

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

Case No: CCT 278/19

RIGHT2KNOW CAMPAIGN First Applicant

PRIVACY INTERNATIONAL Second Applicant

(In the application for admission as amici curiae)

In re:

The matter between:

AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC First Applicant

SOLE, STEPHEN PATRICK Second Applicant

and

MINISTER OF JUSTICE AND CORRECTIONAL SERVICES First Respondent

MINISTER OF STATE SECURITY Second Respondent

MINISTER OF COMMUNICATIONS Third Respondent

MINISTER OF DEFENCE AND MILITARY VETERANS Fourth Respondent

MINISTER OF POLICE Fifth Respondent

THE OFFICE OF INSPECTOR-GENERAL OF INTELLIGENCE Sixth Respondent

THE OFFICE FOR INTERCEPTION CENTRES Seventh Respondent

THE NATIONAL COMMUNICATIONS CENTRE Eighth Respondent

THE JOINT STANDING COMMITTEE ON INTELLIGENCE Ninth Respondent

THE STATE SECURITY AGENCY Tenth Respondent



FILING SHEET

DOCUMENTS FILED: *AMICI CURIAE* NOTICE OF MOTION AND FOUNDING
AFFIDAVIT

DATE FILED: 31 JANUARY 2020

DATE ON THE ROLL: 25 FEBRUARY 2020

DATED AT **JOHANNESBURG** ON THIS THE **31ST** DAY OF **JANUARY** 2020.



LEGAL RESOURCES CENTRE

Attorneys for the Applicants
15th Floor, Bram Fischer Towers
20 Albert Street
Marshalltown
Johannesburg
Tel: 011 836 9831
E-mail: david@lrc.org.za
Ref: D/Mtshali

**TO: THE REGISTRAR OF THE CONSTITUTIONAL COURT,
BRAAMFORNTEIN**

AND TO: WEBBER WENTZEL
First and Second Applicants' Attorneys
90 Rivonia Road, Sandton
JOHANNESBURG
2196
Tel: (011) 530 5232
Fax: (011) 530 6232
Email: Dario.milo@webberwentzel.com

Ref: Dario Milo / Makhotso Lengane / 3000547

AND TO: THE STATE ATTORNEY, PRETORIA

Fifth Respondent's Attorneys

SALU Building

216 Thabo Sehume Street

Private Bag X 91

PRETORIA 0001

Ref: 2937/2017/Z52/MC

Tel: (012) 309 – 1630

Fax: 086 640 1943

Dx: 298 PRETORIA

Email: memakhubela@justice.gov.za / conkuna@justice.gov.za

Enq: M Makhubela

c/o: THE STATE ATTORNEY, JOHANNESBURG

12th Floor, North State Building

95 Albertina Sisulu Street (Cnr. Kruis Street)

JOHANNESBURG

Tel: (011) 330 7663

Fax: (011) 333 1683 / 086 507 2005

Email: HMaponya@justice.gov.za

Enq: H Maponya

AND TO: THE STATE ATTORNEY, PRETORIA

Third and Fourth Respondents' Attorneys

SALU Building

216 Thabo Sehume Street

Private Bag X91

PRETORIA 0001

Ref: 2937/2017/Z52/MC

Tel: (012) 309 – 1630

Fax: 0860 640 1943

Dx: 298 PRETORIA

Enq: M Makhubela

AND TO: **THE STATE ATTORNEY, PRETORIA**
Second, Seventh, Eighth and Tenth Respondents' Attorneys
SALU Building
216 Thabo Sehume Street
Private Bag X91
PRETORIA 0001

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

Case no: CCT 278/19

Case no: CCT 279/19

In the application for admission as *amici curiae* of:

THE RIGHT2KNOW CAMPAIGN

First Applicant for
Admission

PRIVACY INTERNATIONAL

Second Applicant for
Admission

In the matter between:

**AMABHUNGANE CENTRE FOR INVESTIGATIVE
JOURNALISM NPC**

First Applicant

SOLE, STEPHEN PATRICK

Second Applicant

and

**MINISTER OF JUSTICE AND CORRECTIONAL
SERVICES**

First Respondent

MINISTER OF STATE SECURITY

Second Respondent

MINISTER OF COMMUNICATIONS

Third Respondent

MINISTER OF DEFENCE AND MILITARY VETERANS

Fourth Respondent

MINISTER OF POLICE

Fifth Respondent

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

Sixth Respondent

THE OFFICE FOR INTERCEPTION CENTRES

Seventh Respondent

THE NATIONAL COMMUNICATIONS CENTRE

Eighth Respondent

THE JOINT STANDING COMMITTEE ON INTELLIGENCE

Ninth Respondent

THE STATE SECURITY AGENCY

Tenth Respondent

APPLICATION FOR ADMISSION AS AMICI CURIAE

KINDLY TAKE NOTICE that Right2Know Campaign (**R2K**) and Privacy International (**PI**) hereby make an application for an order in the following terms:

1. R2K and PI are admitted as *amici curiae* in the above proceedings.
2. R2K and PI are granted leave to—
 - 2.1 Make written submissions; and
 - 2.2 Present oral argument at the hearing of this matter.
3. If this application is opposed, any party opposing it is ordered to pay the costs.
4. Further and / or alternative relief.

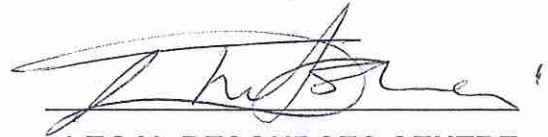
TAKE NOTICE FURTHER that the attached affidavits of **FLOYD THAMI NKOSI** and **ILIA MARIA SIATITSA** will be used in support of this application.

TAKE NOTICE FURTHER that R2K and PI will accept notice and service of all documents in these proceedings at the address of the Legal Resources Centre, Johannesburg office, as set out below.

TAKE NOTICE FURTHER that any party intending to oppose this application is required to give notice thereof within five (5) days of receipt of service of this application.

KINDLY PLACE this application before the Chief Justice to be dealt with in terms of rule 10 of the Constitutional Court Rules.

DATED AT JOHANNESBURG ON THIS 29TH DAY OF JANUARY 2020.



LEGAL RESOURCES CENTRE
Attorneys for R2K and PI
15th Floor, Bram Fischer Towers
20 Albert Street
Marshalltown
Email: david@lrc.org.za
refilwe@lrc.org.za
Ref: D Mtshali

**TO: THE REGISTRAR OF THE CONSTITUTIONAL COURT,
BRAAMFORNTEIN**

AND TO: WEBBER WENTZEL

First and Second Applicants' Attorneys

90 Rivonia Road, Sandton

JOHANNESBURG

2196

Tel: (011) 530 5232

Fax: (011) 530 6232

Email: Dario.milo@webberwentzel.com

Ref: Dario Milo / Makhotso Lengane / 3000547

AND TO: THE STATE ATTORNEY, PRETORIA

Fifth Respondent's Attorneys

SALU Building

216 Thabo Sehume Street

Private Bag X 91

PRETORIA 0001

Ref: 2937/2017/Z52/MC

Tel: (012) 309 – 1630

Fax: 086 640 1943

Dx:298 PRETORIA

Email: memakhubela@justice.gov.za / conkuna@justice.gov.za

Enq: M Makhubela

c/o: THE STATE ATTORNEY, JOHANNESBURG

12th Floor, North State Building

95 Albertina Sisulu Street (Cnr Kruis Street)

JOHANNESBURG

Tel: (011) 330 7663

Fax: (011) 333 1683 / 086 507 2005

Email: HMaponya@justice.gov.za

Enq: H Maponya

AND TO: **THE STATE ATTORNEY, PRETORIA**
Third and Fourth Respondents' Attorneys
SALU Building
216 Thabo Sehume Street
Private Bag X91
PRETORIA 0001

Ref: 2937/2017/Z52/MC

Tel: (012) 309 – 1630

Fax: 0860 640 1943

Dx: 298 PRETORIA

Enq: M Makhubela

AND TO: **THE STATE ATTORNEY, PRETORIA**
Second, Seventh, Eighth and Tenth Respondents' Attorneys
SALU Building
216 Thabo Sehume Street
Private Bag X91
PRETORIA 0001

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

Case no: CCT
278/19
Case no: CCT
279/19

In the application for admission as *amici curiae* of:

THE RIGHT2KNOW CAMPAIGN

First Applicant for
Admission

PRIVACY INTERNATIONAL

Second Applicant for
Admission

In the matter between:

AMABHUNGANE CENTRE FOR INVESTIGATIVE
JOURNALISM NPC

First Applicant

SOLE, STEPHEN PATRICK

Second Applicant

and

MINISTER OF JUSTICE AND CORRECTIONAL
SERVICES

First Respondent

MINISTER OF STATE SECURITY

Second Respondent

MINISTER OF COMMUNICATIONS

Third Respondent

MINISTER OF DEFENCE AND MILITARY VETERANS

Fourth Respondent

MINISTER OF POLICE

Fifth Respondent

THE OFFICE OF INSPECTOR-GENERAL
OF INTELLIGENCE

Sixth Respondent

THE OFFICE FOR INTERCEPTION CENTRES

Seventh Respondent

THE NATIONAL COMMUNICATIONS CENTRE

Eighth Respondent

THE JOINT STANDING COMMITTEE ON INTELLIGENCE

Ninth Respondent

THE STATE SECURITY AGENCY

Tenth Respondent

FOUNDING AFFIDAVIT

JVM T.N

I, the undersigned

FLOYD THAMI NKOSI

state under oath as follows:

I INTRODUCTION

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 Privacy International (PI). A confirmatory affidavit of Dr. Iliia Maria Siatitsa, 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 legal representatives.

T.N

5. This is an application in terms of Rule 10 of this Court's Rules for the admission of R2K and PI as *amici curiae*.
6. The main application concerns, primarily, the constitutionality of a variety of provisions of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA). The High Court declared various provisions of RICA unconstitutional and invalid. The Applicants seek to confirm those orders, whereas the Minister of Justice, the Minister of Policy, and the Minister of State Security seek to appeal various orders.
7. R2K and PI have engaged in extensive work relating to surveillance and the security agencies, both in South Africa and internationally. They seek leave to assist the Court by making submissions particularly on four of the issues before it:
 - 7.1 Post-interception notification;
 - 7.2 The independence of the designated judge;
 - 7.3 Mandatory, blanket retention of communication related data (metadata);
and
 - 7.4 Unauthorised and unregulated bulk surveillance.
8. With one small exception, R2K and PI support the orders made by the High Court on these issues. In general, their submissions focus on:

JUM T.N

- 8.1. Relevant international and comparative law and practice;
- 8.2. The impact of RICA and bulk surveillance on the right to privacy; and
- 8.3. Which issues this Court should decide, and which it should leave for future decision.

9. This affidavit is structured as follows:

- 9.1. **Part II** sets out R2K and PI's interest in these proceedings;
- 9.2. **Part III** addresses the scope of R2K and PI's application for admission and the legal submissions they seek to advance; and
- 9.3. **Part IV** deals with the procedural requirements for admission.

II R2K AND PI'S INTEREST IN THE MAIN APPLICATION

10. In this Part, I describe R2K's and PI's interest in the main matter. My statements about PI are confirmed by Dr. Iliia Maria Siatitsa in the confirmatory affidavit.
11. Both R2K and PI were admitted as *amici curiae* in the High Court. Both have a demonstrated interest surveillance, and extensive expertise that will assist the court in determining the appeals.

