door open for the intended challenge to the scheme as a whole.

### **The Designated Judge**

73. The Applicants argue that the designated judge, and the process she employs to issue directions, is insufficiently independent on two grounds:

73.1. The process is not adversarial; and

- 73.2. The designated judge is appointed by the executive for an indeterminate time (normally one year) that is subject to renewal.
74. R2K and PI supports these arguments. If admitted, it will advance three further lines of argument:
- 74.1. That comparative practice supports the arguments that the designated judge is insufficiently independent;
- 74.2. That the lack of independence also unjustifiably limits the right to privacy; and
- 74.3. That the secrecy with which the designated judge operates enhances the need for independence.
75. First, R2K and PI will place comparative information before the Court to demonstrate that RICA falls far short of international best practice. While there is certainly no uniformity between states, most provide far more independence to the equivalent of the designated judge:
- 75.1. They are normally sitting members of the judiciary whose terms are not subject to renewal.
- 75.2. There is a panel of judges who take turns to decide applications for warrants. While RICA plainly envisages that there may be multiple judges designated to determine applications, the practice has been that only one judge is designated. A panel has two advantages for independence:

75.2.1. It limits the ability for the executive to choose a specific person who will act favourably. Of course, if the executive still appoints all the panel members without a check, this provides only a limited safeguard.

75.2.2. It means that the RICA judge is likely to be overburdened by the number of applications, and therefore unable to devote sufficient time to each application to ensure that only those which meet the requirements of the Act are granted.

76. This international best practice tracks the flaws that the Applicants have identified in RICA.

77. Second, the lack of independence is not only a violation of the rule of law and the right of access to courts as the Applicants allege. It is also a violation of the right to privacy. Leaving aside any other constitutional flaws, RICA's provisions that permit the designated judge to issue directions to intercept communications violate the right to privacy because the judge lacks the necessary independence. This is supported by international human rights law which treats independent authorization of surveillance as a fundamental safeguard of the right to privacy.

78. Third, the designated judge operates largely in secret. Unlike an ordinary court, the applications are secret, and the proceedings are not adversarial. There are also limited reporting requirements. This inherent secrecy enhances the need for the designated judge to be independent.

79. There is legislative provision for the designated judge to file reports with the JSCI. Section 3(a)(iii) of the Intelligence Services Oversight Act 40 of 1994 (**Oversight Act**):

*"The functions of the Committee are-*

- (a) *notwithstanding anything to the contrary contained in any other law or the common law, to obtain from-*

*...*

- (iii) *any designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002), a report regarding the functions performed by him or her in terms of that Act, including statistics regarding such functions, together with any comments or recommendations which such designated judge may deem appropriate; Provided that such report shall not disclose any information contained in an application or direction referred to in that Act"*

80. This reporting function is vital to secure the independence and accountability of the designated RICA judge(s). The work of the designated judge occurs in secret. In order for the public to know that the judge is performing his or her work properly, it is vital that the reports made to the JSCI are publicly available and contain adequate information to assess the work of the judge.



81. The problem is that the Oversight Act does not specify what information should be provided by the designated judge. This has resulted in inconsistent, undetailed and incomplete reporting on the activities of the designated judge, greatly undermining public and Parliamentary oversight of the judicial function in RICA. While the level of information provided by the designated judge that is eventually released has improved significantly, it is still inadequate. The annual report provides only details about the number of applications for interception directions, the state agency that made the applications, and the number that were granted or refused. The judge may also include some general comments on trends.
82. No information is available in these reports on:
- 82.1. What were the warrants for – direct interception of metadata, direct interception of communication, provision of archived metadata?
  - 82.2. To how many people did the warrant pertain?
  - 82.3. To which alleged offence did the investigation pertain?
  - 82.4. What technology/method was used for the interception?
  - 82.5. What number of interceptions actually resulted in arrests and convictions?
83. This and similar information is vital to allow the public to assess whether the directions the judge grants are actually fulfilling their supposed purpose. If only a very small percentage of directions led to arrests or prosecutions, the public could legitimately ask whether too many directions are being granted.

84. In contrast, in the US the publicly available annual reports on what they call wiretaps include information on the offenses under investigation, types and locations of interception devices, costs and duration of authorized intercepts, and number of arrests and convictions resulting from intercepts. These reports are available at <http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports>. If made available, this information could be used to assess the effectiveness of various surveillance techniques. Aggregate information on the offences underlying the investigations for which directions were granted would also be important to provide.
85. On 17 March 2017, in my capacity as the Advocacy Coordinator for R2K, I wrote a letter to the late Judge G Maluleke, who had recently been appointed as the only designated judge. The letter informed Judge Maluleke about R2K's work relating to surveillance, and particularly its concern about certain elements of RICA. In addition, the letter requested the designated judge to "*consider specific recommendations ... regarding the format and ... detail that might be included in annual reports by the Office of the Designated Judge. These would aim to aid public oversight and research of RICA*". I attach a copy of this letter marked **MH4**.
86. Judge Maluleke responded on 10 April 2017. He noted the obligations placed on him by s 3(a)(iii) of the Oversight Act. He also wrote: "*The need for transparency and oversight in respect of the interception of communications and the provision of communication-related information is acknowledged as essential in a democratic society.*" He then stated that he was aware that the Department of

MH

11

Justice and Constitutional Development was considering amendments to RICA. He therefore requested R2K *"to engage with the Department on possible amendments to the RICA, which may also include any suggestions which you would like to make in respect of the form and detail of any report by a designated judge regarding his or her responsibilities in terms of the RICA."* I attach a copy of this letter marked **MH5**.

87. There is no challenge to s 3 of the Oversight Act in this application and R2K and PI do not intend to raise one. We mention the absence of reporting solely because it provides the background to assess the independence challenge actually brought by the Applicants. This is an institution about which very little is known and which has very limited and broadly stated reporting requirements. That makes it all the more important that its independence is absolutely beyond question.

### **Mass surveillance**

88. The Applicants rightly submit that the bulk surveillance of foreign signals conducted by the NCC is unlawful because:

88.1. There is no legal basis for the exercise of that power;

88.2. It is expressly prohibited by s 2 of RICA;

88.3. It limits the constitutional right of access to court without being justified by a law of general application; and

MH

§

- 88.4. Even if there was a law of general application that permitted the NCC's operation, it would not be a justifiable limitation of the right of access to court.
89. R2K and PI endorse these arguments and will not repeat them. However, there are three inter-related ways in which it wishes to supplement the Applicants' arguments:
- 89.1. By demonstrating the nature and extent of the bulk surveillance that the NCC conducts;
- 89.2. By highlighting the impact of bulk surveillance on the right to privacy; and
- 89.3. By relying on relevant comparative and international authority to support the argument that bulk surveillance is inherently unconstitutional.
90. The remainder of this section:
- 90.1. Explains at a very basic level how bulk surveillance operates;
- 90.2. Demonstrates the absence of any meaningful limits on bulk surveillance;
- 90.3. Shows that the limitation of privacy is unjustifiable; and
- 90.4. Briefly sets out two supplementary arguments R2K and PI will advance.

MIT

#

Operation of Bulk Surveillance

91. The Government has provided scant detail about how its mass surveillance system operates. Based on the affidavit of the DG of the State Security Agency, the following emerges:

91.1. Bulk surveillance is employed for "*environmental scanning*" to search internet traffic "*for certain cue words or key phrases*".

91.2. It is conducted by "*tapping or recording transnational signals*", including undersea fibre optic cables. It also seems to include interception of other signals, although the details are not spelled out. For the purposes of this litigation, the primary concern is the interception of internet traffic on undersea cables.

91.3. The interception includes both the communication itself, and the information about the communication (the metadata).

91.4. Bulk surveillance "*is not directed at individuals*". For that reason, it is not "*restricted by Foreign Signal Intelligence requirements*".

91.5. Once data is intercepted, it is stored, and backup copies of all the data are automatically made. There are both internal storage, and external storage. The process of recording, copying and storing data is "*automated, executed and managed internally by the system*." However, the stored information can be accessed by "*authorised technical personnel*".

91.6. However, the "*direction of communication can only accurately be determined by human intervention and analysis*". It is not clear what is meant by the "*direction of communication*". In the Government's view (which is refuted below) all the data are useless unless they are subject to human intervention and analysis.

92. The explanation is unsatisfactory as it does not provide a full picture of how the bulk surveillance occurs. In particular, there is very little explanation of how the data is accessed, analysed and deleted. Who is able to access the data? What criteria must be met in order to permit access? What criteria are used to discard data? What tools are used to analyse the data? Is the information shared with other domestic or foreign intelligence agencies? If so, under what conditions? No mention is made of provisions to delete these data. Is the data stored indefinitely?
93. All of this information is vital to assessing the nature and extent of the violation of the right to privacy. Yet it is absent precisely because the NCC operates in secrecy, and without a legal mandate.
94. Based on comparative information – particularly information disclosed by the US government in the aftermath of the Edward Snowden revelations and evidence before the European Court of Human Rights concerning the UK's mass surveillance operations – bulk surveillance happens in six stages. At each stage, there is a substantial interference with the privacy of communications and private life.

- 94.1. **Interception** – The first step is to obtain a signal from a source, e.g. by tapping a fibre optic cable.
- 94.2. **Extraction** – The intercepted signals are then copied and converted into a digital stream so that the data can be reconstructed into an intelligible format.
- 94.3. **Filtering** – The data can then be filtered, including in real-time or shortly after interception. Information of potential interest may be selected at this stage through the use of a database of identifiers or selectors. Low value information, such as the content of video streaming from well-known commercial providers, may be discarded.
- 94.4. **Storage** – Information is retained in a database for potential future analysis or dissemination.
- 94.5. **Analysis** – Once held in databases, there can then be further querying, examining or data-mining of the information.
- 94.6. **Dissemination** – The product of the intercept may then be shared with or distributed to other persons, organisations or agencies. Sharing can also occur in earlier stages of the interception process, for example, by providing foreign agencies access to entire databases, which may store raw intercept material.

mt

#

95. Based on the available evidence, it appears that the NCC follows the same process.
96. The right to privacy is violated at each one of these stages – when data is intercepted, extracted, filtered, stored, analysed and disseminated.

Scope of the Violation

97. Given the limited information available about bulk surveillance, it is impossible to determine the precise extent to which our right to privacy is being violated by the Government. In fact, the absence of clear information compounds the violation.
98. While the lack of legal authority, and the violation of s 34 of the Constitution are serious, the real problem with bulk foreign surveillance is that – even if permitted by law – it would impermissibly limit the right to privacy. This is not an issue of a minor legal vacuum that should be filled so that the NCC can continue to operate as it currently does. Nor is the difficulty primarily one of inconsistency with RICA or access to court. The fundamental problem is that the state asserts the right to capture virtually all internet traffic that enters and leaves South Africa.
99. Because of the nature of internet communications, which rely on servers and service providers across the world, the ability to monitor “foreign” signals is, in fact, the ability to monitor the content of local South African internet communications. When a South African sends an email from South Africa to another South African in South Africa, that signal will often travel to a foreign server, through one of the undersea fibre optic cables that the state admits that it taps. The same is true



when a South African visits a website, makes a Skype call, downloads a document from Dropbox, or accesses their online diary. All those communications are "foreign" and are liable to be intercepted by the NCC.

100. The Government does not shy away from this reality. It asserts that foreign signals intelligence *"includes any communication that emanates from outside the borders of [South Africa] and passes through or ends in the Republic"* (para 132). Indeed, the Director-General of Intelligence candidly admits that the NCC cannot even determine *"whether a communication emanates from outside the borders or simply passes through or ends in the Republic of South Africa."* Therefore, on the Government's own version, they are entitled to intercept, store, and analyse virtually all emails and internet traffic, without a warrant, and without statutory safeguards.

101. On any approach to privacy, this is a massive violation. While access to digital services is still so expensive it remains beyond the reach of many South Africans, as more and more South Africans gain access to the internet, a significant portion of our lives are lived online. We communicate online. We work online. We socialise online. We obtain our news, information and entertainment online. We use the internet to keep records and diaries, arrange travel, and conduct financial transactions. Much of this activity is conducted on mobile digital devices, which are seamlessly integrated into our personal and professional lives. They have replaced and consolidated our telephones, our filing cabinets, our wallets, our private diaries, our photo albums and our address books.

MH

\$

102. All of this information about our private and professional lives travels back and forth between individual computers and smartphones in South Africa, and servers located all over the world. And every time that information crosses the South African border, the NCC asserts a right to intercept, copy (repeatedly), store, access and analyse this information about our lives.
103. This traffic includes both the communication content itself, and the metadata. In this case, the metadata includes information about emails and other electronic communications, as well as browser history. It may, in some instances, also include location data if the device is interacting with a server outside the Republic. For example, if a person uses Google Maps, the search information as well as their location may well be captured by bulk surveillance because the signal will travel to Google's servers that are located outside South Africa.
104. I have already explained above why the interception, storage and analysis of metadata alone constitutes a serious interference of privacy. That is particularly so when – as with bulk surveillance – it can be analysed over a long period of time.
105. But bulk surveillance also includes the actual emails, the actual Skype calls, Facebook messages, photographs, diary entries, address books and so on.
106. It is difficult to think of a more serious systemic violation of the right to privacy of all South Africans who use the internet.
107. The violation is exacerbated by the fact that it is virtually unregulated. The Government does not seek authorisation for these immense powers under RICA

or any other statute. They appear to admit that RICA prohibits the interception, recording and copying of this information without judicial warrant. Instead, they argue that the interception of all "foreign" signals is permitted by s 2 of the National Strategic Intelligence Act 39 of 1994 (**NSIA**). The section grants the State Security Agency, in broad terms, the power to "*gather, correlate, evaluate and analyse domestic and foreign intelligence*".

