IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

Case No: CCT 278/19

Case No: CCT 279/19

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

and

MEDIA MONITORING AFRICA TRUST	First Amicus Curiae
RIGHT2KNOW CAMPAIGN	Second Amicus Curiae

PRIVACY INTERNATIONAL Third Amicus Curiae

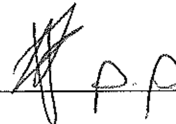
FILING SHEET

DOCUMENTS FILED: SECOND AMICUS CURIAE PRACTICE NOTE, WRITTEN SUBMISSIONS AND TABLE OF AUTHORITIES

DATE FILED: 12 FEBRUARY 2020

DATE ON THE ROLL: 25 FEBRUARY 2020

DATED AT **JOHANNESBURG** ON THIS THE **12**[TH] DAY OF **FEBRUARY** 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/
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
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

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

Ref: 2937/2017/Z52/MC

Tel: (012) 309 – 1630

Fax: 0860 640 1943

Dx: 298 PRETORIA
Email: memakhubela@justice.gov.za / conkuna@justice.gov.za
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
Tel: (012) 309 1543
Fax: (012) 309 1649/50
Ref: 5928/2019/Z65/MM
Email: MMotsau@justice.gov.za

AND TO: **POWER SINGH INCORPORATED**
First Amicus Attorneys
First Floor, 20 Baker Street
Rosebank
JOHANNESBURG
Tel: (011) 268 6811
Fax: 086 614 5818
Email: avani@powersingh.africa/ michael@powersingh.africa/
tina@powersingh.africa
Ref: PSIMM-202002

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

CCT 278/19

In the application of:

AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC	First Applicant
SOLE, STEPHEN PATRICK	Second Applicant
and	
MINISTER OF JUSTICE AND CORRECTIONAL SERVICES	First Respondent
NINE OTHERS	Second to Tenth Respondents
and	
THE RIGHT2KNOW CAMPAIGN	Second *Amicus Curiae*
PRIVACY INTERNATIONAL	Third *Amicus Curiae*

SECOND AMICUS CURIAE'S PRACTICE NOTE

NATURE OF PROCEEDINGS

1. This is an application for confirmation of, and appeals against, declarations that various provisions of the Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002 are unconstitutional and invalid.

2. The High Court's judgment is reported as: *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services* and Others [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP) ; 2020 (1) SACR 139 (GP)

THE ISSUES THAT WILL BE ARGUED

3. Right2Know Campaign (**R2K**) will make submissions concerning:

   3.1. Post-surveillance notification (High Court Order 1); and

   3.2. The independence of the designated judge (High Court Order 2).

ESTIMATED DURATION OF ARGUMENT

4. R2K estimates that it will require 15 minutes for oral argument.

NECESSARY PORTIONS OF THE RECORD

5. R2K defers to the parties on which portions of the Record are necessary.

SUMMARY OF APPLICANTS' ARGUMENT

Post-Surveillance Notification

6. R2K will advance two arguments to support confirmation of the High Court's order.

7. First, the prohibition on post-surveillance notification limits s 38 of the Constitution.

8. Second, international and comparative law support the need for post-surveillance notification, and the ability to do so without prejudicing efforts to fight crime.

The Designated Judge

9. R2K will advance four arguments to support confirmation of the High Court's order.

10. First, the failure to ensure the designated judge is independent is, primarily, a violation of the right to privacy.

11. Second, the fact that the designated judge operates in secrecy demands a higher degree of structural independence.

12. Third, combined with term renewal, the fact that the designated judge must be a retired judge undermines her independence.

13. Fourth, international and comparative law support the need for independence, and

the claim that the designated judge is insufficiently independent.

LIST OF AUTHORITIES ON WHICH SPECIAL RELIANCE WILL BE PLACED

1. *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* [2008] ZACC 13; 2008 (2) SACR 421 (CC); 2009 (1) SA 1 (CC).

2. *Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age,* U.N. Doc. A/HRC/27/37 (30 June 2014).