AM T.N

R2K

12. 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 undertakes 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.

13. R2K mobilises on four main issues:

10.1 **To stop secrecy**, in particular to ensure that security legislation and the conduct of security agencies are aligned with the Constitution and its underlying values;

10.2 **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;

10.3 **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

AM

T.N

- 10.4 **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.
14. R2K has a long track record of opposing the current surveillance regime.
15. 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 R2K, PI, and the Association for Progressive Communications, 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.
16. The submissions, and the report of the Committee is attached to the Applicants' papers as annexure **SPS24** (Record Vol 5, p 486).
17. 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

JM

T.N

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 TN1.

18. R2K and its members have also made numerous public statements and given countless 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.
19. R2K also has knowledge of and experience in litigating on the rights to free expression, assembly, privacy and protest:
 - 19.1. 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;
 - 19.2. 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

AM TM

several civil society organisations that intervened as *amici curiae* in a matter concerning access to court records; and

- 19.3. In *Primedia Broadcasting v Speaker of the National Assembly* [2016] ZASCA 142; 2017 (1) SA 572 (SCA), R2K was one of the successful applicants challenging limits on broadcasting parliamentary proceedings and the use of a signal jamming device in Parliament.
- 19.4. Most recently, in *Moyo and Another v Minister of Police and Others; Sonti and Another v Minister of Police and Others* [2019] ZACC 40, R2K made submissions to this Court on the constitutionality of section 1(1)(b) of the Intimidation Act 72 of 1982.
20. The subject-area of this matter falls squarely within R2K's interest. 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.
21. In addition to the activity described above, R2K is considering its own challenge to aspects of RICA and the current practice of surveillance in South Africa that have not been directly challenged in this application. It has been advised to await the outcome of these proceedings before deciding whether to launch that application. I discuss that intended application in more detail below when it relates to elements of the present application.

JUM

T.N

Privacy International

22. Privacy International is a non-profit, non-governmental organization based in London, the United Kingdom, which defends the right to privacy around the world. PI 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, Kenya, France, Germany, 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).
23. PI 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, PI advocates for strong national, regional, and international laws that protect this fundamental right. As a part of this mission, PI works with various partner organizations across the world to identify and address threats to privacy.
24. PI has litigated several cases addressing issues central to the main application. In particular, PI was one of the applicants in *10 Human Rights Organisations v United Kingdom*, a case currently before the Grand Chamber of the ECtHR, challenging two aspects of the UK's surveillance regime:
- 24.1. Mass interception of internet traffic transiting undersea fibre-optic cables landing in the UK; and

AM
TN

- 24.2. UK access to the information gathered by the US through its various mass surveillance programs.
25. The 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. PI's central claims in this case were that both programs violate articles 8 and 10 of the European Convention on Human Rights, which respectively protect the right to privacy and the right to freedom of expression.
26. Together with Open Rights Group, PI 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 articles 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

JVM
T.N

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] EUJECJ C-203/15 at para 134.*)

27. Privacy International is currently a party to two cases pending before the CJEU that challenge the retention and collection of bulk communications data by UK and French authorities from mobile network operators (or electronic communications network providers):

27.1. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (Case C-623/17)*; and

27.2. The joined cases *La Quadrature du Net, French Data Network, and Others v Premier Ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées (C-511/18 and C-512/18)*.

These cases also address the question of notification of interception.

28. On 15 January 2019, the Advocate General to the CJEU issued his opinion on how he advises the Court to decide on the case. He suggested that the mass surveillance regimes in the UK, France and Belgium are in violation of the EU law.
29. The CJEU is expected to issue its decision in the next couple of months.

AM TD

30. Based on its commitment to privacy and human rights, PI has a strong interest in this matter. Its legal expertise and experience on surveillance issues make it well-placed to make legal submissions and to assist the Court particularly with regard to international and comparative law.

III LEGAL SUBMISSIONS

31. In terms of Rule 10 of the Constitutional Court Rules, an *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:

- 31.1. Post-surveillance notification;
- 31.2. The independence of the designated judge;
- 31.3. Mandatory, blanket retention of metadata; and
- 31.4. Unauthorised and unregulated bulk surveillance.

Post-surveillance notification

32. 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

AM
TN

notification would cause no harm to the investigation. This unjustifiably limits the rights to privacy and of access to court.

33. The High Court upheld this argument. It declared the relevant provisions of RICA unconstitutional, suspended the declaration of invalidity, and granted appropriate interim relief putting in place a default notification regime.
34. R2K and PI support the Applicants' argument, and the finding of the High Court. 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 must 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.
35. R2K and PI seek leave to advance three further submissions:
 - 35.1. The absence of notification violates section 38 of the Constitution;
 - 35.2. Comparative law and practice support the need for appropriate notification; and
 - 35.3. International law supports the need for appropriate notification.

JUM
T.N

Section 38

36. The Applicants argue that the absence of notification is arbitrary and violates the right to privacy and the right of access to court. But the absence of notification also violates section 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.
37. In the context of interception of communications, this seems to be the most relevant right:
- 37.1. While section 34 protects the right to approach a court to resolve any legal dispute, section 38 provides special protections for allegations of constitutional rights violations.
- 37.2. The usefulness of notification is to enable the notified individual to know whether their right to privacy was interfered with. It may be that there is no violation of the right to privacy. Section 38 is about ensuring that those who *"alleg[e] that a right in the Bill of Rights has been infringed or threatened"* can approach a court. That can only happen if there is notification. Consequently, notification is a pre-requisite for individuals to exercise their rights under section 38.

JUM
T.N

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

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

38. For these reasons, R2K and PI will argue that RICA also unjustifiably limits section 38 of the Constitution.

Comparative Law

39. 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.

40. But they share the common themes identified by the Applicants:

40.1. The subject must be notified after the surveillance unless it will threaten the purpose of interception; and

40.2. The decision whether to notify or not is overseen by an independent authority.

JUM
TIN

41. This analysis is important for several reasons.
42. First, in interpreting the Bill of Rights, this Court may consider foreign law (section 39(1)(c) of the Constitution). In particular, in assessing whether a limitation of a right is justifiable in terms of section 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.
43. Second, the Ministers of Police and Justice contend that RICA is in line with other foreign jurisdictions, particularly the United Kingdom, Canada, New Zealand, Australia and the European Union. It is not clear why the Minister only relied on these four jurisdictions. However, R2K and PI will demonstrate that:
- 43.1. While it is true that the UK and Australia do not require notification, Canada and New Zealand respectively require and permit notification when doing so would no longer threaten the purpose of the investigation;
- 43.2. The CJEU and the ECtHR have both recognized that notification constitutes a critical safeguard when governments conduct surveillance. While the Applicants refer to the decision of the ECtHR in *Zakharov v Russia* [2016] 63 EHRR 17, there are several other judgments where this point has been affirmed; and

JUM
T.N

43.3. A broader survey of other countries in Europe, South America, Africa and Asia demonstrate that most comparable democracies require notification. I expand on this point below.

44. The clear trend in comparative democracies is towards post-surveillance notification. The following countries all have some notification provision:

44.1. The Netherlands;¹

44.2. Germany;²

44.3. Belgium;³

44.4. Austria;⁴

44.5. Ireland;⁵

44.6. The Czech Republic;⁶

44.7. Switzerland;⁷

44.8. Slovenia;⁸

44.9. Montenegro;⁹

¹ Intelligence and Security Services Act 2002.

² German Code of Criminal Procedure 1987, Article 101.

³ Belgium, Constitutional Court Case No. 145/2011 at paras 88 and 92.

⁴ Code of Criminal Procedure of the Republic of Austria 1975, Annexe 2 (138).

⁵ Criminal Justice (Surveillance) Act 2009, s 10(3).

⁶ Amendment Code of Criminal Procedure No. 177/2008 (information withheld only if this is in the interest of public security, crime prevention, health protection or the protection of the rights and freedoms of others).

⁷ Swiss Criminal Procedure Code 2007, Chapter 8: Covert Surveillance Measures - Article 279.

⁸ Criminal Procedure Code, Article 154.

⁹ Criminal Procedure Code 2009, Article 162.

AM
T.N

44.10. Hungary;¹⁰

44.11. The United States of America;¹¹

44.12. Canada;¹²

44.13. Japan;¹³

44.14. South Korea;¹⁴

44.15. Taiwan;¹⁵

44.16. New Zealand;¹⁶ and

44.17. Chile.¹⁷

45. These countries use a variety of methods to identify when a person must be notified. Many use language such as "*as soon as it is possible to do so without compromising intelligence work*" or without compromising the investigation, or "*unlikely to hinder the investigation in the future of such offences*". Others include a risk to life or physical integrity of a third party (such as Chile).

46. Some provide for a default duty to inform unless that condition is present (such as Austria). Others provide for a duty to inform unless some other condition is

¹⁰ Act on Criminal Proceedings XIX 1998, Title V, s 205(5).

¹¹ 18 U.S. Code § 2518.

¹² Canadian Criminal Code 1990, Part VI: Invasion of Privacy s 196(1).

¹³ Act on the Interception of Communications.

¹⁴ Protection of Communications Secrets Act 2002, art 9-2.

¹⁵ Communications Protection and Surveillance Act 1999, art 15.

¹⁶ Search and Surveillance Act 2012, Part 3.

¹⁷ Code of Criminal Procedure.

AM
T.N

met – for example, if the communications are not used in criminal proceedings. Hungary requires notification unless the material is used in criminal proceedings and notification would jeopardise those proceedings.

47. Some countries require the intervention of a court to justify not notifying the person (such as Switzerland, the United States, Taiwan and Montenegro). That can be at the judge's own instance, or on application by a prosecutor. Normally, the judge merely postpones notification until it will no longer pose a threat to the investigation.
48. Some include timeframes – the Netherlands, for example, requires the authorities to re-assess whether notification is possible after five years. Slovenia assumes notification should be done if the prosecutor does not act within two years. Japan and South Korea require notification within 30 days. Some, like Ireland, allow the Minister to enact regulations addressing the details.
49. Of course, not all countries provide for notification. Croatia,¹⁸ Bulgaria,¹⁹ Sweden²⁰ and Mexico,²¹ for example, currently do not. African countries largely do not have legislation that directly regulates the interception of communications.

¹⁸ Criminal Procedure Code 2009, art 335(5).

¹⁹ Special Surveillance Means Act.

²⁰ Act (2007: 980) on the Supervision of Certain Law Enforcement Activities.

²¹ Mexico (Ley Federal de Telecomunicaciones (2014) Arts. 189, 190, 191.

JM
T.N

Those that do – including Zambia and Lesotho – do not currently require notification.

50. But it is undeniably clear that it is possible to design a mechanism that appropriately balances the respective interests – protecting the investigation, and providing an effective remedy. Countries all across the world have designed such mechanisms. As the Ministers of Justice and Police argue, they recognise that there will be situations where ongoing secrecy is necessary to protect ongoing investigations. But they also accept that where those concerns are not present, the rights to privacy and to a remedy demand notification.

International Law

51. International law, too, recognises 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 Court is obliged to consider international law by section 39(1)(b) of the Constitution.
52. The Applicants refer to *The International Principles on the Application of Human Rights to Communications Surveillance*. But there are several other international agencies that have endorsed that position:
- 52.1. The UN Human Rights Committee;
- 52.2. The UN High Commissioner for Human Rights; and

JM

T.N

- 52.3. The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.
53. These entities are interpreting state parties' obligations under the International Covenant on Civil and Political Rights (ICCPR), which South Africa has ratified.
54. If admitted, R2K and PI will place the relevant international material before this Court.