108. The NSIA contains no limits on the s 2 power, and no procedural safeguards for the exercise of this power. The Government points to none in its answering affidavits.

109. As a result:

109.1. There are no laws governing what data may be collected and for what purposes, how it must be stored, who may access or use it and under what conditions, how long it may be kept, when it can be shared, with whom and under what conditions, or when it must be destroyed.

109.2. There are no procedures for independent authorization of the collection or access to the information. The SSA is given completely free reign to determine what data may be collected and accessed and under what conditions.

109.3. Oversight occurs only at the most general level through the Inspector General of Intelligence, and the Joint Standing Committee on Intelligence. There is no regular oversight of how the SSA conducts bulk surveillance.

110. The effect of an absence of any regulatory framework is clear in the instances of abuse pointed out by the Applicants (paras 142-143).
111. To be clear, R2K and PI's position is that unregulated, untargeted surveillance of information, merely because it happens to cross South Africa's borders is unconstitutional. That is not to say that the intelligence services are prohibited from intercepting any foreign communication. But they can only do so in a way that is targeted and carefully regulated. The current regime exhibits neither of those features.

Justification

112. Substantively, the Government makes little attempt to justify foreign bulk surveillance. Its defences can be summarised as follows:
- 112.1. These practices are common in other jurisdictions; and
- 112.2. Bulk surveillance and environmental scanning are necessary to deal with *"unconventional threats to peace and stability"*.
113. Neither argument is sufficient to justify the current form of untargeted, unregulated mass surveillance of South Africans.
114. First, while these mass surveillance systems exist in other countries, they do not comply with international human rights law, including the International Covenant on Civil and Political Rights to which South Africa is a party. Courts and

MH

#

international authorities have decried the type of unregulated surveillance conducted by the NCC.

115. Second, the Government claims it needs to record internet traffic to deal with "unconventional threats" which include organised crime and terrorism. But it also includes "food security, water security and illicit financial flows." R2K and PI do not deny that surveillance of foreign signals on a targeted basis may sometimes be necessary to deal with terrorism and other threats to national security. But the current system is unjustifiable:

115.1. The Government's understanding of the ends that can be pursued through bulk surveillance is extremely broad. On its own version it is not limited to an ordinary understanding of national security. It is closer to a definition of national interest. It is also far wider than the definition used in the NSIA, which reads:

" '**national security**' includes the protection of the people of the Republic and the territorial integrity of the Republic against-

(a) the threat of use of force or the use of force;

(b) the following acts:

(i) Hostile acts of foreign intervention directed at undermining the constitutional order of the Republic;

(ii) terrorism or terrorist-related activities;

- (iii) *espionage;*
  - (iv) *exposure of a state security matter with the intention of undermining the constitutional order of the Republic;*
  - (v) *exposure of economic, scientific or technological secrets vital to the Republic;*
  - (vi) *sabotage; and*
  - (vii) *serious violence directed at overthrowing the constitutional order of the Republic;*
- (c) *acts directed at undermining the capacity of the Republic to respond to the use of, or the threat of the use of, force and carrying out of the Republic's responsibilities to any foreign country and international organisation in relation to any of the matters referred to in this definition, whether directed from, or committed within, the Republic or not,*

*but does not include lawful political activity, advocacy, protest or dissent"*

115.2. The NCC's powers to conduct surveillance are far broader than is needed to achieve the above purposes.

115.2.1. The Government simply does not require access to all the information that enters or leaves South Africa in order to defend its national security. Far narrower powers would adequately

achieve the goal without bringing all information into the government's net.

115.2.2. There is no reason why the exercise of foreign surveillance cannot be subject to appropriate regulation of what information may be intercepted, extracted, filtered, stored, analysed and disseminated. And there is no reason those powers should not be subject to direct oversight to ensure they are not abused.

116. Accordingly, the purpose is simply inadequate to justify the limitation.

Additional Submissions

117. In addition to the primary argument that the practice of bulk surveillance unjustifiably limits the right to privacy for the reasons set out above, R2K and PI will advance two further, related submissions:

118. First, properly interpreted, the NSIA can never provide the legal authority to justify its admitted practice of bulk surveillance. The NSIA, like all statutes, must be interpreted in terms of s 39(2) to promote the spirit, purport and objects of the Bill of Rights. Interpreting the NSIA to authorise the current practice would be an interpretation that permits massive, systemic violation of the right to privacy. That interpretation is not required by the text of the NSIA, particularly when it is read in light of the limitations in RICA.

119. Second, this Court could decide this part of the case narrowly by simply holding that the NCC lacks the legal basis to function. However, it should also hold that the admitted practice of bulk surveillance is unconstitutional because it violates the relevant rights in the Constitution, and particularly the right to privacy. If this Court decides the issue on the narrow basis that there is no legal authority, there will inevitably be a future challenge once the legal authority is provided. This Court should make it clear that untargeted, unregulated, bulk surveillance will always be unconstitutional, even if it is conducted with legal authority.

#### IV PROCEDURAL REQUIREMENTS FOR ADMISSION

120. In terms of Rule 16A(2), a party seeking to be admitted as an *amicus curiae* must seek the written consent of all the parties in the proceedings.
121. R2K sent letters to the Applicants and Respondents requesting their consent to its admission in both matters on 16 October 2017. A copy of that letter is attached as annexure **MH 6**.
122. R2K has received the following responses:
- 122.1. On 24 October 2017 Applicants consented to the admission of R2K as *amicus curiae* in this application. A copy of the letter is attached as Annexure **MH 7**.



- 122.2. On 3 November 2017, the State Attorney – representing the first, third, fourth, fifth, sixth and the ninth consented to R2K's request. I attach a copy of the letter as annexure **MH 8**.
123. R2K has not received any response from attorneys representing the second, seventh, eighth and tenth respondents.
124. Given the absence of consent from those parties, it is necessary for R2K to bring this application for admission.
125. I have been advised that R2K's application for admission as *amicus curiae* is outside of the time period provided for in Rule 16A of the Uniform Rules of Court in this matter. The applicants filed their Rule 16A notice on 29 June 2017. The 20 day period for obtaining consent of the other parties in terms of Rule 16A(2) expired on 27 July 2017.
126. I set out below the reasons of R2K's late filing of the application and the steps that have been taken by R2K's attorneys since learning about the main application to bring this application as expeditiously as possible. R2K seeks condonation from this Court for the late filing of this application in this matter
127. R2K only became aware of the matter during May 2017. R2K approached the Legal Resources Centre (**LRC**) for legal representation during May 2017. The LRC obtained the founding papers documents in the matter but decided that it would be more appropriate to wait for the filing of the answering affidavit before making a decision on whether it could make a helpful contribution as *amicus curiae*. It was

only after receipt of the answering affidavits that R2K could assess whether it could make a useful contribution in the matter. This required both the LRC and R2K to peruse the documents this application, and to conduct detailed research on the position in comparative and international law.

128. The answering affidavit on behalf of the second, seventh, eighth and tenth respondents was filed on 19 July 2017. During September 2017 R2K determined (based on the advice received from the LRC) that it would be able to make novel and relevant submissions.
129. The letter requesting consent was sent to the parties on the 16 October 2017 and required the parties to respond by 29 October 2017. However, we considered it prudent to allow additional time for the State Attorney to respond as their response would have a substantial impact on the application. As indicated above, the State Attorney, on behalf of the second respondent, consented to R2K's admission as *amicus curiae* but only did so on 3 November 2017.
130. In addition, R2K's request to the parties for consent to be admitted as *amicus curiae* noted that the *dies* set out in Rule 16A had expired. R2K's request further noted that a date had not been allocated for hearing the main application and that the parties would not be prejudiced by the late filing of the application to be admitted as *amicus curiae*. None of the parties who responded to our letter raised a concern in this regard.
131. Insofar as Privacy International is concerned, the following timeline is relevant:

- 131.1. PI first became aware of R2K's plans to intervene as an *amicus curiae* during February 2018.
- 131.2. It then communicated with both R2K and its attorneys, the LRC, to determine whether PI could apply to be admitted, and for PI to ascertain whether it would support the submissions to be advanced by R2K.
- 131.3. R2K and PI decided that counsel would first settle a draft for R2K, and then PI would consider whether it was willing to join the application.
- 131.4. A draft was provided to PI on 27 March 2018. Privacy considered the draft and indicated that it wished to join the application on 25 April 2018, but that it wished to comment on the draft.
- 131.5. PI proceeded to comment on the draft which then had to be settled by counsel. That was completed on 25 June 2018.
- 131.6. On the same day, PI sent a letter to the other parties requesting that they indicate whether they object to PI's admission as *amicus curiae* together with R2K. I attach a copy of that letter marked **MH 9**. The letter indicates that PI's submissions are identical to R2K's. It requested any party that objected to PI's admission to inform the attorneys by Friday 29 June 2018.
- 131.7. The attorneys for the second, seventh, eight and tenth respondents responded requesting more information on PI's interest in the matter. Their correspondence is attached hereto as **MH 10**. Our response setting out PI's

interest in the matter is attached as **MH 11**. We did not receive any further correspondence from the attorneys for the second, seventh, eighth and tenth respondents.

132. Given the wide-ranging and complicated nature of this matter and the need to avoid duplicating argument advanced by the parties, R2K and PI was advised that it would be appropriate to await the filing of the answering and replying affidavits. It was only after the pleadings had closed that we could be sure that the submissions it sought to advance would be both relevant and novel as required by Rule 16A. The last answering affidavit was filed during November 2017. The replying affidavit has still not been filed. However, as the application was already complete, we were advised to file it notwithstanding that the replying affidavit was still outstanding. As a result, while late, the amicus application will not delay the hearing of this matter.
133. I respectfully submit that R2K and PI have shown good cause for the late filing of this application, and that no party will be prejudiced should condonation be granted. That is demonstrated by the fact that those parties that responded to R2K's request have all consented to its admission. Moreover, the subject matter of the main application is undoubtedly a matter of public importance, and I submit that that the submissions and evidence to be presented by R2K and PI are relevant and will be of assistance to this Court.
134. I therefore request that this Court grant condonation for R2K and PI for the late filing of this application.

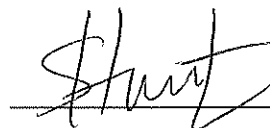
## CONCLUSION

135. R2K and PI submit that their submissions are both relevant and novel, and that it would be in the interests of justice for them to be admitted as *amici curiae*. In light of the above, R2K and PI accordingly pray for an order in terms of the notice of motion to which this affidavit is attached, admitting them as *amici curiae* for the purpose of making oral and written legal submissions and adducing evidence limited to this affidavit.



**MURRAY HUNTER**

The Deponent has acknowledged that he knows and understands the contents of the affidavit, which was signed and sworn to or solemnly affirmed before me at **Cape Town** on this the 12<sup>th</sup> day of JULY 2018, the regulations contained in Government Notice No. R1648 of 19 August 1977, as amended, having been complied with.



**COMMISSIONER OF OATHS**

SALLY HURT  
COMMISSIONER OF OATHS  
Practising Attorney, RSA  
Sally Hurt & Associates  
Unit 12 Geriva Mansions  
27 St James St  
Vredehoek  
Cape Town, 8001.

Human Rights Committee, Privacy International  
Submission: 114th Session, June-July 2015

# The Right to Privacy in South Africa

Submitted by Privacy International, the Association  
for Progressive Communications & the Right2Know  
Campaign

**Suggestions for right to privacy-related questions to be included in the list of issues on South Africa, Human Rights Committee, 114th session, June-July 2015**

April 2015

**Main concerns on the right to privacy and communication surveillance in South Africa**

Article 17 of the International Covenant on Civil and Political Rights provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour or reputation. Any interference with the right to privacy can only be justified if it is in accordance with the law, has a legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human rights.<sup>1</sup>

Privacy International, Right2Know, and the Association for Progressive Communications have on-going concerns on the practices of surveillance by South African intelligence and law enforcement agencies.<sup>2</sup> National legislation governing surveillance is inadequate, leaving significant regulatory gaps and providing weak safeguards, oversight and remedies against unlawful interference with the right to privacy, including mass surveillance. The government has also failed to meaningfully regulate the practice of the surveillance industry, having instead provided public funding to companies that export surveillance technologies to be used in violation of the right to privacy.