3. *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights* (2018) A/HRC/39/29.

MICHAEL BISHOP

PATRICK WAINWRIGHT

Counsel for the R2K

Chambers, Cape Town

12 February 2020

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

CCT 278/19

In the application of:

AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC	First Applicant
SOLE, STEPHEN PATRICK	Second Applicant

and

MINISTER OF JUSTICE AND CORRECTIONAL SERVICES	First Respondent
NINE OTHERS	Second to Tenth Respondents

and

THE RIGHT2KNOW CAMPAIGN	Second *Amicus Curiae*
PRIVACY INTERNATIONAL	Third *Amicus Curiae*

SECOND AMICUS CURIAE'S WRITTEN SUBMISSIONS

TABLE OF CONTENTS

I INTRODUCTION 1

II INTERNATIONAL AND COMPARATIVE LAW 3

III POST-SURVEILLANCE NOTIFICATION 4

SECTION 38 VIOLATION 4

INTERNATIONAL LAW 6

COMPARATIVE LAW 9

CONCLUSION 11

IV THE DESIGNATED JUDGE 12

RIGHT TO PRIVACY 12

SECRECY 13

THE DANGER OF A RETIRED JUDGE 15

INTERNATIONAL AND COMPARATIVE LAW 17

IV CONCLUSION 18

I INTRODUCTION

1. *"Everyone has the right to privacy, which includes the right not to have … the privacy of their communications infringed"*.[1] The right to privacy – and particularly to the privacy of our communications – is central to the constitutional order founded on human dignity. As O'Regan J has held, we protect privacy because of *"our constitutional understanding of what it means to be a human being"*.[2] That understanding *"presupposes personal space within which to live this life."*[3] That personal space is the way we *"live our daily lives. This sphere in which to pursue our own ends and interests in our own ways, although often mundane, is intensely important to what makes human life meaningful."*[4]

2. This personal privacy extends to where we go, and what we do with our mobile phones. As Langa DCJ (as he then was) explained in *Hyundai*: *"when people are … on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied."*[5]

3. This application concerns serious threats to the privacy of our constitutionally protected personal space. It is a challenge to the constitutionality of the Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002 (**RICA**). RICA, combined with the development of modern technology and the way we use that technology allow intense intrusions by the South African state authorities into our personal daily lives.

---

[1] Constitution s 14(d).

[2] *NM and Others v Smith and Others* [2007] ZACC 6; 2007 (5) SA 250 (CC) at para 131 (O'Regan J dissenting).

[3] Ibid.

[4] Ibid at 130.

[5] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* [2000] ZACC 12; 2001 (1) SA 545 (CC) at para 16.

4. RICA allows the state to intercept our personal electronic communications – our phone calls, our text messages and emails. Those interception orders are made without any notification to the subject, even after the investigation has been completed. And they are made by a "*designated judge*" who lacks the most basic protections to ensure her independence from the executive.

5. An independent judge, and notification of surveillance after it has occurred are two basic protections of the right to privacy. They are required by international law, and are common in comparable democracies. The orders of the High Court declaring the relevant provisions of RICA unconstitutional should be upheld.

6. These written submissions are structured as follows:

    6.1. **Part II** briefly summarises the importance of **international and comparative law**;

    6.2. **Part III** address **post-interception notification**; and

    6.3. **Part IV** concerns the independence of the **designated judge**.

7. The Right2Know Campaign (**R2K**) also endorses the written submissions of Privacy International on the issue of the safeguards for the retention of metadata, and bulk surveillance.

II INTERNATIONAL AND COMPARATIVE LAW

8. The *Amici* rely in detail on international and comparative law. It is necessary to explain its relevance.

9. **International law** is relevant for three reasons:

   9.1. When interpreting the Bill of Rights, s 39(1)(b) of the Constitution mandates courts to consider international law.[6]

   9.2. When it determines whether a limitation of a right is reasonable and justifiable "*in an open and democratic society*" in terms of s 36(1), a court will look to international norms.