The Designated Judge

55. The Applicants argue that the designated judge, and the process she employs to issue directions, is insufficiently independent on two grounds:
- 55.1. The process is not adversarial; and
- 55.2. The designated judge is appointed by the executive for an indeterminate time (normally one year) that is subject to renewal.
56. R2K and PI support these arguments. If admitted, it will advance four further lines of argument concerning the independence of the designated judge:
- 56.1. The lack of independence also unjustifiably limits the right to privacy;
- 56.2. The secrecy with which the designated judge operates enhances the need for independence;

JUM

T.N

- 56.3. The fact that the designated judge must be a retired judge further undermines her independence; and
- 56.4. Comparative practice and international law supports the arguments that the designated judge is insufficiently independent;

Right to Privacy

57. 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 and the High Court appeared to conclude. It is, most fundamentally, a violation of the right to privacy.
58. The right to privacy demands that the state will only be able to intercept another person's communications with independent judicial authorisation. This Court's jurisprudence with regard to search warrants makes that clear. Allowing RICA interceptions to be issued by a person without the same degree of independence as an ordinary, sitting judge, unjustifiably limits the right to privacy.

Secrecy Requires Greater Independence

59. Of necessity, 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.

AM

T.N

60. Not only does the designated judge operate in secrecy, but there is very little publicly available information about the work she has done. There is legislative provision for the designated judge to file reports with the Joint Standing Committee on Intelligence (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"

61. 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.

AM

T.N

62. 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.
63. No information is available in these reports on:
- 63.1. What were the warrants for – direct interception of metadata, direct interception of communication, provision of archived metadata?
 - 63.2. To how many people did the warrant pertain?
 - 63.3. To which alleged offence did the investigation pertain?
 - 63.4. What technology/method was used for the interception?
 - 63.5. What number of interceptions actually resulted in arrests and convictions?
64. 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

AM
TN

very small percentage of directions led to arrests or prosecutions, the public could legitimately ask whether too many directions are being granted.

65. In contrast, in the United States, for example, 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.
66. On 17 March 2017, Murray Hunter, who was then the Advocacy Coordinator for R2K, wrote a letter to the late Judge 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 TN2.

MH
T.N

67. Judge Maluleke responded on 10 April 2017. He noted the obligations placed on him by section 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 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 TN3.
68. There is no challenge to section 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 Applicants' independence challenge. This is an institution that operates in secret, and 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.
69. Openness ensures independence. Where judicial functions are performed in secret, the risk that they will not be performed independently is higher. That enhances the need to ensure that the structural measures to guarantee independence are in place.

AM

T.N

70. Instead, for the reasons given by the Applicant and above, the designated judge has less structural independence than an ordinary member of the judiciary.

A Retired Judge

71. The primary flaws the Applicants identify are: that the designated judge is appointed by the executive, for a renewable term. The fact that RICA requires the designated judge to be a retired judge is, *combined with term renewal*, extremely problematic.
72. The legislation governing retired judges – the Judges' Remuneration and Conditions of Employment Act 47 of 2001 – creates a clear financial incentive for the designated judge to make decisions that will make it more likely that her term will be renewed. Those financial incentives would not be present if the designated judge was a sitting judge.
73. That is not to say that any designated judge has acted in this way. The “independence of the judiciary” inquiry is objective. Objectively, the ability to earn additional income creates a reasonable apprehension that the office is not independent.
74. That would not be the case if RICA required the designated judges to be sitting judges. Sitting judges who were merely assigned to consider RICA applications would not be paid an additional amount. It would also not be the case if the retired RICA Judge's term was not subject to renewal. There would be no

AM

L.N

possibility of future enrichment as a result of renewal. In either case, there would be no financial incentive that could possibly affect the decisions the designated judge is required to make if the sitting judges were the designated judges.

Comparative Practice

75. R2K and PI seek leave to place comparative information before the Court to demonstrate that RICA falls far short of international best practice in ensuring the independence of the judiciary — in particular, here, the term of office of the designated judge and the absence of guarantees against outside pressure. While there is certainly no uniformity between states, most provide far more independence to the equivalent of the designated judge.
76. Firstly, many states require surveillance to be approved by a sitting member of the judiciary.
77. In Africa, the following countries require a sitting judge to authorise the issue of a surveillance warrant: Egypt;²² Ghana;²³ Kenya;²⁴ and Lesotho.²⁵

²² Constitution of Egypt arts 57 and 58, Egyptian Criminal Code (Law 58 of 1937) and the Criminal Procedures Code (Law 150 of 1950) and Communications Law (Law 10 of 2003).

²³ Anti-Terrorism Act 2008 (a senior police officer (not below the rank of an Assistant Commissioner of Police) with the written consent of the Attorney-General and Minister of Justice (AG) may apply to a court for an order to require service providers to intercept customer communications for the purpose of obtaining evidence of commission of an offence); Electronic Transactions Act 2008 section 101 (the government or law enforcement agency must first apply to the court and seek judicial approval before an order is granted relating to the disclosure of customers' communications that are in transit or held in electronic storage in an electronic communications system by a communication service provider)

RM

T.N

78. Outside of Africa, countries that require judicial authorisation include:

78.1. Germany;²⁶

78.2. Belgium;²⁷

78.3. Austria;²⁸

78.4. Ireland;²⁹

78.5. the Czech Republic;³⁰

78.6. Bulgaria;³¹

78.7. Switzerland;³²

²⁴ National Intelligence Service Act 2012 s 42(2) (warrant issued by a judge of the High Court).

²⁵ Communications Act 2012 read with the Criminal Procedure and Evidence Act 1981.

²⁶ The German Code of Criminal Procedure (Measures pursuant to s 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within three working days.)

²⁷ Intelligence and Security Services Law (The head of the department submits a draft authorisation to the Commission (made up of 3 individuals - one public prosecutor and two judges - nominated by the Ministers of Defence and Justice, approved by the Council of Ministers and appointed by the King) for approval, which checks whether the provisions relating to the use of the method for data collection and the principles of proportionality and subsidiarity are respected.)

²⁸ Code of Criminal Procedure of the Republic of Austria 1975, Annexe 2 (138) (Surveillance measures are ordered by the public prosecutor's office based on judicial approval).

²⁹ Criminal Justice (Surveillance) Act 2009 s 5 (application is made to a judge assigned to any district court district.).

³⁰ Amendment Code of Criminal Procedure No. 177/2008.

³¹ Special Surveillance Means Act (the application is made to the president of the Sofia City Court or of the respective regional court, or to a duly authorised deputy).

³² Swiss Criminal Procedure Code 2007, Chapter 8: Covert Surveillance Measures art 272 (the surveillance of post and telecommunications requires the authorisation of the compulsory measures court).

JUN
T.N

78.8. Slovenia;³³

78.9. Croatia;³⁴

78.10. Portugal;³⁵

78.11. Montenegro;³⁶

78.12. Hungary;³⁷

78.13. Mexico;³⁸

78.14. South Korea;³⁹

78.15. Taiwan;⁴⁰

78.16. Hong Kong;⁴¹

³³ Slovenia Criminal Procedure Code (ordered by means of a written order by the investigating judge following the public prosecutor's written proposal).

³⁴ Croatia Criminal Procedure Code 2009 art 332 (if the investigation cannot be carried out in any other way or doing so would lead to great difficulties, the investigating judge may, upon the written request with a statement of reasons by the State Attorney).

³⁵ Code of Criminal Procedure art 269 (interception of communication measures requested by the Prosecutor falls within the acts that must be ordered or authorised by the Examining Judge).

³⁶ Montenegro Criminal Procedure Code 2009 art 159 (shall be ordered via a written order by the investigative judge at the motion of the State Prosecutor containing a statement of reasons).

³⁷ Hungary Act on Criminal Proceedings XIX s 203 (covert data gathering shall be permitted by the court at the motion of the prosecutor).

³⁸ Mexico Federal Telecommunications Act 2014 art 189 (only the federal judicial authority can authorize telephone tapping and interception of private communications at the request of the appropriate federal authority or the State Public Prosecution Service).

³⁹ Protection of Communications Secrets Act 2002 art 6(1) (any prosecutor may ask a court to permit wiretapping of telecommunications).

⁴⁰ Communications Protection and Surveillance Act 1999 art 15(5) (the prosecutor of competent jurisdiction shall, upon application by a law enforcement agency or ex officio, file a motion with the court of competent jurisdiction for the communications surveillance warrant).

⁴¹ SAR Ordinance, Chapter 589 ss 6 and 8 (The Chief Executive appoints a panel of 3-6 eligible judges for a period of 3 years. Interception warrants are granted by one of the judges on the panel).

JUM
T.N

78.17. New Zealand;⁴²

78.18. Canada;⁴³

78.19. the USA;⁴⁴ and

78.20. Chile.⁴⁵

79. In some of these countries (including Bulgaria, Germany, Austria, New Zealand, Taiwan and Mexico) the executive – either the police or the prosecutor – must approach a court to authorise the surveillance.

80. In many European civil-law countries, such as Slovenia, Montenegro and Croatia, it is the investigating judge who performs the role. The investigating judge is a unique civil law institution that oversees the investigative process and also performs other tasks such as issuing ordinary search warrants.

81. In other countries, the sitting judge is part of a panel of judges who performs this role.⁴⁶ Many countries provide an exception for when interception is urgent and a warrant cannot be obtained in time.

⁴² Search and Surveillance Act 2012 s 53 (a surveillance device warrant may be issued by a Judge, on application).

⁴³ Canadian Criminal Code, Part VI (apart from certain exceptions outlined in the Code, judicial authorization is required for the interception of private communications, but in comparison to ordinary search warrants the requirements for obtaining such an authorization are more onerous).

⁴⁴ US Code, Title 18, ss 2510-2522.

⁴⁵ Code of Criminal Procedure arts 222 et seq (interception is ordered by the Constitutional Judge).

⁴⁶ For example, Belgium (Intelligence Security Services Law); Germany (Communications Intelligence Gathering Act 2016); and Hong Kong (SAR Ordinance, Chapter 589, Section 48).

JM
T.N

82. None of the countries R2K and PI considered provide for a single, retired judge to determine surveillance applications.
83. Of course, there are other countries that do not require judicial authorisation,⁴⁷ or that require judicial authorisation in some circumstances, and executive authorisation in others.⁴⁸
84. But the clear trend is for independent, judicial authorisation.
85. Secondly, international law supports the need for independent judicial determination of surveillance requests. Both the Special Rapporteur and the UN High Commissioner for Human Rights have held that surveillance can only be conducted on authorisation by an independent, judicial body. If admitted, R2K and PI will refer to the relevant findings of these bodies.
86. There is an obvious advantage to requiring the government to approach the ordinary courts rather than a specifically designated judge. It limits the ability for the executive to choose a specific person who will act favourably. It also ensures

⁴⁷ Some examples are: India (Indian Telegraph Act 1885); Singapore (Criminal Procedure Code (amended in 2012) and the Computer Misuse and Cybersecurity Act 2013).

⁴⁸ See, for example, Albania, France, Italy, the United Kingdom and Australia. In Italy and France, a judge must approve the surveillance if the interception is to investigate a crime, but an administrative authority authorizes if the interception is to prevent a crime. In the United Kingdom, the warrant must be approved by the Home Secretary, but if the Investigatory Powers Act 2016 applies, the warrant (if not urgent) must be approved by a Commissioner (a senior judge, appointed by the Prime Minister).