**1. Inadequacies of national legislation regulating domestic surveillance**

Broad powers to intercept personal communications and cases of abuse

Surveillance of domestic communications is regulated by the 2002 Regulation of

<sup>1</sup> See Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014. See also International Principles on the Application of Human Rights to Communications Surveillance, available at <https://necessaryandproportionate.org>

<sup>2</sup> Privacy International is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. The Right2Know Campaign is a broad-based, grassroots campaign formed to champion and defend information rights and promote the free flow of information in South Africa. The Association for Progressive Communications (APC) is an international network and non-profit organisation founded in 1990 that wants everyone to have access to a free and open internet to improve lives and create a more just world.

MA

#



Interception of Communications and Provision of Communications Related Information Act (RICA).<sup>3</sup> The most recent report of the Parliamentary oversight committee noted a significant increase (170%) of the number of warrants for interceptions between 2008 and 2011, followed by a drop from 2012 to 2013.<sup>4</sup>

RICA requires the permission of a judge for the interception of communications, which can be granted if there are "reasonable grounds to believe" that a serious criminal offence has been or is being or probably will be committed (Section 16.)

There is no provision to require that those subjected to communication surveillance are notified that their communications have been intercepted, not even after the completion of the relevant investigation.

To guarantee the capacity of relevant state agencies to conduct interceptions, RICA requires that telecommunication service providers provide telecommunication services which have the capability of being intercepted (i.e. by building in their networks a backdoor for surveillance) (Section 30.)

The South Africa periodic report notes that "while the Act [RICA] may seem draconian on the face of it, one ought to bear in mind the elaborate mechanisms that the Act puts in place to ensure that its provisions are not abused."<sup>5</sup> In fact, the low threshold to trigger surveillance ("reasonable grounds") under RICA and the weakness of the oversight mechanism have led to abuses leading to violations of the right to privacy.

Notably, two journalists of the Sunday Times (the biggest weekend newspaper in South Africa) investigating cases of government corruption had their communications intercepted from 2010 reportedly with the view to disrupt their investigations and uncover their sources. The police obtained the judicial approval to intercept the mobile phone communications of the journalists by giving fictional names and suggesting such interception was needed to investigate a criminal syndicate. The Sunday Time has taken the case to court and two officers have been charged with violations of RICA.<sup>6</sup>

### Retention of metadata

RICA also requires companies to store metadata (information about a communication, but not the content of such communication.)<sup>7</sup> Unlike for content of communication, a warrant to collect metadata requires the permission of any judge or magistrate.

<sup>3</sup> Available at: <http://www.internet.org.za/ricpci.html#interceptionofcommunicationunderinterceptiondirection>

<sup>4</sup> See Right2Know, Secret State of the Nations Report 2014, available at: <http://www.r2k.org.za/2014/09/09/r2k-secrecy-report-2014/>

<sup>5</sup> South Africa initial report, UN doc. CCPR/C/ZAF/1, 28 November 2014, paragraph 184.

<sup>6</sup> For more information, see Global Information Society Watch 2014, Communications surveillance in the digital age, pages 224-227.

<sup>7</sup> This is defined in RICA as including "switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system".

MH

#



The interception, collection and use of metadata interfere with the right to privacy, as it has been recognized by human rights experts, including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.<sup>8</sup> The Court of Justice of the European Union noted that metadata may allow “very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained” and concluded that the retention of metadata relating to a person’s private life and communications is, in itself, an interference with the right to privacy.<sup>9</sup>

#### Weak oversight and insufficient transparency

A Parliamentary committee to oversight the work of intelligence services in South Africa is mandated to release public report on the application of RICA. However, the data released do not provide number of individuals whose communications are subject to interception (only the number of warrants, that could include any number of individuals.) The report does not go into any details on the reasons these interceptions are carried out nor on the outcome and effectiveness they may have in preventing or investigating crimes. Further, there appears to be no centralised oversight or requirement of public disclosures of statistics on metadata's collection and use.

The lack of transparency on RICA's implementation has been a growing concern. Notably, Section 42 of RICA prohibits the disclosure of any information on the demands of interception. As a result, telecommunications companies are barred from publishing information, including aggregated statistics, both of interception of communications and of metadata.<sup>10</sup>

### **3. Mass surveillance by South African intelligence agencies and surveillance of political and social activists**

Despite the aim of RICA to regulate the interception of communications, there have been consistent reports of state surveillance being carried out outside the RICA legal framework, in manners that violate the right to privacy. This is particularly so with regards to the National Communications Centre (NCC), the government’s national facility for intercepting and collecting electronic signals on behalf of intelligence and security services in South Africa. It includes the collection and analysis of foreign signals (communication that emanates from outside the borders of South Africa or

<sup>8</sup> See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

<sup>9</sup> See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

<sup>10</sup> See Vodafone, Law Enforcement Disclosure Report, 2014 and February 2015 update, available at: [http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law\\_enforcement\\_disclosure\\_report\\_2015\\_update.pdf](http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf)

MH

#

passes through or ends in South Africa.)

The capacity of the NCC to conduct unregulated mass surveillance was highlighted by the Mail & Guardian in 2013. The report noted how the agency is able to conduct mass monitoring of telecommunications, including conversations, emails, text messages and data, without judicial authorisations or other safeguards.<sup>11</sup>

A Ministerial Review Commission on Intelligence in South Africa (known as 'Matthews Commission') set up to review intelligence gathering in South Africa found that the NCC carries out surveillance (including mass interception of communications) that is unlawful and unconstitutional, because it fails to comply with the requirements of RICA.

The Matthews Commission report, released in 2008, made a series of recommendations to address the lack of control and regulations of the South African intelligence agencies. These recommendations have, by and large, not yet been acted upon by the government.<sup>12</sup>

South Africa adopted the General Intelligence Laws Amendment Act in 2013. The Act specifically excludes from the mandate of the intelligence agencies surveillance of "lawful political activity, advocacy, protest and dissent." Despite of this positive development, police and intelligence agencies continue to conduct surveillance of those legitimately exercising their right to freedom of expression, association and peaceful assembly.<sup>13</sup>

Concerns about the activities of the South African intelligence agencies have recently been surfaced when Al-Jazeera News reported in February 2015 on the leaked 'Spy Cable' documents.<sup>14</sup> One document, for example, revealed a secret agreement between Zimbabwe's Central intelligence Agency and South Africa's State Security Agency to exchange intelligence and information about "rogue NGOs" and "identify and profile subversive media".<sup>15</sup>

Further, the 2013 Act missed the opportunity to close a significant legislative gap, by failing to regulate the interception of foreign signal intelligence. The regulation of interception of foreign signal intelligence is instead expected to be considered in the context of the on-going review of the South African intelligence services.

<sup>11</sup> Mail & Guardian, Spy wars: South Africa is not innocent, 21 June 2013, <http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent> And also, Secret state: How the government spies on you, available at: <http://mg.co.za/article/2011-10-14-secret-state/>

<sup>12</sup> Available at: [http://www.ssronline.org/document\\_result.cfm?id=3852](http://www.ssronline.org/document_result.cfm?id=3852).

<sup>13</sup> See Right2Know, "Big Brother Exposed: How South Africa's intelligence structures monitor and harass our movements, unions and activists", to be published in 2015.

<sup>14</sup> See <http://www.aljazeera.com/investigations/spycables.html>

<sup>15</sup> See <http://www.documentcloud.org/documents/1672718-south-africa-zimbabwe-joint-action-plan-2011-2012.html>

M#

#

#### 4. Support of surveillance technologies: the case of VASTech

On at least two occasions (2008 and 2010)<sup>16</sup>, the South African government directly provided public funding to a surveillance technology company, VASTech, which in the mid/late '00s supplied mass surveillance technologies to the Libyan government of Colonel Gadhafi.<sup>17</sup> In 2005, according to a report leaked in February 2015, an Iranian delegation reportedly met with the South African government and companies such as VASTech in a bid to obtain surveillance technology.<sup>18</sup>

One of VASTech surveillance products, Zebra, was reportedly provided to the Libyan government in 2011. Zebra allowed the security services to capture "30 to 40 million minutes of mobile and landline conversations a month and archived them for years". Zebra also meant it could help those security services identify relationships between individuals based on analysis of their calling patterns.<sup>19</sup> It is advertised as a monitoring system "which connects to telecoms networks and intercepts voice, fax, and SMS communications" and has the "power and capacity to record everything, content included".<sup>20</sup>

Responding to a Privacy International letter, the South Africa Department of Trade and Industry noted on 18 December 2013 that VASTech provided all the required information in advance of the funding being made available and had the government known that the technology involved was advertised as being capable of mass surveillance, the outcome of the funding would "certainly" have been different.<sup>21</sup> Further, a spokesperson of the Department of Trade and Industry confirmed that the government approved the funding of Zebra and "knew that it would be for mass surveillance". However, the Department noted that when the approval took place, it did not know it would be "used for nefarious purposes" and they were "led to believe" Zebra was only meant for "monitoring borders and stadiums, among other things". However, according to the Mail & Guardian, the South African government continues to fund VASTech, supporting a new software, called "Next".<sup>22</sup>

The government's reply suggests that any due diligence process being carried out in either the direct funding of the development of the technology, or the export process

16 See [http://www.spil.co.za/content/Annual%20Reports/SPII\\_Annual\\_Report\\_2008.pdf](http://www.spil.co.za/content/Annual%20Reports/SPII_Annual_Report_2008.pdf) and [http://www.spil.co.za/content/Annual%20Reports/SPII\\_Annual\\_Report\\_2010.pdf](http://www.spil.co.za/content/Annual%20Reports/SPII_Annual_Report_2010.pdf)

17 Mail & Guardian, Millions were handed to an SA company that supplied mass surveillance technology to Libya, available at: <http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware>

18 See <https://s3.amazonaws.com/s3.documentcloud.org/documents/1672715/south-africa-operational-target-analysis-of-iran.pdf>

19 Wall Street Journal, Firms Aided Libyan Spies First Look Inside Security Unit Shows How Citizens Were Tracked, available at: <http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388>

20 See at: [http://wikileaks.org/spyfiles/files/0/182\\_VASTECH-201110-BROCHURES.pdf](http://wikileaks.org/spyfiles/files/0/182_VASTECH-201110-BROCHURES.pdf)

21 Letter by Dr Rob Davies, MP, Minister of Trade and Industry, 18 December 2013.

22 Mail & Guardian, DTI 'funded Gaddafi spyware', 22 November 2013, available at: <http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware>

did not include any meaningful assessment of the surveillance technology's effects on human rights, including the right to privacy.

## **5. Failure to fully implement legislation on data protection**

In 2013 South Africa passed a data protection law, the Protection of Personal Information Act.

The Act does not apply to the processing of personal information carried out for purposes of national security (including identification of terrorist activities) and prevention or investigation of crimes “to the extent that adequate safeguards have been established in legislation for the protection of such personal information” (Section 6.)

However, the President has yet to set a commencement date for the full enactment of this legislation. As a result, the potential of this law to protect the right to privacy remains untested and notably the authority envisaged to monitor the protection afforded to personal data is yet to be constituted.

This is of particular concern in light of the requirement under RICA for mandatory SIM card registration, and the introduction in recent years of government backed schemes to collect personal data of individuals, such as using of biometrics for passports and banking.

Mandatory SIM registration, in effect, eradicates the ability of mobile phone users to communicate anonymously and facilitates mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies. The potential for misuse of such information is enormous. SIM registration can also have discriminatory effects – the poorest individuals (many of whom already find themselves disadvantaged by or excluded from the spread of mobile technology) are often unable to buy or register SIM cards because they do not have identification documents or proof of residence.<sup>23</sup> The justifications commonly given for SIM registration – that it will assist in reducing the abuse of telecommunications services for the purpose of criminal and fraudulent activity – are unfounded. SIM registration has not been effective in curbing crime, and instead has fueled the growth of identity-related crime and black markets to service those wishing to remain anonymous.<sup>24</sup>

<sup>23</sup> See Freedom House, *Freedom on the Net*, 2014, page 703.

<sup>24</sup> See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2013.

MT

#

## 7. Proposed questions for the list of issues

Based on these observations, Privacy International Privacy International, Right2Know, and the Association for Progressive Communications propose the following questions for the List of Issues:

Article 17:

- What measures is South Africa taking to ensure that its state security and intelligence agencies respect the right to privacy?
- In particular, how does South Africa ensure that all interception activities are only carried out on the basis of judicial authorisation and communications interception regime complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are intercepted?
- What measures is South Africa planning to strengthen effective oversight over the surveillance practices of its state security and intelligence agencies?
- How does South Africa regulate the export of surveillance technologies by private companies based in the country and how such export regulation takes into consideration the potential risks that such technologies pose to the right to privacy when sold to foreign governments or other third parties?
- When is South Africa going to fully operationalise the provisions of the Protection of Personal Information Act 2013?

Articles 19, 21 and 22

- What measures is South Africa taking to address the reports of unlawful surveillance of journalists, political activists and human rights defenders to ensure that their right to freedom of expression, peaceful assembly and association are respected and protected?

#

MP

---

**ADVANCE UNEDITED VERSION**

---

---

**Human Rights Committee**

---

**Concluding observations on the initial report of South Africa\***

1. The Committee considered the initial report of South Africa (CCPR/C/ZAF/1) at its 3234th and 3235th meetings (CCPR/C/SR.3234 and 3235), held on 7 and 8 March 2016. At its 3258th meeting, held on 23 March 2016, it adopted the following concluding observations.