   9.3. Courts must consider not only, the international treaties, but also the relevant commentary on those treaties, particularly those issued by the bodies established to interpret and apply the relevant treaty.[7] This so-called "soft law" is not binding, but is persuasive.

10. Courts are not compelled to consider **comparative law**. But they are permitted to do so when interpreting the Bill of Rights.[8] Courts must be cautious when relying on foreign law, and should not import foreign doctrines to South Africa uncritically.[9] Nonetheless, comparative practice – in the form of both legislation and judicial decisions – can illuminate our own Constitution. It, too, is particularly relevant in

[6] See generally *Glenister v President of the Republic of South Africa and Others* [2011] ZACC 6; 2011 (3) SA 347 (CC) at para 189.

[7] See, for example, *Government of the Republic of South Africa and Others v Grootboom and Others* [2000] ZACC 19; 2001 (1) SA 46 (CC) at paras 29-31; *Motswagae and Others v Rustenburg Local Municipality and Another* [2013] ZACC 1; 2013 (3) BCLR 271 (CC); 2013 (2) SA 613 (CC) at fn 6; *Doctors for Life International v Speaker of the National Assembly and Others* [2006] ZACC 11; 2006 (12) BCLR 1399 (CC); 2006 (6) SA 416 (CC) at paras 95-6.

[8] Constitution s 39(1)(c).

[9] See, for example, *Bernstein and Others v Bester NO and Others* [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (CC) at para 132.

the s 36(1) analysis – if there is a clear trend in comparative practice, it may suggest that a law is or is not justifiable in an "*open and democratic society*".

III POST-SURVEILLANCE NOTIFICATION

11. RICA allows people to be placed under surveillance, and never to be notified that this occurred – even after the surveillance is complete, and when secrecy is no longer necessary to protect the investigation. R2K supports the High Court's order and the Applicants' submissions. It advances three additional arguments:

    11.1. The absence of notification violates **s 38 of the Constitution**;

    11.2. **International law** requires notification; and

    11.3. **Comparative law** shows notification is feasible.

SECTION 38 VIOLATION

12. The Applicants properly rely on s 34 of the Constitution which establishes a "*right to an effective remedy*"[10] for the violation of any legal right, including constitutional rights. But the Constitution includes an additional guarantee for the vindication of constitutional rights – s 38.

13. Section 38 creates a right to approach a court when a constitutional right has been

[10] *President of the Republic of South Africa and Another v Modderklip Boerdery (Pty) Ltd* [2005] ZACC 5; 2005 (5) SA 3 (CC); 2005 (8) BCLR 786 (CC) at para 50; *Government of the Republic of Zimbabwe v Fick and Others* [2013] ZACC 22; 2013 (5) SA 325 (CC); 2013 (10) BCLR 1103 (CC) at para 60.

infringed or threatened, but also a right to "*appropriate relief*".[11] This Court has held it establishes a "*right to a remedy*" where a constitutional right has been infringed.[12] And "*an appropriate remedy must mean an effective remedy, for without effective remedies for breach, the values underlying and the rights entrenched in the Constitution cannot properly be upheld or enhanced.*"[13]

14. Section 38 needs to be read together with s 172(1)(a) of the Constitution which provides: "*When deciding a constitutional matter within its power, a court <u>must</u> declare that any law or conduct that is inconsistent with the Constitution is invalid to the extent of its inconsistency*". And with s 172(1)(b) which empowers a court to grant any order that is "*just and equitable*" when determining a constitutional matter.[14]

15. Surveillance, even with authorisation, will always limit or threaten the right to privacy. It entails state interception of communication which is directly protected by s 14(d). Section 38 entitles the subject to an effective remedy for that limitation. Notification is necessary to allow a subject of surveillance to obtain an "*appropriate remedy*".

16. There are multiple remedies that can effectively vindicate the right even after the surveillance has been concluded – a declaration of rights, constitutional damages, and an order that the surveillance material be destroyed or provided to the subject.