JUM
T.N

that the workload is spread, avoiding the risk that a single judge will 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.

Mandatory, Blanket Retention of Communication Related Information

87. The High Court's Fifth Order declares the whole of RICA, and particularly sections 35 and 37, invalid to the extent that "*fails to prescribe proper procedures to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing*" of data obtained through interceptions.
88. R2K and PI support this order. However, they argue that it is inappropriately narrow and should be expanded to include the absence of safeguards for the storage of information by private companies holding metadata that is not gathered through an interception.
89. If admitted, R2K and PI will make five submissions:
 - 89.1. Contend that the order is inappropriately narrow;
 - 89.2. Assess the relevant provisions of RICA;
 - 89.3. Demonstrate the impact of mandatory, blanket retention of metadata;
 - 89.4. Consider relevant international and comparative law and

JM
T.N

89.5. Argue for the Court to leave open the constitutionality of mandatory, blanket retention of metadata.

The Order is too Narrow

90. Before the High Court, the Applicants challenged two related elements that the High Court dealt with together:

90.1. The absence of safeguards for the storage of interception data by the state; and

90.2. The length of time *and the absence of safeguards* for the storage of communications-related information by private, telephone companies.

91. The first challenge was directed at sections 35 and 37 of RICA which deal with the storage of interception data at "*interception centres*".

92. The second challenge was to section 30(2)(a)(iii) of RICA which provides for the Minister of Communications to issue a directive determining the

"type of communication-related information which must be stored in terms of subsection (1) (b) and the period for which such information must be stored, which period may, subject to subsection (8), not be less than three years and not more than five years from the date of the transmission of the indirect communication to which that communication-related information relates;

JUM
T.N

93. The Applicants' founding papers made it clear that they were concerned with both the period for which the communication-related information would be stored, and the conditions under which it would be stored. In paragraph 89.2, they averred:

"RICA is under-inclusive as there are no oversight mechanisms required by section 30(2)(a)(iii) of the Act. Put differently, the applicants submit that oversight mechanisms need to be put in place by the telecommunication service providers in order to control access to, and ensure the protection of, the information handled and held by the telecommunication service providers."

94. The relief sought with regard to section 30(2)(a)(iii) was simply that it is *"inconsistent with the Constitution and accordingly invalid"* (prayer 1.3 of the Notice of Motion).
95. It is further clear from the answering and replying affidavits that the parties understood there to be a challenge to the absence of safeguards for the storage of communication-related information by phone operators. The relevant passages are at paras 49-52 of the Replying Affidavit (Record Vol 10, p 1003).
96. The High Court appreciated that the attack on the absence of safeguards applied to both the holding of interception data by the state, and the use of communication-related information by phone operators. This appears from paragraph 89 of the judgment, which reads:

AM
TIN

"The attack on this regime for the storage and management of the communications captured is twofold:

89.1 First, it is argued the period of three years is too long for service providers to archive the data because that period is not reasonably connected to the legitimate objectives of RICA and comparison with other jurisdictions suggests, at most, a two-year period. Moreover, it is argued that the inappropriateness of such a long period is exacerbated by the inadequate oversight of service providers in dealing with the data.

89.2 Second, having accessed and stored this material in servers at Interception Centres, RICA per se is bereft of appropriate injunctions on how it is to be managed and used and by whom it may be accessed; the directives issued about such management are said to be inadequate to meet the need to be an effective safeguard against abuse or impropriety."

97. The directives the High Court is referring to are the directives published in terms of section 30(2)(a) concerning the retention of communications-related information by phone operators. They are the *Directives in Respect of Different Categories of Telecommunications Service Providers Made in Terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 Of 2002)*, published as GN 1325 of 2005.

AM

TIN

98. The problem is this: the High Court's order is limited to the storage of interception data by the state, and does not extend to the storage of communication-related information by telecommunications service providers. It reads:

"RICA, especially sections 35 and 37, are inconsistent with the Constitution and accordingly invalid to the extent that the statute, itself, fails to prescribe proper procedures to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions."

99. But, as R2K and PI hope to establish, there is no difference – from the perspective of the right to privacy – between the retention of intercepted communications data by the state, and the retention of communications-related information by private companies. Both pose serious risks to the privacy of South Africans. The only way to cure those risks is to ensure that the safeguards to limit any inappropriate disclosure are contained in the legislation that creates the risk.

100. The Applicants have not appealed against this part of the High Court's order. However, R2K and PI submit that given the manner in which it was pleaded, it is within this Court's power to grant a just and equitable order that reflects the full extent of the constitutional violation. Accordingly, R2K and PI will argue that Order 4 should be amended as follows:

"(1) RICA, especially sections 30, 35 and 37, is inconsistent with the Constitution and accordingly invalid to the extent that the statute, itself, fails to prescribe proper procedures to be followed when state

JM
T.N

officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions, and when a telecommunication service provider is examining, copying, sharing, sorting through, using, destroying and/or storing archived communications-related data;

- (2) *The declaration of invalidity is suspended for two years to allow Parliament to cure the defects."*

101. In order to justify the amendment to Order 4 proposed above, it is necessary to show that mandatory, blanket retention of metadata is a serious infringement of the right to privacy. The first step is to explain how RICA operates with regard to mandatory retention of metadata.

The Operation of RICA

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

103. "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,

JUN

T.N

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".

104. 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"

105. Communications-related information is information about any type of electronic communication.

106. 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

JW
T.N

provider", without amending the references to the former in the body of the Act, including in section 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;*

107. 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.

108. 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 section 30(2)(a)(iii). The Minister has – in the Directive discussed above – exercised that power with regard to phone operators. She has not issued a

AM
T.N

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.

109. 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.

110. However, it can be accessed by the government using a direction issued in terms of section 19 of RICA. This has the limitations and safeguards described by the Applicant:

110.1. It can only be obtained to investigate certain types of serious offences, and threats to national security;

110.2. The application can be made only by specified senior officials within the definition of "*applicant*" in RICA; and

110.3. The application must include the detailed information set out in section 17(2) (with the necessary changes based on the context).

111. However, archived communication-related information can also be accessed outside of section 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.

AM
T.N

112. This flows from section 15 of RICA read with section 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."

113. 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

JUM
T.N

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.)

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

114.1. A request under section 205 can be made to investigate any offence;

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

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

114.4. Judicial officers dealing with section 205 applications are not subject to any reporting requirements, unlike the Designated Judge who under section 3 of the Strategic Intelligence Oversight Act is required to report certain information to Parliament.

115. The only advantage of section 205 warrant is that it is issued by a sitting member of the judiciary, and therefore does not suffer from the same independence problems as the designated judge.

116. In practice, section 205 warrants are extremely easy to obtain. Indeed, the vast majority of metadata requests are not made in terms of section 19, but in terms

JUM
T.N

of section 205. In 2018, R2K made requests in terms of the Promotion of Information Act to the various phone operators to determine how many section 205 requests they received, and how many RICA requests they received. Vodacom was the only operator to provide information on the number of RICA requests and section 205 requests. In 2018, it received 22 690 section 205 requests. It received only 190 requests for archived communication-related information, and only 1 550 RICA requests in total.

117. The applications are generally determined on paper, in chambers by any magistrate or judge.

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

118.1. All phone companies must maintain a record of the who, when, how and where of every single communication by their users. The only information not recorded is the content of the communication.

118.2. 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.

JUM
T.N

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

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

The Impact of Mandatory, Blanket Retention of Metadata

119. For those people who have cellphones and computers, 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. Metadata can 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.

120. 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. Under RICA, information about our use of all of these devices must be captured and stored.

JUM
1.10

121. 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.
122. 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.
123. The type of information section 30 of RICA requires companies to store is fundamentally personal information, particularly when it is aggregated over a period of time.
124. 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

JUM
T.N

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.

125. 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.
126. 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.
127. But to do away with the requirement of individualised reasonable suspicion is to abandon the basic premise of the right to privacy. There must be some reason to suspect a particular person of wrongdoing in order to justify limiting their privacy.

2004
T.N

128. Under RICA, everybody's metadata is retained, regardless of whether they are suspected of having committed a crime or not. And the metadata is available for an investigation into any crime.
129. The same purpose could be achieved through a less restrictive, more targeted regime for the retention of metadata. The onus should be 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.

International and Comparative Law

130. International law supports the proposition that mandatory, blanket retention of metadata is impermissible. The UN High Commissioner on Human Rights, the UN Human Rights Committee, and the UN Special Rapporteur have all argued that it is impermissible.
131. The CJEU, too, has repeatedly found that mandatory, blanket retention of metadata is unlawful. See *Digital Rights Ireland (Judgment of the Court)* [2014] EUECJ C-293/12 and *Tele2 Sverige AB v. Post- Och telestyrelsen; Secretary of State for the Home Department v. Tom Watson et. al.*
132. Just this year, the Advocate General to the CJEU expressed the opinion that the practice of France, Belgium and the United Kingdom in retaining metadata remains unlawful in Europe.

AM
T.N

R2K and PI's Position

133. Accordingly, R2K and PI take the position that the scheme for the mandatory, blanket retention of metadata is inherently unconstitutional.

134. In this application, this Court is limited to particular, limited aspects of that scheme – the absence of oversight and safeguards. It is not called upon to adjudicate the constitutionality of mandatory, blanket retention of metadata itself. R2K and PI do not suggest that it should. Instead, they will submit:

134.1. The consequences of mandatory, blanket retention of metadata demand (at the very least) that it is subject to the same safeguards and oversight as the retention of intercepted communications data by the state.

134.2. This Court should expressly leave open the question of whether mandatory, blanket retention of metadata is itself constitutional.

Mass surveillance

135. Before the High Court, the Applicants successfully argued that the bulk surveillance of foreign signals conducted by the National Communications Centre is unlawful because:

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

135.2. It is expressly prohibited by section 2 of RICA;

JUM
T.W

- 135.3. It limits the constitutional rights of privacy and of access to court without being justified by a law of general application; and
- 135.4. Even if there was a law of general application that permitted the NCC's operation, it would not be a justifiable limitation of the rights of privacy and of access to court.
136. The High Court upheld these arguments and declared the practice of bulk surveillance by the NCC unlawful and invalid.
137. R2K and PI supported these arguments. But they argued, in addition, that even if bulk surveillance was authorised by law, it would be unconstitutional. It asked the High Court to leave this issue open for future determination. The High Court did so (para 166).
138. This issue is not formally before this Court. It was not part of the confirmation application, because it was not an order with regard to legislation or conduct of the President. Nor was it subject to an appeal by the Minister of Police, or the Minister of Justice.
139. However, the Minister of State Security has, belatedly, brought an "appeal" against that part of the High Court. As the Applicants correctly point out, the appeal is defective. The Minister of State Security has no right to appeal that part of the order. While he is entitled to apply for leave to appeal, he has not



T.N

done so. Nor has he made a proper case for condonation, or for why this issue should not be heard, first, by the SCA.