**A. Introduction**

2. The Committee welcomes the submission of the initial report of South Africa and the information presented therein, and regrets that it is 14 years overdue. It expresses appreciation for the opportunity to engage in a constructive dialogue with the State party's high-level delegation on the measures that the State party has taken since the entry into force of the Covenant to implement its provisions. The Committee is grateful to the State party for its written replies (CCPR/C/ZAF/Q/1/Add.1) to the list of issues (CCPR/C/ZAF/Q/1), which were supplemented by oral responses provided by the delegation, and supplementary information provided to it in writing.

**B. Positive aspects**

3. The Committee welcomes the following legislative and institutional steps taken by the State party:

(a) The enactment on 25 July 2013 of the Prevention and Combating of Torture of Persons Act, which criminalises torture;

(b) The enactment on 29 July 2013 of the Prevention and Combating of Trafficking in Persons Act, which became operational on 9 August 2015;

(c) The enactment of the Child Justice Act in 2008, which took effect on 1 April 2010, which enhances protections for children in conflict with the law;

---

\* Adopted by the Committee at its 116th session (7–31 March 2016).

(d) The adoption of several legislative and institutional reforms aimed at combating violence against women, including the Domestic Violence Act of 2003 and the Criminal Law (Sexual Offences and Related Matters) Amendment Act of 2007, the re-establishment of specialized sexual offences courts, and the establishment of Thuthuzela Care Centres;

(e) The establishment in 2011 of the National Task Team to counter discrimination and violence against persons based on their actual or perceived sexual orientation and gender identity and expression, and the launch in 2014 of the National Intervention Strategy; and

(f) The passing of the Choice on Termination of Pregnancy Act in 1996 and other measures designed to increase access to safe abortion resulting in the significant decrease in maternal mortality and morbidity.

4. The Committee welcomes the ratification of, or accession to, the following international instruments by the State party since the entry into force of the Covenant in 1998:

(a) The Optional Protocol to the International Covenant on Civil and Political Rights, on 28 August 2002;

(b) The Convention on the Rights of Persons with Disabilities and its Optional Protocol, on 30 November 2007;

(c) The International Covenant on Economic, Social and Cultural Rights, on 12 January 2015;

(d) The Optional Protocols to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography on 30 June 2003; and on the involvement of Children in Armed Conflict on 24 September 2009;

(e) The Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women, on 18 October 2005;

5. The Committee welcomes the State party's declaration made under article 41 of the Covenant, recognizing the competence of the Committee to receive and consider inter-State communications.

## **C. Principal matters of concern and recommendations**

### **Domestic applicability of the Covenant**

6. The Committee notes the apparent inconsistency between the text of the Constitution, which provides that a self-executing provision of an international agreement approved by Parliament is considered to be part of domestic law, and the information contained in the Core Document (HRI/CORE/ZAF/2014, para. 95), which states that provision of an international treaty cannot be invoked before or directly enforced by the Courts. The Committee also notes that only two individual communications have been submitted under the Optional Protocol to the Covenant since 2002, and that this may be illustrative of lack of awareness of the Covenant and the Optional Protocol (art. 2).

7. **The State party should consider taking measures to give full legal effect to the Covenant under domestic law, and it should make more vigorous efforts to raise awareness about the Covenant and the Optional Protocol among judges, lawyers, prosecutors and the public at large. In the event of a violation of the Covenant, the State party should ensure access to an effective remedy, in accordance with article 2, paragraph 3.**

#

#### **Non-compliance with domestic court decisions**

8. The Committee notes the ruling of the North Gauteng High Court, which considered the authorities' failure to detain Sudan President Omar al-Bashir in June 2015 pursuant to an International Criminal Court arrest warrant to be inconsistent with the Constitution, and expresses concern that President al-Bashir was authorized to leave the country in violation of an interim Court order (arts. 2, and 14).

9. **The State party should continue its investigation of the events surrounding the failure to comply with the interim Court order on President Al-Bashir and take the necessary measures to ensure compliance with rulings of domestic courts, including in cases relating to the State party's international treaty obligations.**

#### **Oversight and monitoring mechanisms**

10. While acknowledging the important work of State institutions exercising oversight over government operations in connection with the protection of Covenant rights, the Committee is concerned about various challenges faced by some of these oversight bodies in terms of budget limitations, lack of institutional independence from supervised government departments, and limited mandates and powers. The Committee notes the State party's intention to ratify the Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, but it is concerned about the absence of independent and sustained monitoring of places of deprivation of liberty other than prisons (arts. 2, 6 and 7).

11. **The State party should ensure that all oversight bodies are institutionally independent, adequately funded and equipped with the necessary powers and functions to deal with complaints and investigations promptly and effectively, hold authorities accountable, and facilitate access by victims of human rights violations to an effective remedy. The State party is encouraged to speed up the preparations for the ratification of the Optional Protocol to the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment and should establish a system for the regular and independent monitoring of all places of detention, as well as a confidential mechanism for receiving and processing complaints lodged by persons deprived of their liberty.**

#### **Truth and Reconciliation Commission**

12. The Committee commends the State party for the work of the Truth and Reconciliation Commission in investigating gross human rights violations perpetrated during the apartheid era. It is concerned, however, that the recommendations of the Commission have not been fully implemented, in particular with regard to prosecution of perpetrators, investigations of cases of disappearances, and adequate reparation to all victims (arts. 2, 6 and 7).

13. **The State party should increase its efforts to implement the recommendations of the Truth and Reconciliation Commission, investigate cases of serious human rights violations documented by the Commission, including those involving enforced disappearances, prosecute and punish perpetrators, and provide adequate reparation to all victims.**

#### **Racism and xenophobia**

14. The Committee is concerned about numerous manifestations of racism and xenophobia, including violent attacks against foreign nationals and migrants, refugees and asylum-seekers, resulting in deaths, injuries, displacement and property destruction. The Committee is further concerned about the inability of the authorities to prevent and address



racist and xenophobic attacks and to hold perpetrators accountable (arts. 2, 6, 7, 9, 17, 20 and 26).

15. The State party should redouble its efforts to prevent and eradicate all manifestations of racism and xenophobia, protect all communities in South Africa against racist or xenophobic attacks, and improve policing responses to violence against non-nationals. Effective investigations into alleged racist or xenophobic attacks and other hate crimes should be systematically conducted, perpetrators should be prosecuted and, if convicted, punished with appropriate sanctions, and victims should be provided with adequate remedies. The State party should also pass as soon as possible appropriate legislation explicitly prohibiting hate crimes and hate speech.

#### Persons living with HIV/AIDS

16. While acknowledging the many efforts taken by the State party to promote and protect the life and health of persons living with HIV/AIDS, the Committee remains concerned at the persistence of stigma and discrimination against such persons and at barriers to the equal access to health services for such persons, particularly for women and persons living in poor or rural areas (arts. 2, 6, and 26).

17. The State party should continue its efforts to:

- (a) Raise awareness on HIV/AIDS with a view to combating prejudices and negative stereotypes and discrimination against people living with HIV/AIDS;
- (b) Speedily adopt the draft National Policy on HIV, STIs and TB and implement its sexual and reproductive health policy, especially towards adolescents;
- (c) Ensure that all persons at risk or living with HIV/AIDS have equal access to medical care and treatment, including adequate counselling services.

#### Harmful cultural traditions and practices

18. The Committee is concerned at the persistence of harmful traditional or cultural practices as *ukuthwala*, virginity testing and witchcraft, and about reports suggesting the prevalence of death and injury resulting from the practice of *initiation*. The Committee is also concerned at the existence in law and in practice of polygamous customary marriages in the State party, which undermine the principle of non-discrimination, as provided under the Covenant in the field of marriage and family relations (arts. 2, 3, 6, 7, 17, 24 and 26).

19. The State party should amend the Children's Act with the aim of prohibiting virginity tests for children, irrespective of their age, and undertake effective measures, including education campaigns, designed to combat harmful traditional, customary or religious practices. It should also take adequate measures to reduce the incidence of polygamy, with a view to bringing about its abolition. Initiation schools should be strictly regulated and monitored throughout the territory.

#### Violence based on sex, gender, sexual orientation and gender identity

20. While acknowledging the considerable efforts invested by the State party in this field, the Committee is concerned that gender-based and domestic violence remains a serious problem in the State party, that the conviction rate for such acts is low, and that there is a lack of disaggregated data on the phenomenon. It is also concerned about the persistence of stigma against persons on the basis of their real or perceived sexual or gender orientation, gender identity or bodily diversity, and that such persons are subject to harassment, acts of discrimination and to sexual and physical violence (arts. 2, 3, 6, 7 and 26).

21. The State party should redouble its efforts to prevent and combat sexual, gender-based and domestic violence and to eradicate discrimination and violence against persons on the basis of their real or perceived sexual or gender orientation, gender identity or bodily diversity, including through implementation of the National Intervention Strategy. The State party should also facilitate reporting and collection of data on sexual and gender-based crimes, and ensure that all such crimes are promptly and thoroughly investigated, that perpetrators are brought to justice and that victims have access to full reparation and means of protection, including access to State- and NGO-run shelters or centres throughout the State party's territory. The State party should also ensure adequate training for law enforcement and health service personnel regarding domestic and gender-based violence, and violence based on sexual orientation and gender identity.

#### **Civil remedies for victims of torture**

22. The Committee notes with concern that the Prevention and Combating of Torture of Persons Act does not itself provide for civil claims for redress of torture, and that such claims consequently need to be framed as a common law tort claim for assault or related less serious offences, since torture is not recognized as a tort (art. 2 and 7).

23. The State party should consider amending the Prevention and Combating of Torture of Persons Act with a view to including specific provisions relating to the right of civil redress and remedy for victims of torture.

#### **Corporal punishment**

24. The Committee is concerned that corporal punishment in the home is not prohibited, and is traditionally accepted and widely practiced, and that it is still lawful in private education institutions and continues to be used in certain schools as a means of discipline, despite its legal prohibition (arts. 7 and 24).

25. The State party should take practical steps, including through legislative measures, where appropriate, to put an end to corporal punishment in all settings.

#### **Excessive and disproportionate use of force**

26. The Committee is concerned about numerous reports of excessive and disproportionate use of force by law-enforcement officials in the context of public protests, which resulted in loss of lives. The Committee is also concerned about the slow pace of the investigation into the Marikana incident, including with respect to the criminal responsibility of members of the South African Police Service and the potential liability of the Lonmin Mining Company (arts. 6, 7 and 21).

27. The State party should:

(a) Expedite the work of the Ministry of Police Task Team, and the Panel of International Experts in implementing the recommendations of the Farlam Commission of Inquiry, revise laws and policies regarding public order policing and the use of force, including lethal force by law enforcement officials, to ensure that all policing laws, policies, and guidelines are consistent with article 6 of the Covenant and the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials;

(b) Take all necessary measures, particularly in terms of training and equipment to prevent law enforcement and security forces from using excessive force or using lethal weapons in situations that do not warrant recourse to such force;

H

(c) Ensure that prompt, thorough, effective, independent and impartial investigations are launched into all incidents involving the use of firearms and all allegations of excessive use of force by law enforcement officers, as well as the potential liability of the Lonmin Mining Company for the Marikana incident, prosecute and punish perpetrators of illegal killings, and provide effective remedies to victims; and

(d) Review the compliance of companies with their responsibilities under all relevant legal standards for operations in the mining sector.

#### **Violence, torture, ill-treatment, and deaths in custody**

28. The Committee is concerned about the number of reported cases of violence, including sexual violence, excessive use of force, torture and other forms of ill-treatment against detainees, as well as deaths resulting from actions of police and prison officials. It also notes with concern that few investigations into such reported cases have led to prosecutions resulting in the punishment of those responsible (arts. 2, 6, 7 and 10).

29. The State party should ensure that all deaths occurring in detention and all cases of violence, committed in State or contract-managed prisons are properly investigated by an independent mechanism. It should also ensure that perpetrators of and accomplices in such violent acts are duly prosecuted and punished in accordance with the law, and that victims and their families are provided with remedies, including rehabilitation and compensation.

#### **Prison conditions**

30. The Committee is concerned at poor conditions of detention in some of the State party's prisons, particularly with respect to overcrowding, dilapidated infrastructures, unsanitary conditions, inadequate food, lack of exercise, poor ventilation, and limited access to health services. The Committee notes with concern the conditions of detention in the two super-maximum security prisons and the segregation measures imposed, for instance in Ebongweni super-maximum prison where prisoners are locked up 23 hours a day for a minimum period of six months (art. 10).

31. The State party should continue to strengthen its efforts to improve conditions of detention by taking practical measures to, inter alia:

(a) Reduce overcrowding, particularly through the promotion of alternatives to detention, the loosening of bail requirements, and the revision of arrest quotas as indicators of police performance, and by ensuring that bail determinations are made promptly and that persons on remand are not kept in custody for an unreasonable period of time;

(b) Increase efforts to guarantee the right of detainees to be treated with humanity and dignity and ensure that conditions of detention in all of the country's prisons, including those operated by private contractors, are compatible with the United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules);

(c) Ensure that de facto solitary confinement measures, including segregation, are used only in the most exceptional circumstances and for strictly limited periods of a short duration.