---

[11] Constitution s 38 reads: "*Anyone listed in this section ...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.*"

[12] *Law Society of South Africa and Others v Minister for Transport and Another* [2010] ZACC 25; 2011 (1) SA 400 (CC); 2011 (2) BCLR 150 (CC) at paras 102-3.

[13] *Fose v Minister of Safety and Security* 1997 (3) SA 786 (CC), 1997 (7) BCLR 851 (CC). The Court has since made it clear that this holding applies to s 38. See *National Coalition for Gay and Lesbian Equality v Minister of Home Affairs & Others* 2000 (2) SA 1 (CC), 2000 (1) BCLR 39 (CC) at para 65.

[14] See *Head of Department : Mpumalanga Department of Education and Another v Hoërskool Ermelo and Another* [2009] ZACC 32; 2010 (2) SA 415 (CC); 2010 (3) BCLR 177 (CC) at para 97.

Section 38 expressly recognises a declaration of rights as an appropriate remedy.[15] None of those remedies are available if the subject does not know that she has been under surveillance.

17. The right to an effective remedy is a firm part of international law. The UDHR[16] and the ICCPR[17] require states to provide remedies for rights violations. The HRC has emphasised that "*[a]dministrative mechanisms are particularly required to give effect to the general obligation to investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies.*"[18] The Committee also recognises that "*public apologies, public memorials, guarantees of non-repetition and changes in relevant laws and practices*" can provide an effective remedy.[19]

INTERNATIONAL LAW

18. International law provides strong support for the need for post-interception notification.

---

[15] *Rail Commuters Action Group v Transnet Ltd t/a Metrorail* [2004] ZACC 20; 2005 (2) SA 359 (CC); 2005 (4) BCLR 301 (CC) at para 107 ("*A declaratory order is a flexible remedy which can assist in clarifying legal and constitutional obligations in a manner which promotes the protection and enforcement of our Constitution and its values.*")

[16] Article 8 of the Universal Declaration on Human Rights provides: "*Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law*".

[17] Article 2(3) of the International Covenant on Civil and Political Rights reads in full:

> *3. Each State Party to the present Covenant undertakes:*
>
> *(a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;*
>
> *(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;*

(c) To ensure that the competent authorities shall enforce such remedies when granted."

[18] UN Human Rights Committee (HRC) *General Comment no. 31, The Nature of the General Legal Obligation imposed on States Parties to the Covenant* (26 May 2004) CCPR/C/21/Rev.1/Add.13 at para 15.

[19] Ibid at para 16.

19. First, the United Nations Office of the High Commissioner for Human Rights (**OHCHR**) has determined that, to be effective, "*remedies must be known and accessible to anyone with an arguable claim that their rights have been violated.*"[20] That makes notice a "*critical issue[ ] in determining access to effective remedy.*"[21] In 2018, the OHCHR wrote explicitly: "*Recognizing that advance or concurrent notification might jeopardize the effectiveness of legitimate surveillance measures, individuals should nevertheless be notified once surveillance has been completed*".[22]

20. Second, the Special Rapporteur put the position in even stronger terms. In 2013, he concluded: "*Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State.*"[23] That notification can occur after the surveillance ends.

21. Third, in its 2016 evaluation of Poland, the HRC expressed "*particular concern*" about "*the lack of notification, complaints procedure or mechanism for remedies*".[24]

22. In sum, international treaties binding on South Africa have been interpreted to require post-surveillance notification. That is a powerful factor in favour of a finding that the limitation of the rights to privacy, access to court, and to a remedy is not justifiable.

---

[20] See *Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age,* U.N. Doc. A/HRC/27/37 (30 June 2014) at 40. The Commissioner noted that "*States take different approaches to notification*". While some require notification, others do not, and others require notification only in criminal cases. Of course, the conduct of states cannot justify what is otherwise a rights violation.

[21] Ibid.