140. At the time of deposing to this affidavit, R2K and PI was not aware of any order or directions issued by this Court with regard to this "appeal". R2K and PI agree with the Applicants that this Court should not entertain this appeal.
141. However, if it does so, R2K and PI endorse the Applicants' arguments that found favour in the High Court.
142. In addition, R2K and PI seek leave to make the following submissions:
 - 142.1. Explain at a basic level how bulk surveillance operates;
 - 142.2. Demonstrates the impact of bulk surveillance;
 - 142.3. Provide international and European law supporting a finding it is unconstitutional;
 - 142.4. The state's justifications are without merit; and
 - 142.5. Argue why that should lead to upholding the High Court's judgment.

Operation of Bulk Surveillance

143. 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:

JVM

T.N

- 143.1. Bulk surveillance is employed for "*environmental scanning*" to search internet traffic "*for certain cue words or key phrases*".
- 143.2. 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.
- 143.3. The interception includes both the communication itself, and the information about the communication (the metadata).
- 143.4. Bulk surveillance "*is not directed at individuals*". For that reason, it is not "*restricted by Foreign Signal Intelligence requirements*".
- 143.5. 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. No human intervention is required for this process*". However, the stored information can be accessed by "*authorised technical personnel*".
- 143.6. 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*".
- 143.7. In the government's view (which is refuted below) all the data are useless unless they are subject to human intervention and analysis.

JM
T.N

144. 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. Are the data stored indefinitely?
145. 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.
146. Based on comparative information – particularly the documents disclosed by Edward Snowden concerning the US bulk surveillance programmes, 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.
- 146.1. **Interception** – The first step is to obtain a signal from a source, e.g. by tapping a fibre optic cable.

- 146.2. **Extraction** – The intercepted signals are then copied and converted into a digital stream so that the data can be reconstructed into an intelligible format.
- 146.3. **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.
- 146.4. **Storage** – Information is retained in a database for potential future analysis or dissemination.
- 146.5. **Analysis** – Once held in databases, there can then be further querying, examining or data-mining of the information.
- 146.6. **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.
147. Based on the available evidence, it appears that the NCC follows the same or a similar process.
148. R2K and PI submit that the right to privacy is violated at each one of these stages – when data is intercepted, extracted, filtered, stored, analysed and disseminated.

NM
TN

Impact of Bulk Surveillance

149. 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.
150. While the lack of legal authority, and the violation of section 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. The fundamental problem is that the state asserts the right to capture virtually all internet traffic that enters and leaves South Africa.
151. 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, plans a trip on Google Maps, or accesses their online diary. All those communications travel back and forth

AM
T.N

between South Africa and another country. They are "foreign" signals and are liable to be intercepted by the NCC.

152. 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 any statutory safeguards.
153. On any approach to privacy, this is a massive violation. While data 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.

AM

T.N

154. 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. And it does so without limit, safeguards or oversight.
155. 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.
156. I have already explained above why the interception and storage 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. But bulk surveillance also includes the actual emails, the actual Skype calls, Facebook messages, photographs, diary entries, address books and so on.

T.N. AM

157. It is difficult to think of a more serious systemic violation of the right to privacy of all South Africans who use the internet.
158. The violation is exacerbated by the fact that it is entirely unregulated. The government does not seek authorisation for these immense powers under RICA. 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 section 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*".
159. The NSIA contains no limits on the section 2 power, and no procedural safeguards for the exercise of this power. The government points to none in its answering affidavits.
160. As a result:
- 160.1. 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.

AM

T.N

160.2. 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 without every seeking permission from a judicial officer.

160.3. 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.

161. The effect of an absence of any regulatory framework is clear in the instances of abuse pointed out by the Applicants.

162. 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.

International and European Law

163. If admitted, R2K and PI will demonstrate that bulk surveillance is contrary to international law.

AM
T.N

164. First, bulk Surveillance is inconsistent with the ICCPR. UN Special Rapporteur and the UN Human Rights Commissioner have concluded that this practice is not permissible under the ICCPR. In the words of the UNHCR:

"Mass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate." (Report of the Office of the United Nations High Commissioner for Human Rights submitted to the UN Human Rights Council on 30 June 2014 (A/HRC/27/37) at 25.

165. The UNHCR's concern for the "haystack" is vital. Obviously bulk surveillance will turn up information that is useful for fighting crime. So too would allowing warrantless searches of people's homes. The Constitution prohibits those actions because fighting crime cannot justify any and all limitations of the right to privacy. And bulk surveillance permits innumerable violations of the haystack's privacy to find a single needle.
166. Second, European law sets certain basic requirements for a surveillance measure to be lawful. In *Liberty and Others v United Kingdom* [2008] ECHR 568, the ECHR held that the British bulk surveillance system was inconsistent with the Charter. It held that the surveillance must be "in accordance with the law" which requires both that the surveillance has a "basis in domestic law", and that it

AM

T.W

meets a certain quality of law "requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him" (para 59). It held that the same requirement of foreseeability used for individual surveillance applies (para 63).

167. There are two recent, not final judgments, where the ECHR has accepted that, with appropriate safeguards, bulk surveillance programs can fall within the "margin of appreciation" the Court affords to member countries to protect their national security – but only if it is properly authorised and complies with minimum safeguards. See *Big Brother Watch & Others v United Kingdom* [2018] ECHR 722 *Centrum för Rättvisa v Sweden* [2018] ECHR 520.

168. R2K and PI do not agree with this position. Our position is that bulk surveillance will always be an unjustifiable limitation of the right to privacy. It is necessarily inconsistent with the requirements of being authorised by law that is clear and precise, and the requirements of necessity and proportionality.

169. PI and our attorneys, the Legal Resources Centre, are parties to the *Big Brother Watch* case where an appeal is currently before the Grand Chamber of the ECtHR. The Applicants in that matter argue that bulk surveillance is inherently inconsistent with the right to privacy. The Applicants' submissions are available at <https://privacyinternational.org/sites/default/files/2019-07/Applicants%27%20Observations%20-%20May%202019.pdf>

AM
T.W

170. The Grand Chamber heard the matter on 10 July 2019. Judgment is pending.
171. The LRC was a party to the application because its emails were unlawfully intercepted and read by the British Government Communications Headquarters (GCHQ). It became aware of this unlawful conduct through a complaint to the British Information Protection Tribunal. The LRC still does not know which emails were unlawfully intercepted, nor why they were intercepted. That is precisely the danger that bulk surveillance poses – including with regard to lawyers and journalists.
172. In any event, even if the Grand Chamber were to uphold the decisions in *Big Brother Watch* and *Centrum för Rättvisa*, the current unregulated and unauthorized practice of bulk surveillance in South Africa would be patently unlawful. It is not authorized by law, and it includes none of the minimum safeguards for communications surveillance consistently adopted by the European Court on Human Rights. This Court should have no hesitancy in finding that system to be unconstitutional and leave the question of whether bulk surveillance can ever be justified to be decided later.

Justification

JUM
T.N

173. Substantively, the government made little attempt to justify foreign bulk surveillance before the High Court. Its defences can be summarised as follows:

173.1. These practices are common in other jurisdictions; and

173.2. Bulk surveillance and environmental scanning are necessary to deal with "*unconventional threats to peace and stability*".

174. Neither argument is sufficient to justify the current form of untargeted, unregulated mass surveillance of South Africans.

175. First, while these mass surveillance systems exist in other countries, that does not mean they are constitutional. Indeed, since the Snowden revelations, the international community – and particularly international human rights bodies – have concluded that these practices are contrary to international law. That is the case even when the systems are properly authorised and regulated by law. The bulk surveillance conducted by the NCC meets neither of those very basic requirements. It is *not* supported by international law or practice. Quite the opposite.

176. 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

QUM
T.N

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.

177. But the current system means everyone is under surveillance, all the time. That is not necessary or proportionate to protect national security.
178. 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.
179. 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.
180. Accordingly, the purpose is simply inadequate to justify the limitation of the right to privacy.

Uphold the High Court

181. In light of the impact of bulk surveillance, the international law, and the absence of a justification, how should this Court deal with the merits of the bulk surveillance challenge? If admitted, R2K and Privacy will make three submissions.

JUM
T.N

182. First, the key issue is how to interpret the NSIA. The Minister of State Security argues that it should be interpreted to permit bulk surveillance. That interpretation must be rejected for two reasons:

182.1. The NSIA, like all statutes, must be interpreted in terms of section 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.

182.2. The NSIA must also be interpreted consistently with international law. That includes South Africa's obligations under the ICCPR. As set out above, the ICCPR prohibits bulk surveillance. It undoubtedly prohibits unregulated bulk surveillance not expressly authorised by law.

183. Second, this Court could decide this part of the case narrowly by simply holding that the NCC lacks the legal basis to function. However, if admitted R2K and PI will submit that it should also hold that the admitted practice of bulk surveillance is unconstitutional because it violates 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.

CM
T.N

184. Third, the Court should leave open whether authorised, regulated, bulk surveillance is constitutional. As set out above, there are strong arguments that only targeted surveillance is permissible. This Court should confine itself to the question before it – untargeted, unregulated bulk surveillance.

IV PROCEDURAL REQUIREMENTS FOR ADMISSION

185. In terms of Rule 10(1), a party seeking to be admitted as an *amicus curiae* must seek the written consent of all the parties in the proceedings.

186. R2K and PI sent letters to the Applicants and Respondents requesting their consent to its admission on 22 January 2030. A copy of that letter is attached as annexure TN4.

187. R2K and PI have received the following responses:

187.1. On 27 January 2020, both the Applicants and Minister of State Security consented to the admission of R2K and PI as *amici curiae* in this application. A copy of the letter is attached as annexure TN5 and TN6 respectively.

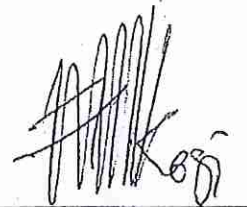
AM TN

187.2. On 24 January 2020, the State Attorney representing the Minister of Justice and the Minister of Police consented to the request. I attach a copy of the letter as annexure TN7.

V CONCLUSION

188. 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*.

189. 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.



FLOYD THAMI NKOSI



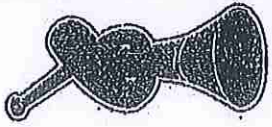
The Deponent has acknowledged that he knows and understands the contents of the affidavit, which was signed and sworn to or solemnly affirmed before me at Armen Dvalenshin on this the 79 day of January 2020, the regulations contained in Government Notice No. R1648 of 19 August 1977, as amended, having been complied with.

Armen Dvalenshin
COMMISSIONER OF OATHS

29 JAN 2020
GEMEENSKAPSDIENSTSENTRUM
GROOT-DRAKENSTEIN
SUID-AFRIKAANSE POLISIEDIENS

T.N

TN1



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 metadata¹ 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

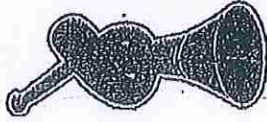
¹ Metadata is all the information about a communication, rather than the actual content of the communication (e.g. the identity of each party in a communication, the time and their locations, networks and devices). Once stored, it is used to create a huge, searchable database of every electronic interaction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

T.N #
JUM

MH

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

T.N #
JUM



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 practices¹.

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

¹ 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

TN #

MH

JUM

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 is 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 communities².
- 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 unconstitutional³.
- 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 RICA⁴.
- Recent reports in the Mail & Guardian point to serious failings in RICA's safeguards⁵, and ongoing use of the state's unregulated mass surveillance capabilities⁶.

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-cellphone-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>

T.N. #
JUM

M11

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 anonymous⁷.

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

⁷ 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. 106, London School of Economics and Political Science, London, UK.

mlj.

T.N #
JM

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 2016, 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.