#### **Human trafficking and labour exploitation**

32. While taking note of the progress made with regard to combating trafficking in persons, the Committee is concerned that the State Party still lacks proper identification and

referral mechanisms for victims of trafficking in persons. The Committee welcomes the adoption of the Labour Relations Amendment act, 2014 (Act No 6 of 2014), which provides greater protection for workers placed in temporary employment service, but it remains concerned at reports of migrant workers employed through labour brokers' services to work in the mining industry, who are victims of exploitative labour conditions (arts. 7, and 8).

33. The State party should continue its efforts to prevent and eradicate trafficking in persons and take the necessary steps to outlaw and hold responsible labour brokers involved in the exploitation of workers in violation of articles 7 and 8 of the Covenant. It should also step up its efforts to identify and protect persons who may be vulnerable to human trafficking and establish a nationwide identification and referral system for victims of trafficking.

#### Access to refugee determination process

34. The Committee is concerned at increased difficulties in accessing refugee status determination processes due to the closure of several urban Refugee Reception Offices, and about the reports of inadequate safeguards in the status determination process. The Committee is concerned about allegations that some immigration officers refuse to provide asylum seekers with transit permits at the port of entry, putting them at risk of immediate arrest or deportation. The Committee is concerned about allegations that these obstacles have resulted in the development of corrupt practices and have increased the vulnerability of migrants, especially children, rendering them undocumented and stateless (arts. 6, 7 and 13).

35. The State party should facilitate access to documentation and fair procedures for asylum seekers, including translation services and, where the interest of justice so require, access to legal representation. It should ensure that asylum applications are processed expeditiously and that the principle of non-refoulement is respected under all circumstances.

#### Immigration detention

36. The Committee is concerned about reports of: (a) cases of undocumented migrants detained in police stations and in prison facilities; (b) individuals detained at Lindela Repatriation Centre for lengthy periods of time without a warrant; and, (c) protracted detention of stateless persons and their deportation to countries where they were not recognised as citizens. It also notes with concern the poor conditions at Lindela Repatriation Centre, including overcrowding, lack of hygiene and of medical services (arts. 6, 9, 10 and 23).

37. The State party should ensure that detention pending deportation is applied as a last resort only, with special regard being given to the needs of particularly vulnerable persons, and that individuals detained for immigration-related reasons are held in facilities specifically designed for that purpose. The State party should also strengthen its efforts to ensure adequate living conditions in all immigration centres, by reducing overcrowding, providing adequate health-care services, and ensuring proper sanitary conditions.

#### Juvenile justice

38. The Committee welcomes the delegation's statement that the age of criminal responsibility will be increased from 10 to 12 years old, with a rebuttable presumption (*doli incapax*) for children aged between 12 and 14. The Committee also welcomes efforts to strengthen the juvenile justice system, but notes with concern the lack of funding allocated

to community diversion programmes and the over-use by courts of placement in Child and Youth Care Centres, where children in need of care are reportedly not always separated from children in conflict with the law (arts. 9, 10, 14 and 24).

39. The State party should allocate adequate funding to community based diversion programmes for children and reduce the number of children held in Child and Youth Care Centres. It should also ensure that children in conflict with the law are separated from children in need of care. When raising the age of criminal responsibility to 12 years old, the State party should ensure that the current level of protection afforded to children aged between 12 and 14 years old is maintained.

#### **Protection of Human Rights Defenders**

40. The Committee is concerned about reports of threats, intimidation, harassment, excessive use of force and physical attacks, some resulting in deaths, by private actors and police forces against human rights defenders, in particular those working on corporate accountability, land rights, and transparency issues, as well as LGBTI and HIV activists. It also notes with concern reports about the lack of due diligence of law enforcement officers in protecting human rights defenders, including registering and investigating allegations of human rights violations, and in securing accountability for such violations (arts. 2, 6, 9, 19, 21 and 22).

41. The State party should take all the necessary steps to protect the right of human rights defenders to freedom of expression, association and peaceful assembly. It should ensure that police officials receive adequate training regarding the protection of human rights defenders. The State party should also thoroughly investigate all attacks on the life, physical integrity and dignity of these persons, bring perpetrators to justice and provide victims with appropriate remedies.

#### **Right to privacy and interception of private communications**

42. The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Relation of Interception of Communications and Provisions and Provision of Communications Related Information Act (RICA). It is also concerned about the wide scope of the data retention regime under the Act. The Committee is further concerned at reports of unlawful surveillances practices, including mass interception of communications, carried out by the National Communications Centre and at delays in fully operationalizing the Protection of Personal Information Act, 2013, due in particular to delays in the establishment of an Information Regulator (arts. 17 and 21).

43. The State party should take all necessary measures to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality. The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization and consider revoking or limiting the requirement for mandatory retention of data by third parties. It should also ensure that interception of communications by law enforcement and security services is carried out only on the basis of the law and under judicial supervision. The State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies.

### **Land claims**

44. While welcoming the reopening of the land claims process and the development of a policy and legislation on exceptions to the 19 June 1913 cut-off date to accommodate the descendants of the Khoi-San communities, the Committee is concerned about delays in processing of claims before the Restitution Commission pursuant to the 1994 Restitution of Land Act, and the inability of Khoi-San communities dispossessed prior to 1913 to benefit from the land restitution process (art. 27).

45. The State party should step up its efforts to ensure the processing of land restitution claims lodged under the Restitution of Land Act, 1994, and the Restitution of Land Rights Amendment Act, 2014. In addition, it should consider legislative measures to ensure that dispossession of indigenous peoples of their lands prior to 1913 is adequately addressed.

### **Indigenous peoples**

46. While welcoming the introduction of the Traditional and Khoi-San Leadership Bill into parliament in September 2015, the Committee notes concerns raised by traditional and indigenous communities, including with regard to some of the recognition criteria. It is concerned that some of the Khoi-San languages are on the verge of extinction. In addition, the Committee is concerned that existing subsistence fishing quotas of indigenous groups have been taken away on a temporary basis without warning, leaving families with insufficient means of livelihood (arts. 2, 25, 26 and 27).

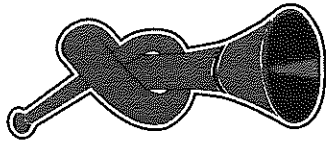
47. In consultation with indigenous and traditional communities, the State party should revise the Traditional and Khoi-San Leadership Bill with a view to taking into consideration their concerns. It should step up its efforts to promote and preserve Khoi and San indigenous languages. The State party should ensure that small scale fishing communities are not discriminated against in their access to traditional means of subsistence.

## **D. Dissemination of information relating to the Covenant**

48. The State party should widely disseminate the Covenant, the two Optional Protocols to the Covenant, its initial report, the written replies to the Committee's list of issues and the present concluding observations with a view to raising awareness of the rights enshrined in the Covenant among the judicial, legislative and administrative authorities, civil society and non-governmental organizations operating in the country, and the general public. The State party should ensure that the report and the present concluding observations are translated into its official languages.

49. Pursuant to rule 71, paragraph 5, of the rules of procedure of the Committee, the State party should provide, within one year, relevant information on the implementation of the recommendations made by the Committee in paragraph 13 (Truth and Reconciliation Commission), 15 (racism and xenophobia) and 31 (prison conditions) above.

50. The Committee requests the State party to submit its next periodic report by 31 March 2020 and to include in that report specific up-to-date information on the implementation of the recommendations made in the present concluding observations and of the Covenant as a whole. The Committee also requests the State party, in preparing the report, to broadly consult civil society and non-governmental organizations operating in the country, as well as minority and marginalized groups. In accordance with General Assembly resolution 68/268, the word limit for the report is 21,200 words.



# RIGHT2KNOW

26 April 2016

## **Joint statement STAND AGAINST SURVEILLANCE: FIX RICA NOW!**

This is a joint statement of civil society organisations committed to upholding human rights and seeking social justice in South Africa.

On 30 March 2016, the United Nations Human Rights Committee issued a strong condemnation of South Africa's surveillance capabilities, and the law that is meant to regulate them — the Regulation of Interception of Communications and Communication-Related Information Act (RICA).

We agree with the Human Rights Committee: South Africa's communications surveillance capabilities are untransparent, open to abuse, and a major threat to human rights in South Africa.

Evidence is mounting that these surveillance capabilities have been used to target investigative journalists, political activists, unionists, and interfere in South Africa's politics and public life.

Many of these abuses are possible because RICA lacks transparency or adequate safeguards, and because the most powerful mass surveillance capabilities are not regulated by RICA at all.

These capabilities potentially affect everyone. By forcing every user in South Africa to link their identity to a particular SIM card, and by forcing all telecommunications providers to store every user's metadata<sup>1</sup> for three to five years, RICA effectively puts every communications user in South Africa under mass, untargeted surveillance.

The right to privacy is a constitutionally-protected right in itself, contained in Section 14 of the Bill of Rights, but it is also central to other rights, including freedom of expression, freedom of association, media freedom and the right to dignity. In a contested constitutional democracy such as South Africa, the right to privacy is crucial to achieving and defending many other rights.

We therefore demand that the Department of Justice & Constitutional Development fix RICA now, through an open and public process.

### **Endorsed by:**

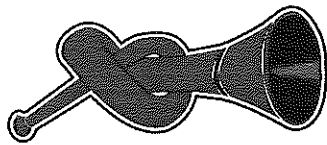
1. Alternative Information Development Centre (AIDC)
2. AmaBhungane Centre for Investigative Journalism
3. Awesome SA
4. Centre for Civil Society, University of KwaZulu-Natal
5. Centre for Environmental Rights
6. Corruption Watch
7. Council for the Advancement of the South African Constitution (CASAC)
8. Democracy Works Foundation
9. Diakonia Council of Churches
10. Environmental Monitoring Group

<sup>1</sup> Metadata is all the information about a communication, rather than the actual content of the communication (e.g. the identity of each party in a communication, the time and their locations, networks and devices). Once stored, it be used to create a huge, searchable database of every electronic interaction a person or community makes.

11. Equal Education
12. Equal Education Law Centre
13. Fossil Free South Africa
14. Freedom of Expression Institute
15. groundWork (Friends of the Earth South Africa)
16. Institute for Justice and Reconciliation (IJR)
17. Media for Justice
18. Media Policy & Democracy Project (MPDP)
19. Media Workers Association of South Africa
20. Ndifuna Ukwazi
21. OpenSecretsZA
22. Operation Khanyisa Movement
23. OWASP Cape Town
24. People Opposing Women Abuse
25. PSAM
26. RAM Network Security Services Pty Ltd
27. Right2Know Campaign
28. Section27
29. Social Justice Coalition
30. Sonke Gender Justice
31. South African Communications Association (SACOMM)
32. STEPS (Social Transformation & Empowerment Projects)
33. Students for Law and Social Justice
34. Sustaining the Wild Coast (SWC)
35. The Governance, Crime and Justice Division of the Institute for Security Studies
36. The Green Connection
37. World Wide Web Foundation
38. United Front

#





# RIGHT2KNOW

Embargoed until 2pm, Tuesday 26 April 2016

## Memorandum: Demands to Stand Against Surveillance and Fix RICA!

26 April 2016

On 30 March 2016, a report by the United Nations Human Rights Committee came down hard on South Africa's surveillance practices<sup>1</sup>.

The Human Rights Committee expressed concern at the Regulation of Interception of Communications and Provision of Communication-related Information Act (Rica), which allows law enforcement, intelligence agencies and the military to intercept communications with the permission of a judge. The Committee expressed concern that mass surveillance takes place outside the law in South Africa, which leaves the most powerful surveillance capacities of the state effectively unregulated. It also noted with concern that the grounds for the issuing of warrants authorising the interception of communications are too vague, and the state's system for interception of communications lacks transparency and accountability. All these problems make it more likely that the surveillance capacities of the state will be abused.

These concerns are not unique to South Africa, but they demand action from those committed to human rights in South Africa.

The right to privacy is a constitutionally-protected right in itself, contained in Section 14 of the Bill of Rights, but it is also foundational to other rights, including freedom of expression, freedom of association, media freedom and the right to dignity. In a contested constitutional democracy such as South Africa, the right to privacy is crucial to achieving and defending many other rights.

### Growing evidence of communication surveillance abuses in South Africa

In South Africa there is growing evidence that the state's powers of communications surveillance are abused. Examples include:

- Evidence has emerged that investigative journalists from at least two media organisations - Mzilikazi wa Afrika and Stephan Hofstatter from the Sunday Times and Sam Sole from the

---

<sup>1</sup> Human Rights Committee, *Concluding observations on the initial report of South Africa*, 30 March 2016. Available at: [www.r2k.org.za/wp-content/uploads/CCPR\\_C\\_ZAF\\_CO\\_1\\_23451\\_E.doc](http://www.r2k.org.za/wp-content/uploads/CCPR_C_ZAF_CO_1_23451_E.doc)

#

MP

amaBhungane Centre for Investigative Journalism - have had their phones bugged. Journalists need to protect the identity of their sources to make sure that crucial information about wrongdoing comes to light, but they cannot do so if their communications are intercepted.