[22] *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights* (2018) A/HRC/39/29 at para 54.

[23] See *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,* U.N. Doc. A/HRC/23/40 (17 April 2013) at 82 (my emphasis).

[24] See *Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee,* U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016).

23. European law adopts the same approach. The Court of Justice for the European Union (**CJEU**) and the European Court of Human Rights (**ECtHR**) have both recognized that notification is a critical safeguard when governments conduct surveillance.[25]

24. In *Szabó and Vissy v Hungary*, the ECtHR held that "*subsequent notification of surveillance measures*" was "*inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers*". [26] It held that notification should occur as soon as possible "*without jeopardising the purpose of the restriction after the termination of the surveillance measure*".[27]

25. In *Tele2 Sverige AB and C-698/15 Watson and Others*,[28] the CJEU held that states "*must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities*". Notification, the Court stressed, is "*necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.*"[29]

26. It is true that the ECtHR has recognised the alternative of standing to challenge the possibility of surveillance.[30] Section 38 of the Constitution likely affords that

---

[25] These cases are in addition to *Zakharov v Russia* (2016) 63 EHRR 17 cited by the Applicants. Applicants' Written Submissions at para 36.

[26] [2016] ECHR 579 at para 86.

[27] Ibid. In *Big Brother Watch & Others v United Kingdom* [2018] ECHR 722 at para 310, the ECHR summarised its earlier jurisprudence as follows:

> "*the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken.*"

The ECHR declined to extend the requirement of subsequent notification to bulk surveillance because it would not be possible to notify all the subjects of surveillance. Ibid at para 317.

[28] [2016] EUCJEU C-203/15 at para 121 (my emphasis).

[29] Ibid at para 121 (my emphasis).

[30] See, for example, *Big Brother Watch* (n 27) at para 310.

standing. However, it is a poor substitute for individual notification. It relies on a person having a reason to suspect that she was under surveillance, and the interest to approach a court on that mere possibility. If surveillance is professionally performed, such suspicions will be rare. Moreover, even if the person has standing to approach a court, it would be impossible to ascertain for certain whether the surveillance had occurred without notifying the person.

27. The hope of such abstract challenges is a very thin thread on which to hang the right to privacy.

Comparative Law

28. R2K and PI conducted a study of a variety of countries. The majority of the countries studied require subject notification.[31] The countries vary in terms of the details of when notification is required, the standard for notification, and how the decision is made. But they share two characteristics:

    28.1. The subject must be notified either before or after the surveillance unless it will threaten the purpose of interception; and

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

29. These countries use a variety of methods and language to identify when a person

[31] R2K and PI FA at paras 44-49.

must be notified.[32] Some provide for a default duty to inform unless a specified condition is present. Some countries require the intervention of a court to justify not notifying the person. Some include timeframes, which vary widely from 30 days to five years.

30. The comparative legislation dispatches the argument that notification will undermine the purpose of surveillance – defeating crime. It plainly is possible to design a mechanism that appropriately balances the respective interests – protecting the investigation and providing an effective remedy.

31. Precisely how to balance those competing concerns is a matter that must ultimately be determined by the Legislature. That is why the High Court suspended the order of invalidity. The interim relief is merely one way of resolving the problem and does not bind Parliament to adopting the same solution.

32. The Minister of Police considers the position in Canada, Australia, New Zealand and the United Kingdom.[33] It is true that Australia and the United Kingdom do not, presently, require post-surveillance notification, while Canada and New Zealand do. There are other countries R2K and PI studied that also do not require notification.[34]

33. But it is not a requirement to rely on comparative law for every single country to have adopted a certain position. There will always be countries late to adopt a developing trend. The comparative exercise establishes that the majority of

[32] 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).

[33] Minister of Police Written Submissions at paras 46-52.

[34] R2K and PI FA at para 49.

comparable countries do require notification, and that there are many effective methods to <u>balance</u> privacy and fighting crime.