T.N. #
RM.

MH

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.

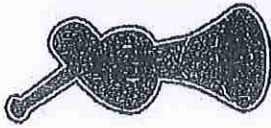
Conclusion

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

T.N #
RM
MH

TN2



RIGHT2KNOW

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

KWA ZULU NATAL
101 Dinwv 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

TN #
AM

MH

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 2016¹. R2K has developed a memorandum of concerns about RICA², 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

¹ UNHCR, *Concluding observations on the initial report of South Africa*, CCPR/C/ZAF/CO/1 (April 2016), 243-44.

² Memorandum, 'Demands to Stand Against Surveillance and Fix RICA' (April 2016). Available at www.r2k.org.za/rica-demands

MH

TN #
JUM

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

T.N. #

M.H.

QUM

TN3

J 404



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

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.

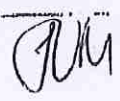
I was made aware of the fact that the Department of Justice and Constitutional Development (the Department) is considering amendments to the RICA. I would therefore request you to engage with the Department on possible amendments to the RICA, which may also include any suggestions which you would like 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

T.N #
MK
GJM


Judge G.S. Matuleka
Designated Judge
Date: 10/04/2017

T.N.#
MH



TN4

Refilwe Chulu

From: Refilwe Chulu <refilwe@lrc.org.za>
Sent: 22 January 2020 15:47
To: 'dario.milo@webberwentzel.com'; 'lavanya.pillay@webberwentzel.com';
'memakhubela@justice.gov.za'; 'rapulane@kgoroadiramudauinc.co.za';
'info@kgoroadiramudauinc.co.za'
Cc: 'david@lrc.org.za'; 'whitney@lrc.org.za'
Subject: [CCT 278/19] amaBhungane Centre for Investigative Journalism NPC and Another //
Minister of Justice and Correctional Services and Others
Attachments: [Letter] amaBhungane v Minister of Justice and Correctional Services.pdf

Dear All

1. We act for the Right2Know Campaign (R2K) and Privacy International (PI).
2. Kindly find the attached letter for your urgent attention requesting permission to intervene as *amici curiae* in the above mentioned matter.
3. Kindly note that David Mtshali is the newly appointed attorney in this matter as Carina du Toit is no longer at the Legal Resources Centre.

Warm regards

Refilwe Chulu | Bertha Justice Fellow, Candidate Attorney



| Tel: 011 836 9831 | Fax: 011 836 8680 | Email: refilwe@lrc.org.za
| Physical: 15th Floor Bram Fischer Towers | 20 Albert Street | Johannesburg
| Postal: P.O Box 9495 | Johannesburg 2000
| Website: www.lrc.org.za
| Johannesburg | Cape Town | Durban | Grahamstown



MAKE A SECURE DONATION

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error, please notify the sender. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Legal Resources Centre. Finally, the recipient should check this email and any attachments for the presence of viruses. The Legal Resources Centre accepts no liability for any damage caused by any virus transmitted by this email.

T.N
JUM

Johannesburg Office

15th Floor Bram Fischer Towers • 20 Albert Street • Marshalltown • Johannesburg 2001 • South Africa
PO Box 9495 • Johannesburg 2000 • South Africa
Tel: (011) 836 9831 • Fax: (011) 836 8680 • Website www.lrc.org.za
PBO No. 930003292
NPO No. 023-004

LRC

Legal Resources Centre

Your Ref: Case no: CCT 278/19

Our Ref: C du Toit / 1125816L

22 January 2020

Dario Milo

Webber Wentzel

By email: dario.milo@webberwentzel.com

javanya.pillay@webberwentzel.com

Office of the State Attorney

By email: hmaponya@justice.gov.za

memakhubela@justice.gov.za

M Kgoroadira

Kgoroadira Mudau Inc

By email: rapulane@kgoroadiramudauinc.co.za

info@kgoroadiramudauinc.co.za

Dear Sir / Madam

amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (Case No. CCT 278/19):

Request for Consent to be admitted as *amici curiae*

- 1 We act for the Right2Know Campaign (R2K) and Privacy International (PI).
- 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

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

N Govender (National Director)
S Dass (Director) A Andrews S Kahanovitz C Mathiso K Motlani M Mudarikwa A Turpin
S Samuel (Director) T Malstry TC Mbhense
C McConnachie (Director) S Mguga C van Schalkwyk
LJ Ltmacher (Acting Director) C du Toit L Nel D Mitchell
SG Magardie (Director) MJ Bishop G Bizos SC L Mgedezl Y Ntoko ER Webber

T.N

meet people's social, 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 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 Privacy International has an interest in the matter based on the following:
- 3.1 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.
 - 3.2 Privacy International has litigated several cases addressing issues central to the main application. In particular, Privacy International was one of the applicants in *10 Human Rights Organisations v United Kingdom*, a case that was before the ECtHR, challenging aspects of the U.K.'s surveillance regime.

T.N.
J.M.

- 3.3 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).
- 4 R2K and PI have considered the application for confirmation to the Constitutional Court as well as the cross appeal on behalf of the respondents. As amici curiae in the High Court, our clients are also familiar with the record in this matter. R2K and PI submit that it has novel legal submissions that will be relevant and helpful to the Court.
- 5 We are therefore instructed to approach you pursuant to Rule 10 of the Constitutional Court Rules, to request your written consent for R2K and PI to enter this matter as amici curiae.
- 6 The submission the amici curiae intend to file can be summarised as followed:
- 6.1 Our clients support the Applicants' arguments on the importance of post-interception notification to persons subject to surveillance and intend to assist the Court by providing comparative jurisprudence that supports the need for post-interception notification.
- 6.2 The Applicants attack RICA's provisions concerning the mandatory retention of communication related data (metadata). Their argument focuses on the length of time for, and the safeguards under, which the metadata is retained. R2K and PI will argue that the bulk retention of metadata is always unconstitutional, no matter the length for which it is kept. In advancing that position, R2K and PI will draw on international and comparative jurisprudence that supports the ban on blanket retention of metadata. R2K and PI will ask the Court to decide the matter in a way that would not preclude such a challenge in the future.
- 6.3 The Applicants argue that RICA does not adequately secure the independence of the designated judge. R2K and PI submit that, in addition to the matters identified by the Applicants, R2K and PI will submit that: (a) the independence of the designated judge is further compromised by the requirement that the designated judge is a retired

T.M.
GUM

judge; (b) the secrecy with which the designated judge operates enhances the need for independence; and (c) the need for an independent adjudicator is supported by comparative and international law and practice. Both of these serve to undermine the independence of the designated judge.

- 7 Our clients are aware of the directions of the Constitutional Court regarding the filing of written submissions. Our clients undertake to act with due haste in filing its application for admission as amici curiae. Furthermore, if admitted as amici curiae, R2k and PI will carefully consider the written submissions of the parties and will not repeat any submissions.
- 8 Accordingly, we request your client's consent that our clients be admitted as amici curiae with the right to make written submissions and to present oral argument.
- 9 We ask that advise whether your client consents to our client's intervention reach us by no later than close of business on 27 January 2020.
- 10 We look forward to hearing from you.



LEGAL RESOURCES CENTRE

Per: DAVID MTSHALI

011 836 9831

david@lrc.org.za/refilwe@lrc.org.za

T.N
AM

Refilwe Chulu

From: Motsau Mamosali <MMotsau@justice.gov.za>
Sent: 24 January 2020 12:58
To: david@lrc.org.za; refilwe@lrc.org.za; dario.milo@webberwentzel.com; lavanya.pillay@webberwentzel.com; Makhubela Meshack
Cc: Seleka Peter; pseleka@gmail.com; Sebelemetsa Ramathiti; ramatics@gmail.com
Subject: FW: NOTICE OF WITHDRAWAL BY Kgoroadia Mudau Inc and replaced by the STATE ATTORNEY -PRETORIA
Attachments: S021001280_2001241222000.pdf
Importance: High

Good day ALL

amaBhungane NPC, Sole Stephen Patrick/Minister of Justice and Correctional Services and Others – CCT 278/2019 and CCT 279/2019

Kindly find attached NOTICE OF WITHDRAWAL as Attorneys of record by M Kgoroadia INC (emails rapulana@kgoraediramudau.co.za and info@kgoroadiramudauinc.co.za .

Please SEND and forward all future correspondence for the MINISTER OF STATE SECURITY who is the Second Respondent in the above CASE with the following:

STATE ATTORNEY: PRETORIA
Attention : G P Seleka
Second Respondent - Minister of State Security)
THE STATE ATTORNEY, PRETORIA
316 SALU BUILDING
CNR FRANCIS BAARD & THABO SEHUME
GROUND FLOOR
PRETORIA
PRIVATE BAG X91
PRETORIA
TEL: (012) 309 1543
FAX: (012) 309 1649/50
REF: 5928/2019/Z65/MM

Regards

Ms Mamosali Motsau

Candidate Attorney to Mr G P. Seleka

Office of the State Attorney, Salu Building, 19th Floor,

316 Thabo Sehume Street, Pretoria 0001

Tel: 012 309 1543.

Cell : 076 376 0998

Email: MMotsau@justice.gov.za

T.N
JUM

COPY

252

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



Case no: 25978/17

In the matter between:

**AMABHUNGANE CENTRE FOR INVESTIGATIVE
JOURNALISM NPC**

1ST APPLICANT

SOLE, STEPHEN PATRICK

2ND APPLICANT

and

MINISTER OF JUSTICE AND CORRECTIONAL SERVICES

1ST RESPONDENT

MINISTER OF STATE SECURITY

2ND RESPONDENT

MINISTER OF COMMUNICATIONS

3RD RESPONDENT

MINISTER OF DEFENCE AND MILITARY VETERANS

4TH RESPONDENT

*T. W.
AM*

MINISTER OF POLICE

5TH RESPONDENT

THE OFFICE OF THE INSPECTOR-GENERAL OF
INTELLIGENCE

6TH RESPONDENT

THE OFFICE OF INTERCEPTION CENTRES

7TH RESPONDENT

THE NATIONAL COMMUNICATIONS CENTRE

8TH RESPONDENT

THE JOINT STANDING COMMITTEE ON
INTELLIGENCE

9TH RESPONDENT

THE STATE SECURITY AGENCY

10TH RESPONDENT

MINISTER OF TELECOMMUNICATIONS AND POSTAL
SERVICES

11TH RESPONDENT

NOTICE OF WITHDRAWAL AS ATTORNEYS

JIN
QUM

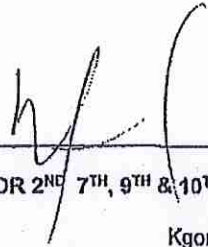
KINDLY TAKE NOTICE that Kgoroadira Mudau Inc herewith withdraw as attorneys of record for the 2nd, 7th, 9th and 10th Respondents.

FURTHER TAKE NOTICE that the provisions of Rule 16(4)(b) reads as follow:

"After such notice, unless the party formerly represented within 10 days after the notice, himself notifies all other parties of a new address for service as contemplated in sub-rule (2), it shall not, be necessary to serve any documents upon such party unless the court otherwise order: Provided that any of the other parties may before receipt of this notice of his new address for service of documents, serve any documents upon the party who was formerly represented."

FURTHER TAKE NOTICE that the 2nd, 7th, 9th and 10th Respondents' address is Musanda Complex, Delmas Road, PRETORIA.