- The fear of surveillance has become an increasing feature of many activist struggles. State security structures have openly monitored the activities of civil society formations, especially organisations in poor communities<sup>2</sup>.
- The 2008 Ministerial Review Commission on the Intelligence services ("The Matthews Commission") found that security and intelligence agencies have mass surveillance capabilities through an unregulated body called the National Communications Centre (NCC). Mass surveillance is not regulated by RICA or any other law, making it unlawful and unconstitutional<sup>3</sup>.
- Government agencies, private corporations and individuals have reportedly acquired "Grabber" devices, a surveillance technology capable of imitating a cell phone tower and identifying, locating and reading information from mobile phones in a certain area. "Grabber" technology is not adequately regulated by RICA<sup>4</sup>.
- Recent reports in the Mail & Guardian point to serious failings in RICA's safeguards<sup>5</sup>, and ongoing use of the state's unregulated mass surveillance capabilities<sup>6</sup>.

These and other examples are not only potentially criminal but represent a direct violation of fundamental constitutional rights which are at the heart of our democracy. They point to a system that is open to abuse, and in which abuses already take place.

These point to a need for urgent and radical reforms to RICA.

We therefore call on the Department of Justice and Constitutional Development as well as the Parliament of the Republic of South Africa to institute urgent reforms of RICA through an open and public process.

### **Key demands to reform RICA:**

---

2 *Big Brother Exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements*, April 2015. Available at: <http://bigbrother.r2k.org.za/>

3 Matthews Commission <http://www.r2k.org.za/matthews-commission>

4 Mail&Guardian, 29 November 2015, Available at: <http://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-celiphone-and-you>

5 Mail&Guardian, 11 November 2015, Available at: <http://mg.co.za/article/2015-11-12-big-brother-is-listening-on-your-phone>

6 Mail&Guardian, 17 December 2015, <http://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening>

### **1) Drop SIM card registration**

SIM card registration violates privacy in that 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. Research shows 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 wishing to remain anonymous<sup>7</sup>.

### **2) End mass storage of data**

RICA requires telecommunications and internet service providers to store *all* users' metadata (a detailed record of all messages and calls sent and received, all internet traffic, etc) for **3 to 5 years**. This means that every single communications user in South Africa is effectively subject to mass, untargeted surveillance. This kind of data retention was struck down in the EU by the European Court of Justice on the basis that it led to a serious interference with fundamental rights. Rather, RICA should make provision for targeted preservation orders, whereby communications companies are ordered to store the data only of certain individuals who are under investigation for serious offences.

### **3) Strengthen judicial protections against surveillance**

#### *3.1 Raise the threshold for issuing warrants*

RICA provides for warrants to be issued on speculative grounds, requiring only that there are "reasonable grounds to believe" that a serious criminal offence has been or is being or probably will be committed. This provision is open to abuse, and has led in at least one case to a warrant being issued to tap the phone of an investigative journalist. There must be a higher threshold.

#### *3.2 Metadata (archived data about the communication) must be better protected*

RICA requires that only a specifically designated judge can issue a warrant to intercept someone's communications or metadata in real time. However, any sitting magistrate or high court judge can issue a warrant for metadata that has been stored under RICA's three-to-five year data storage provision. There appears to be no oversight or reporting on how often magistrates and high court judges issue such warrants. Given that metadata is often as sensitive as the content of the communication, the same safeguards should apply, and only a specially designated judge should have authority to issue warrants.

### **4) Greater transparency**

#### *4.1 Users must be notified when their data has been intercepted*

---

<sup>7</sup> Donovan, K.P. and Martin, A.K., 2012, 'The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance'. Information Systems and Innovation Group Working Paper no. 186, London School of Economics and Political Science, London, UK.

RICA's secrecy provisions forbid any authority from notifying users if their communications have been spied on, even after the warrant has lapsed and any investigation is concluded or at a non-sensitive stage. This creates a situation that is ripe for abuse, as people who are subject to surveillance have no way of knowing that their rights have been violated. All users should be notified; only under exceptional circumstances should the judge have the power to defer notification.

#### *4.2 Network providers and internet service must disclose how often their customers' are intercepted*

The telecommunications industry has accepted the blanket secrecy demanded by RICA and are forbidden from ever disclosing when they have helped law enforcement or intelligence agencies intercept their customers' communications. RICA must require them to release annual transparency reports revealing annually how often this happens.

#### *4.3 Ensure greater transparency around communications surveillance*

There is a general lack of transparency around the uses of the surveillance capacities of the state. Much more information needs to be provided for the public to establish whether the government is using these capacities in ways that are both necessary and proportionate, and that serve legitimate aims. The only form of reporting required under RICA is a brief annual report by the designated RICA judge, which lacks detail and which is withheld by Parliament's intelligence committee for up to a year before its public release.

### **5) Better and more oversight**

#### *5.1 There needs to be independent oversight of the work of the Rica judge*

The Rica judge's only reporting role is an annual report for the Joint Standing Committee on Intelligence on the directions. This turns the judge into an arbiter of his or her own powers. Rather than an independent oversight body is needed to review the designated judge's performance in terms of RICA.

#### *5.2 Appoint key surveillance watchdog figures*

It remains a point of great concern that key watchdog roles are vacant, with no clear timeline for them to be filled. The Inspector General of Intelligence has been vacant since April 2015, as a Parliamentary process to appoint a new, independent Inspector General has dragged on unacceptably long. The Information Regulator, a data protection watchdog created through the Protection of Personal Information Act, has yet to be established and there is no clear time frame or sense of urgency in setting up this watchdog role. This has left the public with no adequate protection or oversight against abusive surveillance practices. Strong, independent and transparent candidates must be appointed urgently to those posts.

MH

HT

## **6) End unregulated mass surveillance**

The government has insisted that the activities of the National Communications Centre – which to our knowledge houses the mass surveillance capacities of the state for the purpose of ‘foreign signals intelligence’ gathering – remain unregulated by RICA. This means that the state’s most powerful communications surveillance body is effectively unregulated by law, which opens the door to widespread abuses. The activities of the NCC, and any mass surveillance capabilities of the state, must be strictly regulated under RICA.

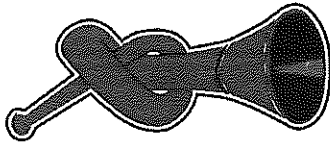
## **Conclusion**

Legal reforms are only a first step in ensuring an end to surveillance abuses; much more needs to be done. However, they are a vital step. Unregulated and controlled surveillance are a violation of human rights and pose a serious threat to democratic participation in South Africa.

#Ends

#

mit



# RIGHT2KNOW

**NATIONAL & WESTERN CAPE**  
 107 Community House  
 41 Salt River Rd  
 Salt River, Cape Town  
 Tel: 021 447 1000  
 Admin@r2k.org.za  
 WesternCape@r2k.org.za

**KWA ZULU NATAL**  
 101 Dinvir Centre,  
 121 Field (Joe Slovo) St  
 Central, Durban  
 Tel: 031 301 0914  
 KZN@r2k.org.za

**GAUTENG**  
 5th floor, Heerengracht Building  
 87 De Korte St  
 Braamfontein, Johannesburg  
 Tel: 011 339 1533  
 Gauteng@r2k.org.za

To: Office of the Designated Judge  
 Judge Maluleke  
 Department of Justice & Constitutional Development  
 By email: mmPhahlane@justice.gov.za

17 March 2017

Your Honour Judge Maluleke,

1. I write to you on behalf of the Right2Know Campaign (R2K), to acknowledge your appointment to the Office of the Designated Judge in 2016, and request an opportunity to engage your Office on annual reporting by your Office in terms of the oversight provisions of the Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA). This letter follows several years of R2K's work on RICA and state surveillance issues, leading to engagements with the Deputy Minister of Justice.
2. R2K is a civil society movement centered on freedom of expression and access to information. It is a democratic, citizen-driven campaign that aims to raise public awareness, mobilise communities and undertake research and advocacy that further the Constitutional values of transparency, openness and the free flow of information.
3. Since its founding in 2010, R2K's work has included public scrutiny of the work of South Africa's intelligence agencies. In recent years especially, R2K has voiced concern that the state's surveillance capabilities have been used unlawfully and to violate constitutional rights, and in some instances to undermine the judicial oversight put in place by RICA. Our work in this area has included research, policy analysis, political mobilisation, parliamentary advocacy, and direct engagement with the Department of

Justice and Constitutional Development. Among other things, this work contributed to the United Nations Human Rights Committee's findings on South Africa's surveillance practices in relation to the International Covenant of Civil and Political Rights (ICCPR) in 2016<sup>1</sup>. R2K has developed a memorandum of concerns about RICA<sup>2</sup>, endorsed by over 40 civil society organisations across South Africa. Following this work, the Deputy Minister of Justice has informed us that the Act may soon undergo legislative review.

4. The memorandum raised the following concerns to be address:
  1. Mandatory registration of SIM card;
  2. Mass retention of users' communication-related information;
  3. A need to strengthen judicial protections;
  4. A need for greater transparency within the RICA oversight regime, including:
    - i. Notification of users of interception of communications;
    - ii. Transparency reports from communication service providers;
    - iii. Improved reporting from designated judges and state transparency reports;
    - iv. Improved oversight structures;
  5. Evidence of mass surveillance practices that have not been sufficiently regulated or curtailed.
5. We appreciate the crucial oversight role of the designated judges in terms of RICA, both in ensuring compliance from law-enforcement agencies, and in providing information needed for public oversight and understanding of RICA's implementation. The annual reports of the Office of the Designated Judge to Parliament have been vital to public oversight of the state's implementation of RICA. We welcome the detail and consistency in these reports in recent years; these have contributed to greater public insight into the Act's implementation. Indeed, the above-mentioned memorandum of concerns was drawn from disclosures made in the annual reports of your predecessor.
6. Our specific request to you, as an organisation that uses the information in these reports to develop policy proposals and improve public understanding of the implementation of RICA, is to consider specific recommendations that we would have

---

<sup>1</sup> UNHCR, *Concluding observations on the initial report of South Africa*, CCPR/C/ZAF/CO/1 (April 2016), s43-44.

<sup>2</sup> Memorandum, 'Demands to Stand Against Surveillance and Fix RICA' (April 2016). Available at [www.r2k.org.za/rica-demands](http://www.r2k.org.za/rica-demands)



regarding the format and detail that might be included in annual reports by the Office of the Designated Judge. These would aim to aid public oversight and research of RICA, in line with the objectives of the Act and without breaching the necessary confidentiality measures in the Act. In light of a possible legislative reform process in the future, this would also assist any deliberations in that regard. We would therefore request an opportunity for Right2Know to put these recommendations before your office for consideration.

7. In addition, for the purposes of information sharing, we would also be happy to share with you briefing materials and research that was prepared for the Department of Justice and Constitutional Development, outlining broader concerns with some provisions of RICA and related communications-interception practices of the South African government.

8. We humbly appeal to you to consider this request.

Sincerely,



**Murray Hunter**  
Advocacy Coordinator  
Right2Know Campaign  
Telephone: 021 447 3007  
Email: murray@r2k.org.za

MH





**the doj & cd**

Department:  
Justice and Constitutional Development  
REPUBLIC OF SOUTH AFRICA

Mr Murray Hunter  
Advocacy Coordinator  
Right@Know Campaign  
107 Community House  
41 Salt River Road  
Salt River  
Cape Town

E-mail: [murray@r2k.org.za](mailto:murray@r2k.org.za)

Dear Mr Hunter

**REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION  
OF COMMUNICATION-RELATED INFORMATION ACT, 2002: FORMAT AND  
DETAIL WHICH MUST BE INCLUDED IN REPORT TO JOINT STANDING  
COMMITTEE ON INTELLIGENCE**

Your letter dated 17 March 2017, in which suggestions were made regarding the format and content of the report that is required to be submitted to the Joint Standing Committee on Intelligence (the Committee) in terms of the Intelligence Services Oversight Act, 1994 (Act 40 of 1994) (the Act), has reference.

The reporting function of the designated judge is regulated by section 3(a)(ii) of the Act, which requires that the Committee must obtain from the designated judge a report regarding the functions performed by him or her in terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002) (the RICA), including statistics regarding such functions, together with any comments or recommendations which such designated judge may deem appropriate. Section 3(a)(ii) of the Act further provides that such report shall not disclose any information contained in an application or direction referred to in the RICA.

The need for transparency and oversight in respect of the interception of communications and the provision of communication-related information is acknowledged as essential in a democratic society. I do not intend to deviate from the format and content of the reports of my predecessor.

I was made aware of the fact that the Department of Justice and Constitutional Development (the Department) is considering amendments to the RICA. I would therefore request you to engage with the Department on possible amendments to the RICA, which may also include any suggestions which you would like to make in respect of the form and detail of any report by a designated judge regarding his or her responsibilities in terms of the RICA.