SIGNED at Rosebank on the 26th day of September 2019



ATTORNEY FOR 2ND, 7TH, 9TH & 10TH RESPONDENTS

Kgoroadira Mudau Inc

Office 26, 3rd Floor 158 Jan Smuts Building

9 Walters Street

T.N. J.M.

Rosebank

Tel: 0112685807 Fax: 0865194846

E-mail: rapulane@kgoroadiramudauiinc.co.za

Ref: MK0002/xm

TO: REGISTRAR OF THE HIGH COURT
PRETORIA

AND TO: WEBBER WENTZEL
ATTORNEY FOR THE APPLICANTS

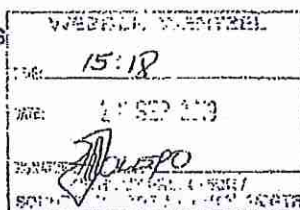
90 RIVONIA ROAD, SANDTON

JOHANNESBURG, 2196

Tel: 011 530 5232

E-mail: dario.milo@webberwentzel.com

Ref: Dario Milo / Makhotso Lengane / 3000547



RECEIVED A COPY ON THIS _____ DAY OF SEPTEMBER 2019

ATTORNEYS FOR THE APPLICANTS

T.N
J.M

AND TO: STATE ATTORNEY PRETORIA
ATTORNEY FOR THE 1ST, 4TH & 5TH RESPONDENTS
SALU BUILDING
316 THABO SEHUME STREET
PRIVATE BAG X91
PRETORIA, 0001
Tel: 012 309 1630
Ref: 2938/2017/Z62/MC

STATE ATTORNEY
RECEPTION
2019-09-27
PRIVATE BAG / PRIVAATBAG X91 (10) PRETORIA 0001
STAATSPROKUREUR

†
Oth'40

RECEIVED A COPY ON THIS ____ DAY OF SEPTEMBER 2019

ATTORNEYS FOR THE 1ST, 4TH & 5TH RESPONDENTS

AND TO: THE LEGAL RESOURCES CENTRE
ATTORNEY FOR THE RIGHT TO KNOW CAMPAIGN AND PRIVACY
INTERNATIONAL (*AMICI CURIAE*)
16TH FLOOR, BRAAM FISCHER TOWERS
20 ALBERT STREET
JOHANNESBURG, 2196
Tel: 011 836 9831
E-mail: Carlna@lrc.org.za
Ref: 1125816/LC du Tolt

TIN
NAM

Refilwe Chulu

From: Refilwe Chulu <refilwe@lrc.org.za>
Sent: 24 January 2020 15:53
To: 'MMotsau@justice.gov.za'
Subject: FW: [CCT 278/19] amaBhungane Centre for Investigative Journalism NPC and Another // Minister of Justice and Correctional Services and Others
Attachments: [Letter] amaBhungane v Minister of Justice and Correctional Services.pdf

Good day

Kindly find the attached for your urgent attention.

Warm regards

Refilwe Chulu | Bertha Justice Fellow, Candidate Attorney



| Tel: 011 836 9831 | Fax: 011 836 8680 | Email: refilwe@lrc.org.za
| Physical: 15th Floor Bram Fischer Towers | 20 Albert Street | Johannesburg
| Postal: P.O Box 9495 | Johannesburg 2000
| Website: www.lrc.org.za
| Johannesburg | Cape Town | Durban | Grahamstown



MAKE A SECURE DONATION

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error, please notify the sender. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Legal Resources Centre. Finally, the recipient should check this email and any attachments for the presence of viruses. The Legal Resources Centre accepts no liability for any damage caused by any virus transmitted by this email.

From: Refilwe Chulu [<mailto:refilwe@lrc.org.za>]

Sent: 22 January 2020 15:47

To: 'dario.milo@webberwentzel.com'; 'lavanya.pillay@webberwentzel.com'; 'memakhubela@justice.gov.za'; 'rapulane@kgoroadramudaulnc.co.za'; 'info@kgoroadramudaulnc.co.za'

Cc: 'david@lrc.org.za'; 'whitney@lrc.org.za'

Subject: [CCT 278/19] amaBhungane Centre for Investigative Journalism NPC and Another // Minister of Justice and Correctional Services and Others

Dear All

1. We act for the Right2Know Campaign (R2K) and Privacy International (PI).
2. Kindly find the attached letter for your urgent attention requesting permission to Intervene as *amici curiae* in the above mentioned matter.
3. Kindly note that David Mtshali is the newly appointed attorney in this matter as Carina du Toit is no longer at the Legal Resources Centre.

Warm regards

AM
IN


Refilwe Chulu | Bertha Justice Fellow, Candidate Attorney

LRC

Legal Resources Centre

| Tel: 011 836 9831 | Fax: 011 836 8680 | Email: refilwe@lrc.org.za
| Physical : 15th Floor Bram Fischer Towers | 20 Albert Street | Johannesburg
| Postal: P.O Box 9495 | Johannesburg 2000
| Website: www.lrc.org.za
| Johannesburg | Cape Town | Durban | Grahamstown



MAKE A SECURE DONATION 

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error, please notify the sender. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Legal Resources Centre. Finally, the recipient should check this email and any attachments for the presence of viruses. The Legal Resources Centre accepts no liability for any damage caused by any virus transmitted by this email.

AK
T.N

Johannesburg Office

15th Floor Bram Fischer Towers • 20 Albert Street • Marshalltown • Johannesburg 2001 • South Africa
PO Box 9495 • Johannesburg 2000 • South Africa
Tel: (011) 836 9831 • Fax: (011) 836 8680 • Website www.lrc.org.za
PBO No. 930003292
NPO No. 023-004



Your Ref: Case no: CCT 278/19

Our Ref: C du Toit / 1125816L

22 January 2020

Dario Milo

Webber Wentzel

By email: dario.milo@webberwentzel.com

lavanya.pillay@webberwentzel.com

Office of the State Attorney

By email: hmaponya@justice.gov.za

memakhubela@justice.gov.za

M Kgoroadira

Kgoroadira Mudau Inc

By email: rapulane@kgoroadiramudauinc.co.za

info@kgoroadiramudauinc.co.za

Dear Sir / Madam

amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (Case No. CCT 278/19):

Request for Consent to be admitted as *amici curiae*

- 1 We act for the Right2Know Campaign (R2K) and Privacy International (PI).
- 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

T.N

meet people's social, 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 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 Privacy International has an interest in the matter based on the following:

- 3.1 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.
- 3.2 Privacy International has litigated several cases addressing issues central to the main application. In particular, Privacy International was one of the applicants in *10 Human Rights Organisations v United Kingdom*, a case that was before the ECtHR, challenging aspects of the U.K.'s surveillance regime.

AM

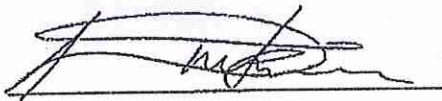
J.N

- 3.3 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).
- 4 R2K and PI have considered the application for confirmation to the Constitutional Court as well as the cross appeal on behalf of the respondents. As amici curiae in the High Court, our clients are also familiar with the record in this matter. R2K and PI submit that it has novel legal submissions that will be relevant and helpful to the Court.
- 5 We are therefore instructed to approach you pursuant to Rule 10 of the Constitutional Court Rules, to request your written consent for R2K and PI to enter this matter as amici curiae.
- 6 The submission the amici curiae intend to file can be summarised as followed:
- 6.1 Our clients support the Applicants' arguments on the importance of post-interception notification to persons subject to surveillance and intend to assist the Court by providing comparative jurisprudence that supports the need for post-interception notification.
- 6.2 The Applicants attack RICA's provisions concerning the mandatory retention of communication related data (metadata). Their argument focuses on the length of time for, and the safeguards under, which the metadata is retained. R2K and PI will argue that the bulk retention of metadata is always unconstitutional, no matter the length for which it is kept. In advancing that position, R2K and PI will draw on international and comparative jurisprudence that supports the ban on blanket retention of metadata. R2K and PI will ask the Court to decide the matter in a way that would not preclude such a challenge in the future.
- 6.3 The Applicants argue that RICA does not adequately secure the independence of the designated judge. R2K and PI submit that, in addition to the matters identified by the Applicants, R2K and PI will submit that: (a) the independence of the designated judge is further compromised by the requirement that the designated judge is a retired

JUM
T.N

judge; (b) the secrecy with which the designated judge operates enhances the need for independence; and (c) the need for an independent adjudicator is supported by comparative and international law and practice. Both of these serve to undermine the independence of the designated judge.

- 7 Our clients are aware of the directions of the Constitutional Court regarding the filing of written submissions. Our clients undertake to act with due haste in filing its application for admission as amici curiae. Furthermore, if admitted as amici curiae, R2k and PI will carefully consider the written submissions of the parties and will not repeat any submissions.
- 8 Accordingly, we request your client's consent that our clients be admitted as amici curiae with the right to make written submissions and to present oral argument.
- 9 We ask that advise whether your client consents to our client's intervention reach us by no later than close of business on 27 January 2020.
- 10 We look forward to hearing from you.



LEGAL RESOURCES CENTRE

Per: DAVID MTSHALI

011 836 9831

david@lrc.org.za/refilwe@lrc.org.za

AM
T.N

TNS

Refilwe Chulu

From: Lavanya Pillay <Lavanya.Pillay@webberwentzel.com>
Sent: 27 January 2020 19:38
To: david@lrc.org.za; refilwe@lrc.org.za; Whitney Stevens
Cc: Dario Milo; Divashen Naidoo; Makhubela Meshack; PSeleka@justice.gov.za; MMotsau@justice.gov.za
Subject: amaBhungane Centre for Investigative Journalism NPC and Another // Minister of Justice and Correctional Services and Others (CCT 278/19)
Attachments: 20200127 Letter from WW to LRC.pdf

Dear all

Please find attached correspondence for your attention.

Yours faithfully

Lavanya Pillay | Associate

T: +27115305078 | M: +27737729947 | lavanya.pillay@webberwentzel.com | www.webberwentzel.com

WEBBER WENTZEL

In alliance with > Linklaters

African Law Firm of the Year (African Legal Awards, 2019)

This email is confidential and may also be legally privileged. If you are not the intended recipient, please notify the sender immediately and then delete it. Please do not copy, disclose its contents or use it for any purpose. Webber Wentzel will not be liable for any unauthorised use of, or reliance on, this email or any attachment. This email is subject to and incorporates our standard terms of business.

AM
TN

WEBBER WENTZEL

In alliance with > Linklaters

Mr David Mtshali
Legal Resources Centre

By email: david@lrc.org.za; refilwe@lrc.org.za;
whitney@lrc.org.za

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

Your reference

Our reference

Date

D Milo / L Pillay / D Naidoo
3034325

27 January 2020

Dear Sir

amaBhungane Centre for Investigative Journalism NPC and Another // Minister of Justice
and Correctional Services and Others (CCT 278/19)

1. We act for the applicants in the above matter.
2. We refer to your letter dated 22 January 2020 ("your letter"). Our clients hereby consent to your clients' request to be admitted as *amicus curiae* in the above matter on the basis set out in your letter.

Yours faithfully

WEBBER WENTZEL

Dario Milo

Partner

Direct tel: +27 11 530 5232

Direct fax: +27 11 530 6232

Email: dario.milo@webberwentzel.com

Letter sent electronically.