With kind regards

MH

#



Judge GSS Matuleke  
Designated Judge  
Date: 10/04/2017

#  
M14

## Constitutional Litigation Unit

16<sup>th</sup> Floor Bram Fischer Towers • 20 Albert Street • Marshalltown • Johannesburg 2001 • South Africa  
 PO Box 9495 • Johannesburg 2000 • South Africa  
 Tel: (011) 838 6601 • Fax: (011) 834 4273 • Website: [www.lrc.org.za](http://www.lrc.org.za)  
 PBO No. 930003292  
 NPO No. 023-004

LRC

Legal Resources Centre

Your Ref: Case no. 25978/17  
 Our Ref: M Kekana / 1125816L

16 October 2017

3 Pages

**For the attention of:**

Dario Milo  
 Webber Wentzel Attorneys  
 Attorneys for the Applicants  
 By email: [dario.milo@webberwentzel.com](mailto:dario.milo@webberwentzel.com)

**And to:**

M Kgoroadira  
 Kgoroadira Mudau Inc  
 Attorneys for the 2<sup>nd</sup>, 7<sup>th</sup>, 8<sup>th</sup> & 10<sup>th</sup> Respondents  
 By email: [rapulane@kgoroadiramudauinc.co.za](mailto:rapulane@kgoroadiramudauinc.co.za)

**And to:**

Office of the State Attorney  
 Attorneys for the 1<sup>st</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, 5<sup>th</sup>, 6<sup>th</sup> & 9<sup>th</sup> respondents  
 By email:

**With a copy to:**

Registrar of the High Court of South Africa  
 Gauteng Provincial Division, Pretoria  
 By email

Dear Sir / Madam

**amaBhungane and Another v Minister of Justice and Correctional Services and Others  
 (Case No. 25978/17): Request For Consent to Intervene as an *Amicus Curiae***

1. We act for the Right2Know Campaign (R2K), a civil society organisation whose objective is to serve the public interest.
2. R2K is a democratic, activist-driven campaign that equips and unites citizens to raise public awareness, mobilise communities, and undertake research and targeted advocacy that aims to ensure the free flow of information necessary to meet people's social,

National Office:  
 Cape Town:  
 Durban:  
 Grahamstown:  
 Johannesburg:  
 Constitutional Litigation Unit:

J Love (National Director), T Wegenif (Deputy National Director), K Reinecke (Director: Finance), EJ Broster  
 SG Magardie (Acting Director), A Andrews, S Kahanovitz, WR Kerfoot, C Malthiso, C May, M Mudarikwa, EL Roos, HJ Smith  
 S Samuel (Director), E Deochand, T Mbense, A Turpin  
 S Sephton (Director), C McConnachie, LK Jobele  
 N Fakir (Director), AF Ashton, Z Khumalo, KS Kropman, LJD Limacher, SP Mkhize, MJ Power  
 SG Magardie (Director), MJ Bishop, G Bizos SC, C du Toit, A Singh, LK Siyo, ER Webber, WC Wicomb

MH

#

economic, political and ecological needs and live free from want, in equality and in dignity. In this regard, our client mobilises on three main issues:

- 2.1 To stop secrecy, in particular to ensure that security legislation and the conduct of security agencies are aligned to the Constitution of the Republic of South Africa, 1996 ("the Constitution") and its underlying values;
  - 2.2 Information access, in particular to ensure that public and private sector information is easily accessible to citizens and that people with information of wrongdoing and/or of the suppression of information in the public interest are free and encouraged to share information with the public; and
  - 2.3 Communication rights, in particular to ensure that South Africa enjoys a free and diverse range of public, private and non-profit media and affordance access to the open and secure internet and telecommunications.
3. R2K has considered the notice of motion, founding affidavit and answering affidavit on behalf of the 2<sup>nd</sup>, 7<sup>th</sup>, 8<sup>th</sup> & 10<sup>th</sup> Respondents in this matter.
4. R2K believes that, in light of the work that our client has engaged in relating to surveillance and the security agencies, it can make novel legal submissions that will be useful to the Court. We are therefore instructed to approach you pursuant to Uniform Court Rule 16A, to request your written consent for R2K to enter this matter as an *amicus curiae*.
5. Our client will not repeat the submissions of the other parties to the proceedings. It intends to make submissions on the following issues:
- 5.1 The importance of post-interception notification to surveilled persons for access to justice. R2K support the Applicants' argument, and intends to assist the Court providing comparative jurisprudence that supports the need for user notification.
  - 5.2 The Applicants attack RICA's provisions concerning the mandatory retention of communication related data (metadata). Their argument focuses on the length of time for which the metadata is retained. R2K will argue that the bulk retention of metadata is always unconstitutional, no matter the length for which it is kept. It will argue that only targeted retention of metadata is constitutionally permissible. In advancing that position, R2K will draw on international and comparative jurisprudence that supports the ban on blanket retention of metadata.
  - 5.3 The Applicants argue that RIC does not adequately secure the independence of the designated judge. R2K agrees. However, it will argue that, in addition to the matters identified by the Applicants, the independence of the designated judge is further compromised by the lack of: (a) clear legal requirements for reporting; and (b) a more adversarial process that adequately protects the rights of surveillance targets. Both of these serve to undermine the perceived independence of the designated judge in the eyes of a reasonable person.

The unconstitutionality of mass surveillance conducted by the National Communications Centre due to the universal nature of the surveillance conducted and absence of empowering legislation.

6. Accordingly, we hereby request your client's consent that our client be admitted as *amicus curiae* with the right to make written submissions and to present oral argument.
7. We ask that advise whether your client consents to our client's intervention by no later than close of business on **30 OCTOBER 2017**.
8. We look forward to hearing from you. All our client's rights are reserved.

Yours faithfully

**LEGAL RESOURCES CENTRE**

Per: Mosima Kekana  
011 836 9831  
mosima@lrc.org.za

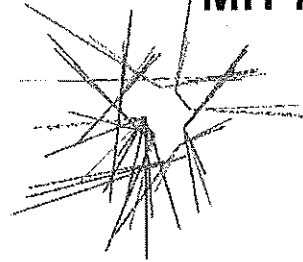
MH

#

## WEBBER WENTZEL

in alliance with > Linklaters

MH 7



**Attention: Mosima Kekana**  
Legal Resources Centre  
16<sup>th</sup> Floor Bram Fischer Towers  
20 Albert Street  
Marshalltown  
Johannesburg 2001

90 Rivonia Road, Sandton  
Johannesburg, 2196  
PO Box 61771, Marshalltown  
Johannesburg, 2107, South Africa  
Docex 26 Johannesburg  
T +27 11 530 5000  
F +27 11 530 5111

[www.webberwentzel.com](http://www.webberwentzel.com)

By email: [mosima@lrc.org.za](mailto:mosima@lrc.org.za)

Your reference  
M Kekana / 1125816L

Our reference  
D Milo / L Pillay  
3000547

Date  
24 October 2017

Dear Sir

**amaBhnngane and Another v Minister of Justice and Correctional Services and Others**  
**(Case No. 25978/17): Request for Consent to Intervene as an *Amicus Curiae***

1. We act for the Applicants in the above matter.
2. We refer to your letter of 16 October 2017 ("**your letter**"). Our clients hereby consent to your client's request to be admitted as *amicus curiae* in the above matter on the basis set out in your letter.

Yours truly

## WEBBER WENTZEL

Dario Milo

Partner

Direct tel: +27 11 530 5232

Direct fax: +27 11 530 6232

Email: [dario.milo@webberwentzel.com](mailto:dario.milo@webberwentzel.com)

*Sent electronically without signature*

**Senior Partner:** JC Els **Managing Partner:** SJ Hutton **Partners:** BW Abraham RB Africa NG Alp OA Ampofo-Anti RL Appelbaum DC Bayman AE Bennett AP Blair DHL Booysen AR Bowley JL Brink S Browne MS Burger RI Carrim T Cassim SJ Chong A Christie KL Collier KM Colman KE Coster K Couzyn JJ Daniels CR Davidow JH Davies PM Daya L de Bruyn PU Dela JHB de Lange DW de Villiers BEC Dickinson MA Diemont DA Dingley G Driver HJ du Preez CP du Toit SK Edmundson AE Esterhuizen MJR Evans AA Felekis GA Fichardt G Fitzmaurice JB Forman C Gabriel CP Gaul KL Gawith OH Geldenhuys MM Gibson SJ Gilmour H Goolam CI Gouws PD Grealy A Harley JM Harvey MH Hathorn JS Henning KR Hillis XNC Hlatshwayo S Hockey CM Hofeld PM Holloway HF Human AV Ismail ME Jarvis CM Jonker S Jooste LA Kahn M Kennedy A Keyser M Kyle J Lamb L Marais S McCafferty MC McIntosh SJ McKenzie M McLaren SI Meltzer CS Meyer AJ Mills JA Milner D Milo NP Mngomezulu S Mogale M Moloi LE Mostert VM Movshovich RA Nelson BP Ngoepe A Ngubo ZN Ntshona MB Nzimande L Odendaal GJP Olivier N Paige AMT Pardini AS Parry S Patel GR Penfold SE Phajane TC Phala MA Phillips D Ramjettan GI Rapson Z Rawoot K Rew G Richards-Smith NJA Robb DC Rudman S Rugan M Sader H Samsodien JW Scholtz KE Shepherd AJ Simpson N Singh N Singh-Nogueira P Singh J Smit MP Spalding PS Stein MW Straeuli LJ Swaine JM Swanepoel Z Swanepoel A Thakor A Toefy PZ Vanda PP van der Merwe SE van der Meulen CS Vanmali JE Veeran D Venter B Versfeld MG Versfeld TA Versfeld DM Visagie J Watson DP Wild KL Williams K Wilson RH Wilson M Yudaken **Chief Operating Officer:** SA Boyd

Webber Wentzel is associated with ALN

MH

11

**WEBBER WENTZEL**

in alliance with > Linklaters

Page 2

CC: Kgoroadira Mudau Inc: [rapulane@kgoroadiramudauinc.co.za](mailto:rapulane@kgoroadiramudauinc.co.za)

The State Attorney: [MeMakhubela@justice.gov.za](mailto:MeMakhubela@justice.gov.za)



MH

From: Mosima Kekana [mosima@lrc.org.za](mailto:mosima@lrc.org.za)  
 Subject: FW: AmaBhungane and Another / Minister of Justice and Correctional Service and Others  
 Date: 11 July 2018 at 13:29  
 To: Carina du Toit [carina@lrc.org.za](mailto:carina@lrc.org.za), [simon@lrc.org.za](mailto:simon@lrc.org.za)



Please find herewith consent from the state attorney.

Mosima

-----Original Message-----

From: Makhubela Meshack [<mailto:MeMakhubela@justice.gov.za>]  
 Sent: Friday, 03 November 2017 8:21 AM  
 To: Mosima Kekana; [rapulane@kgoroadiramudauinc.co.za](mailto:rapulane@kgoroadiramudauinc.co.za);  
[dario.milo@webberwentzel.com](mailto:dario.milo@webberwentzel.com)  
 Cc: Tsanga Mukumba  
 Subject: RE: AmaBhungane and Another / Minister of Justice and Correctional  
 Service and Others  
 Importance: High

GOOD MORNING

The above matter refers.

Kindly be advised that our client do not have a problem with your client to  
 intervene in these proceedings.

Regards

Meshack Tiyane Makhubela  
 Senior Assistant State Attorney  
 Office of the State Attorney - Pretoria  
 Tel: 012 309 1630  
 Fax: 086 640 1943  
 Cell: 083 753 6229  
 Email: [memakhubela@justice.gov.za](mailto:memakhubela@justice.gov.za) / [mtiyani1@gmail.com](mailto:mtiyani1@gmail.com)  
 Website:  
[https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.doj.gov](https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.doj.gov.za&umid=90960F33-5D0E-1D05-ABF4-9059839F8392&auth=223f124b9888cf0f5fd3685bb9dec53a7cc7de-a75ae76df37da8669f5d2d3c9c0d65a2fde5f1ac)  
[za&umid=90960F33-5D0E-1D05-ABF4-9059839F8392&auth=223f124b9888cf0f5fd368](https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.doj.gov.za&umid=90960F33-5D0E-1D05-ABF4-9059839F8392&auth=223f124b9888cf0f5fd3685bb9dec53a7cc7de-a75ae76df37da8669f5d2d3c9c0d65a2fde5f1ac)  
[5bb9dec53a7cc7de-a75ae76df37da8669f5d2d3c9c0d65a2fde5f1ac](https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.doj.gov.za&umid=90960F33-5D0E-1D05-ABF4-9059839F8392&auth=223f124b9888cf0f5fd3685bb9dec53a7cc7de-a75ae76df37da8669f5d2d3c9c0d65a2fde5f1ac)  
 "I can do all things through Christ who strengthens me" Philippians 4:13

-----Original Message-----

From: Mosima Kekana [<mailto:mosima@lrc.org.za>]  
 Sent: Monday, October 30, 2017 3:48 PM  
 To: [rapulane@kgoroadiramudauinc.co.za](mailto:rapulane@kgoroadiramudauinc.co.za); Makhubela Meshack  
 Cc: Tsanga Mukumba  
 Subject: RE: AmaBhungane and Another / Minister of Justice and Correctional  
 Service and Others

Good Day

I refer to the above matter and the attached correspondence which was  
 forwarded to your respective offices on the 16th of October 2017 and have to  
 date not received any response thereto . Kindly but urgently favour us with  
 your response herein .