Senior Partners: JC Els Managing Partner: SJ Hutton Partners: BW Abraham RB Africa M Adderley NG Alp RL Appelbaum DC Bayman
KL Bellings AE Bennett AP Blair DHL Booysen AR Bowley MS Burger RI Carrim T Cassim SJ Chong KL Collier KM Colman KE Coster K Couzyn
DB Cron PA Crosland JH Davies PH Daya L de Bruyn PJ Dela M Denenga DW de Villiers BEC Dickinson MA Diemont DA Dingley G Driver W Drue
HJ du Preez CP du Toit SK Edmundson KH Eiser AE Esterhuizen MJR Evans K Fazel AA Feleklis G Fitzmaurice JB Forman C Gabriel CP Gaul
KL Gawlth Oil Geldenhuys MM Gibson CI Gouws PD Grealy S Haroun JM Harvey MH Hathorn JS Henning KR Hillis S Hockey CM Hoffeld
PN Holloway AV Ismail ME Jarvis CA Jennings CM Jonker S Jooste LA Kahn ACR Katzke M Kennedy A Keyser MD Kota JC Kraamwinkel M Kyle
J Lamb E Louw M Mahlangu L Marais S McCafferty MC McIntosh SJ McKenzie CS Meyer AJ Mills D Milo NP Mngomezulu M Moloi LE Mostert
VM Movshovich RA Nelson G Niven ZN Mtshona M Nxumalo AN Nyatumba I Odendaal GJP Olivier N Palge AMT Pardini AS Parry S Patel
GR Penfold SE Phajane M Philippides BA Phillips MA Phillips D Ramfettan GI Rapson Z Rawoot K Rew SA Ritchie NJA Robb DC Rudman G Sader
M Sader H Samsodien JW Scholtz KE Shepherd AJ Simpson N Singh N Singh-Nogueira P Singh S Sithole J Smit RS Smith MP Spalding PS Stein
MW Straeuli LJ Swaine Z Swanapoel A Thakor TK Thekiso C Theodossou R Thavanji PZ Vanda SE van der Meulen JP van der Poel CS Vanmali
JE Veeran B Versfeld MG Versfeld TA Versfeld DM Visagie EME Warrington J Watson AWR Westwood RH Wilson M Yutaken Chief Operating
Officers: SA Boyd

JM

T.N

TN 6

Refilwe Chulu

From: Motsau Mamosali <MMotsau@justice.gov.za>
Sent: 27 January 2020 07:34
To: Refilwe Chulu
Cc: Seleka Peter; Sebelemetsa Ramathiti; Ken@law.co.za; Lesirelal@gmail.com
Subject: RE: [CCT 278/19] amaBhungane Centre for Investigative Journalism NPC and Another // Minister of Justice and Correctional Services and Others

Good day Ms Chulu

Our client has no objection to your request. We therefore agree to your request.

The Notice of Withdrawal by M Kgoroadia INC was sent to your email on Fri 2020/01/24 12:58 and copied to david@lrc.org.za with the following message:

"Kindly find attached NOTICE OF WITHDRAWAL as Attorneys of record by M Kgoroeadia INC (emails rapulana@kgoraediramudau.co.za and info@kgoraediramudauinc.co.za).

Please SEND and forward all future correspondence for the MINISTER OF STATE SECURITY who is the Second Respondent in the above CASE with the following:

STATE ATTORNEY: PRETORIA
Attention : G P Seleka
Second Respondent - Minister of State Security)
THE STATE ATTORNEY, PRETORIA
316 SALU BUILDING
CNR FRANCIS BAARD & THABO SEHUME
GROUND FLOOR
PRETORIA
PRIVATE BAG X91
PRETORIA
TEL: (012) 309 1543
FAX: (012) 309 1649/50
REF: 5928/2019/Z65/MM

Thanking you for removing the above attorney in your correspondence to our office regarding the above matter.

Regards,

Ms Mamosali Motsau
Candidate Attorney to Mr GP Seleka
Office of the State Attorney. Salu Building, 19th Floor,
316 Thabo Sehume Street, Pretoria 0001
Tel: 012 309 1543.
Cell : 076 376 0998
Email: MMotsau@justice.gov.za

MM
TN

From: Refilwe Chulu [mailto:refilwe@lrc.org.za]
Sent: 24 January 2020 03:53 PM
To: Motsau Mamosali
Subject: FW: [CCT 278/19] amaBhungane Centre for Investigative Journalism NPC and Another // Minister of Justice and Correctional Services and Others

Good day

Kindly find the attached for your urgent attention.

Warm regards

Refilwe Chulu | Bertha Justice Fellow, Candidate Attorney



| Tel: 011 836 9831 | Fax: 011 836 8680 | Email: refilwe@lrc.org.za
| Physical : 15th Floor Bram Fischer Towers | 20 Albert Street | Johannesburg
| Postal: P.O Box 9495 | Johannesburg 2000
| Website: www.lrc.org.za
| Johannesburg | Cape Town | Durban | Grahamstown



MAKE A SECURE DONATION

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error, please notify the sender. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Legal Resources Centre. Finally, the recipient should check this email and any attachments for the presence of viruses. The Legal Resources Centre accepts no liability for any damage caused by any virus transmitted by this email.

From: Refilwe Chulu [mailto:refilwe@lrc.org.za]
Sent: 22 January 2020 15:47
To: 'darlo.milo@webberwentzel.com'; 'lavanya.pillay@webberwentzel.com'; 'memakhubela@justice.gov.za'; 'rapulane@kgoroadiramudaulinc.co.za'; 'info@kgoroadiramudaulinc.co.za'
Cc: 'david@lrc.org.za'; 'whitney@lrc.org.za'
Subject: [CCT 278/19] amaBhungane Centre for Investigative Journalism NPC and Another // Minister of Justice and Correctional Services and Others

Dear All

1. We act for the Right2Know Campaign (R2K) and Privacy International (PI).
2. Kindly find the attached letter for your urgent attention requesting permission to intervene as *amici curiae* in the above mentioned matter.
3. Kindly note that David Mtshali is the newly appointed attorney in this matter as Carina du Toit is no longer at the Legal Resources Centre.

Warm regards

Refilwe Chulu | Bertha Justice Fellow, Candidate Attorney

LRC

Legal Resources Centre

| Tel: 011 836 9831 | Fax: 011 836 8680 | Email: refilwe@lrc.org.za
| Physical: 15th Floor Bram Fischer Towers | 20 Albert Street | Johannesburg
| Postal: P.O Box 9495 | Johannesburg 2000
| Website: www.lrc.org.za
| Johannesburg | Cape Town | Durban | Grahamstown



MAKE A SECURE DONATION

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error, please notify the sender. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Legal Resources Centre. Finally, the recipient should check this email and any attachments for the presence of viruses. The Legal Resources Centre accepts no liability for any damage caused by any virus transmitted by this email.

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.

AM

T.N

TN7

Refilwe Chulu

From: Makhubela Meshack <MeMakhubela@justice.gov.za>
Sent: 24 January 2020 12:29
To: refilwe@lrc.org.za; david@lrc.org.za
Subject: RE: AMABHUNGANE MATTER
Attachments: S021001280_2001241226000.pdf

Importance: High

Good Day

Please find attached herewith our self-explanatory letter dated 24th January 2020 for your attention.

Regards



the doj & ccd

Department:
 Justice and Constitutional Development
 REPUBLIC OF SOUTH AFRICA

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 / mtiyani1@gmail.com

Website: www.doj.gov.za

"I can do all things through Christ who strengthens me" Philippians 4:13

From: minolta@justice.gov.za [mailto:minolta@justice.gov.za]
Sent: Friday, January 24, 2020 2:27 PM
To: Makhubela Meshack <MeMakhubela@justice.gov.za>
Subject:

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.

MTN



Office of the State Attorney Pretoria

Private Bag X 91
PRETORIA
0001

SALU Building
316 Andries Street
PRETORIA

Tel: (Switchboard): (012) 309 1500
(Direct Line): (012) 309 1630
(Secretary): (012) 309 1570

Fax (General) (012) 309 1849/50
(Direct) 086 640 1943

24th January 2020

Enquires: M Makhubela
Email: mamakhubela@justice.gov.za

My ref: 2936/2017/Z52/mc
Your ref: C du Toit / 1125816L

FAX: (011) 836 8680

TEL: (011) 836 9831

ATT: DAVID MTSHALI
Legal Resources Centre
20 Albert Street
Marshalltown
Johannesburg
200
Email: david@lrc.org.za / refilwe@lrc.org.za

ATT: DARIO MILO
Webber Wentzel
Email: Dario.milo@webberwentzel.com
Lavanya.pillay@webberwentzel.com

Sir / Madam

Re: AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC
AND OTHERS V MINISTER OF JUSTICE AND CORRECTIONAL
SERVICES AND OTHERS (Case No. CCT 278/19)

1. We refer to the above matter and in particular your letter dated 22 January 2020 requesting consent for your clients Right2Know and Privacy International to be admitted as *amici curiae*.
2. Having read your letter our clients Minister of Police and the Minister of Justice and Correctional Services hereby grant

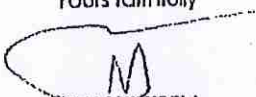
Access to Justice for All

Always quote my reference number

JUM T.N

consent for your clients to be admitted as *amici curiae* in regard to the above mentioned Case.

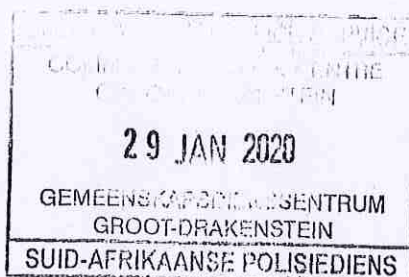
Yours faithfully



M. MAKHUBELA
FOR: STATE ATTORNEY (PRETORIA)

Access to Justice for All

Always quote my reference number



JM TN

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

Case no: CCT 278/19

In the matter between:

AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC First Applicant

SOLE STEPHEN PATRIC Second Applicant

and

MINISTER OF JUSTICE AND CORRECTIONAL SERVICES First Respondent

MINISTER OF STATE SECURITY Second Respondent

MINISTER OF COMMUNICATIONS Third Respondent

MINISTER OF DEFENCE AND MILITARY VETERANS Fourth Respondent

MINISTER OF POLICE Fifth Respondent

THE OFFICE OF INSPECTOR-GENERAL OF INTELLIGENCE Sixth Respondent

THE OFFICE FOR INTERCEPTION CENTRES Seventh Respondent

THE NATIONAL COMMUNICATIONS CENTRE Eighth Respondent

THE JOINT STANDING COMMITTEE ON INTELLIGENCE Ninth Respondent

THE STATE SECURITY AGENCY Tenth Respondent

CONFIRMATORY AFFIDAVIT

I, the undersigned

ILIA MARIA SIATITSA

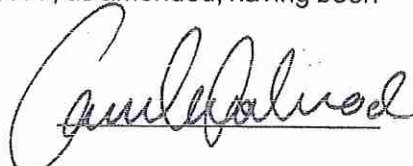
state under oath/affirm and declare as follows:

1. I am an adult female and employed as a 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 Floyd Thami Nkosi and confirm the content thereof insofar as it relates to myself and Privacy International.



ILIA MARIA SIATITSA

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, UK on this the 29 day of January 2020, the regulations contained in Government Notice No. R1648 of 19 August 1977, as amended, having been complied with.



COMMISSIONER OF OATHS
CAMILLA GRAHAM WOOD
SOLICITOR 465175

2
Privacy International
62 Britton Street
London
EC1M 5UY