Kind Regards  
 Mosima Kekana  
 Attorney

I Tel: 011 838 6601 I Fax: 011 838-4876 I Email: [mosima@lrc.org.za](mailto:mosima@lrc.org.za)  
 I Physical : 16th Floor Bram Fischer Towers I 20 Albert Street I  
 Johannesburg I  
 I Postal: P.O Box 9495 I Johannesburg 2000 I  
 I Website:  
 I [https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.](https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.lrc.org.za%2fa0&umid=41B87E02-5CC3-E805-B78C-B8293CB6CB1B&auth=223f124b9888cf0f5fd3685bb9dec53a7cc7de-60e681ee87a14b6e0f4c639ad82081f340717d6db)  
[lrc.org.za%2fa0&umid=41B87E02-5CC3-E805-B78C-B8293CB6CB1B&auth=223f12](https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.lrc.org.za%2fa0&umid=41B87E02-5CC3-E805-B78C-B8293CB6CB1B&auth=223f124b9888cf0f5fd3685bb9dec53a7cc7de-60e681ee87a14b6e0f4c639ad82081f340717d6db)  
[4b9888cf0f5fd3685bb9dec53a7cc7de-60e681ee87a14b6e0f4c639ad82081f3407](https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.lrc.org.za%2fa0&umid=41B87E02-5CC3-E805-B78C-B8293CB6CB1B&auth=223f124b9888cf0f5fd3685bb9dec53a7cc7de-60e681ee87a14b6e0f4c639ad82081f340717d6db)  
[17d6db](https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.lrc.org.za%2fa0&umid=41B87E02-5CC3-E805-B78C-B8293CB6CB1B&auth=223f124b9888cf0f5fd3685bb9dec53a7cc7de-60e681ee87a14b6e0f4c639ad82081f340717d6db) I Johannesburg I Cape Town I Durban I Grahamstown I

#

MH



-----Original Message-----

From: Mosima Kekana [mailto:[mosima@lrc.org.za](mailto:mosima@lrc.org.za)]  
Sent: Monday, 16 October 2017 1:19 PM  
To: [dario.milo@webberwentzel.com](mailto:dario.milo@webberwentzel.com); [rapulane@kgoroeadiramudauinc.co.za](mailto:rapulane@kgoroeadiramudauinc.co.za)  
Subject: AmaBhungane and Another / Minister of Justice and Correctional Service and Others

Good Day

Please find attached hereto, correspondence for your urgent attention.

Kind Regards

Mosima Kekana  
Attorney

I Tel: 011 838 6601 | Fax: 011 838-4876 | Email: [mosima@lrc.org.za](mailto:mosima@lrc.org.za)  
I Physical : 16th Floor Bram Fischer Towers | 20 Albert Street |  
Johannesburg |  
I Postal: P.O Box 9495 | Johannesburg 2000 |  
I Website:  
<https://imsva91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=www.lrc.org.za%2c%a0&umid=90960F33-5D0E-1D05-ABF4-9059839F8392&auth=223f124b9888cf0f5fd13685bb9dec53a7cc7de-36d6fbb340ca9e0ca913bb013048588ea68cf731> |  
I Johannesburg | Cape Town | Durban | Grahamstown |

Privileged/Confidential information may be contained in this message. If you are not the addressee indicated in this message (or responsible for delivery of the message to such person) you may not copy or deliver this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply E-Mail. Please advise immediately if you or your employer do not consent to e-mail messages of this kind. Opinions, conclusions and other information in this message that do not relate to the official business of the Department of Justice and Constitutional Development shall be understood as neither given nor endorsed by it. All views expressed herein are the views of the author and do not reflect the views of the Department of Justice unless specifically stated otherwise.



MIT

## Constitutional Litigation Unit

16<sup>th</sup> Floor Bram Fischer Towers • 20 Albert Street • Marshalltown • Johannesburg 2001 • South Africa  
 PO Box 9495 • Johannesburg 2000 • South Africa  
 Tel: (011) 838 6601 • Fax: (011) 834 4273 • Website [www.lrc.org.za](http://www.lrc.org.za)  
**PBO No. 930003292**  
**NPO No. 023-004**



Your Ref: Case no. 25978/17

Our Ref: M Kekana / 1125816L

26 June 2018  
 3 Pages

**For the attention of:**

Dario Milo  
 Webber Wentzel Attorneys  
 Attorneys for the Applicants  
 By email: [dario.milo@webberwentzel.com](mailto:dario.milo@webberwentzel.com)

**And to:**

M Kgoroadira  
 Kgoroadira Mudau Inc  
 Attorneys for the 2<sup>nd</sup>, 7<sup>th</sup>, 8<sup>th</sup> & 10<sup>th</sup> Respondents  
 By email: [rapulane@kgoroadiramudauinc.co.za](mailto:rapulane@kgoroadiramudauinc.co.za)

**And to:**

Office of the State Attorney  
 Attorneys for the 1<sup>st</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, 5<sup>th</sup>, 6<sup>th</sup> & 9<sup>th</sup> respondents  
 By fax: M Makubela – 0860 640 1943

---

Dear Sir / Madam

**amaBhungane and Another v Minister Of Justice And Correctional Services And Others (Case No. 25978/17): Request For Consent to Intervene as an *Amicus Curiae***

1. We act for the Right2Know Campaign (LRC), a civil society organisation whose objective is to serve the public interest.

2. On 8 October 2017, we wrote on behalf of our client, requesting consent to enter the abovementioned matter as *amicus curiae*.
3. All parties granted consent.
4. R2K has subsequently been approached by Privacy International in relation to the submissions to be made and expressed an interest in the matter.
5. Privacy International has a strong interest in the matter based upon the following:
  - 5.1. Privacy International is a non-profit, non-governmental organization based in London, the United Kingdom, which defends the right to privacy around the world. It conducts research and investigations into government and corporate surveillance activities with a focus on the policies and technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of Colombia, South Korea, the United States, the U.K., and Europe, including the Court of Justice of the European Union ("CJEU") and the European Court of Human Rights ("ECtHR"). Privacy International contributes regularly to the activities of United Nations human rights bodies, such as the U.N. Human Rights Committee, the Universal Periodic Review, and U.N. special procedures.
  - 5.2. Privacy International has litigated several cases addressing issues central to the main application. In particular, Privacy International is one of the applicants in *10 Human Rights Organisations v. United Kingdom*, a case currently before the ECtHR, challenging aspects of the U.K.'s surveillance regime.
  - 5.3. Privacy International, together with Open Rights Group, also intervened in the case of *Secretary of State for the Home Department v. Tom Watson and Others*, which was decided by the CJEU in 2016 (jointly with *Tele2 Sverige AB v. Post- Och telestyrelsen*). Those cases involved respective challenges to the UK and Swedish national data retention

regimes, which mandated telecommunications companies retain communications data (or metadata).

6. R2K has agreed to partner with Privacy International for purposes of this matter. We are therefore writing to inform you that Privacy International and the Right2Know Campaign will file a joint application for admission as *amici curiae*.
7. The submissions will remain as described in the letter of 18 September 2017, and we believe that no party will be prejudiced by the expertise contributed by Privacy International.
8. We are in the process of finalising our clients' application for admission, which we hope to file next week (week of 2 July 2018). Should any party have an objection to the admission of Privacy International together with R2K, we request that you let us know by Friday 29 June 2018.
9. We look forward to hearing from you.

Yours faithfully

**LEGAL RESOURCES CENTRE**

Per: Carina du Toit  
011 836 9831  
Carina@lrc.org.za

MA

H



**KGOROEADIRA MUDAU INC**

4 July 2018

LEGAL RESOURCES CENTRE

Per email: [Carina@lrc.org.za](mailto:Carina@lrc.org.za)

Our Ref: MK0002xm

Your Ref: M Kekana/1125816L

Dear Sir / Madam,

Re: **AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM / MINISTER OF STATE SECURITY**

We refer to your letter dated the 26<sup>th</sup> June 2018 as well as the telephonic conversation of even date between the writer and your Simon Ferreira.

We confirm that we are obtaining our clients' instructions and will revert back to you.

May you kindly advise what Privacy International's interest in the national policies and/or legislation of South Africa is.

Yours faithfully,

**Kgoroeadira Mudau Inc**

Per: RGM Kgoroeadira

#

MH

**From:** Carina@lrc.org.za  
**Subject:** RE: Amabhungane Center for Investigative Journalism / Minister of State Security  
**Date:** 05 July 2018 at 12:58  
**To:** info@kgoroadiramudauinc.co.za  
**Cc:** simon@lrc.org.za

---

Your Ref: MK0002xm  
Our Ref: M Kekana/1125816L

Dear Mr Kgoroadira

Your letter of 4 July refers.

With regard to your specific question, Privacy International (PI) is a *global* NGO and the scope of its international interest include South Africa. As previously noted in our correspondence PI "conducts research and investigations into government and corporate surveillance activities with a focus on the policies and technologies that enable these practices". This includes South African government activities and policies, which are matters arising in the abovementioned case, and the activities and policies of various other countries. In addition, PI "advocates for strong national, regional, and international laws"; and South African legislation has been included in their focus.

We point out that PI wishes to participate as a friend of the court. The international and comparative experience highlighted in our previous letter has direct relevance to the issues in this matter. The unique perspective PI is able to bring due to its global reach will assist the court by providing context and allowing an international comparison.

Kind regards

**Carina du Tolt | Attorney**  
**Constitutional Litigation Unit**

cid:image001.png@01D20463.69993F50

Tel: 011 836 9831	Fax: 011 838 4876	Email: [carina@lrc.org.za](mailto:carina@lrc.org.za)
Physical : 16<sup>th</sup> Floor Bram Fischer Towers	20 Albert Street	Johannesburg
Postal: P.O Box 9495	Johannesburg 2000	
Website: [www.lrc.org.za](http://www.lrc.org.za)		
Johannesburg	Cape Town	Durban



cid:image004.gif@01CEC106.27B7E210

**IN THE HIGH COURT OF SOUTH AFRICA  
(GAUTENG DIVISION, PRETORIA)**

The matter between:

**Case no: 25978/17**

**AMABHUNGANE CENTRE FOR INVESTIGATIVE  
JOURNALISM NPC**

**1<sup>st</sup> Applicant**

**SOLE STEPHEN PATRIC**

**2<sup>nd</sup> Applicant**

**And**

**MINISTER OF JUSTICE AND CORRECTIONAL  
SERVICES**

**1<sup>st</sup> Respondent**

**MINISTER OF STATE SECURITY**

**2<sup>nd</sup> Respondent**

**MINISTER OF COMMUNICATIONS**

**3<sup>rd</sup> Respondent**

**MINISTER OF DEFENCE AND MILITARY VETERANS**

**4<sup>th</sup> Respondent**

**MINISTER OF POLICE**

**5<sup>th</sup> Respondent**

**THE OFFICE OF INSPECTOR-GENERAL  
OF INTELLIGENCE**

**6<sup>th</sup> Respondent**

**THE OFFICE FOR INTERCEPTION CENTRES**

**7<sup>th</sup> Respondent**

**THE NATIONAL COMMUNICATIONS CENTRE**

**8<sup>th</sup> Respondent**

**THE JOINT STANDING COMMITTEE ON INTELLIGENCE**

**9<sup>th</sup> Respondent**

**THE STATE SECURITY AGENCY**

**10<sup>th</sup> Respondent**

---

**CONFIRMATORY AFFIDAVIT**

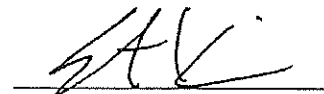
---

I, the undersigned

**SCARLET KIM**

state under oath/affirm and declare as follows:

1. I am an adult female and employed as the Legal Officer for Privacy International currently situated at 62 Britton Street, London EC1M 5UY.
2. I am duly authorised to depose to this affidavit on behalf of Privacy International.
3. The facts contained herein are to the best of my knowledge true and correct and, unless otherwise stated or indicated in the context, are within my personal knowledge.
4. I have read the signed affidavit of Murray Hunter and confirm the content thereof insofar as it relates to myself and Privacy International.



**SCARLET KIM**

The Deponent has acknowledged that she knows and understands the contents of the affidavit, which was signed and sworn to or solemnly affirmed before me at **LONDON** on this the 16<sup>th</sup> day of July 2018, the regulations contained in Government Notice No. R1648 of 19 August 1977, as amended, having been complied with.



**COMMISSIONER OF OATHS**





Solicitors  
Regulation  
Authority

# Practising Certificate for the year 2016-2017

Under the Solicitors Act 1974

**Camilla Graham-Wood**

is entitled to practise as a solicitor

Paul Philip  
Chief Executive

The Independent regulator of solicitors and law firms in England and Wales

Practising certificate commencement date 01/11/2016      Replacement date 31/10/2017

SRA number 465175