CONCLUSION

34. Without notification, the possibility of a remedy for violations of rights is extremely low. A person illegally placed under surveillance will not be able to test whether the surveillance was lawful unless they know they have been under surveillance. This not only leaves that individual without a remedy, it creates impunity within the system because the risk of abuses being identified and punished are slim. Notification is vital to protect individual rights, and to ensure accountability within the surveillance system.

IV THE DESIGNATED JUDGE

35. The designated judge is central to RICA's mechanism. She has the ultimate power to authorise the interception of communications. It is vital that she is adequately independent to perform that function.

36. R2K supports the findings and order of the High Court, and the Applicants' arguments in support of confirmation of that order. It advances four additional arguments in support of the High Court's order:

    36.1. Independence is central to the right to **privacy**;

    36.2. Inescapable **secrecy** enhances the need for independence;

    36.3. The requirement of **retirement** undermines independence; and

    36.4. **Comparative** practice and **international** law supports it.

RIGHT TO PRIVACY

37. The Applicants focus on the *Glenister* line of cases to make the constitutional case for independence.[35] That is good authority. But there is a stronger constitutional source: s 14.

38. This Court has repeatedly held that the limitation of privacy caused by a search authorised by a warrant is justifiable only if the warrant is issued by an independent

[35] Applicants' Written Submissions at paras 54-6.

judicial officer. In *Heath*,[36] *Thint*[37] and *Van der Merwe*[38] this Court held independence was central to a constitutional search warrant. In Langa CJ's words: "*The fact that the decision as to whether a warrant is to be issued is taken by an impartial and independent judicial officer has been recognised as an important consideration in determining the constitutionality of search powers.*"[39]

39. The independence of a warrant-issuing authority[40] is therefore a key element that justifies the limitation of the right to privacy. If the issuing authority is not independent of the executive, the limitation of privacy will seldom be justifiable.

SECRECY

40. The designated judge is required by RICA to operate largely in secret. There are two parts to the designated judge's operation that render it secret.

40.1. First, all the applications are, necessarily, determined in secret.[41]

---

[36] *South African Association of Personal Injury Lawyers v Heath and Others* [2000] ZACC 22; 2001 (1) SA 883; 2001 (1) BCLR 77 (CC) at para 34 (Chaskalson P (as he then was) held that the granting of a search warrant "*calls for the qualities and skills required for the performance of judicial functions – independence, the weighing up of information, the forming of an opinion based on information, and the giving of a decision on the basis of a consideration of relevant information.*" (my emphasis)).

[37] *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* [2008] ZACC 13; 2008 (2) SACR 421 (CC); 2009 (1) SA 1 (CC) at paras 82-83.

[38] *Minister of Safety and Security v Van der Merwe and Others* 2011 (5) SA 61 (CC) at para 36-8 (Mogoeng J (as he then was) pointed out that, while warrants served to combat crime, they "*inevitably interfere with the equally important constitutional rights of individuals who are targeted by these warrants.*" Ibid at para 35. The limitation is justified by various "*safeguards*" to "*ensure that the power to issue and execute warrants is exercised within the confines of the authorising legislation and the Constitution.*" Ibid at para 36. The first safeguard is "*the significance of vesting the authority to issue warrants in judicial officers*". Ibid at para 37. Citing *Thint* and *Heath*, he again noted that the judicial granting of warrants justifies the limitation of privacy because they "*possess qualities and skills essential for the proper exercise of this power, like independence and the ability to evaluate relevant information so as to make an informed decision.*" Ibid at para 38.)

[39] *Thint* (n 37) at para 82 (*This Court too has recognised that requiring a search warrant to be issued by a judicial officer is an important part of the protection of fundamental rights and, in particular, the right to privacy.*").

[40] The Constitutional Court has not held that the warrant issuing authority must be a judicial officer. But it has held that, if it is not a judge, the issuing authority must have similar characteristics of independence. See, for example, *Thint* (n 37) at para 84.

[41] RICA s 16(7).

40.2. Second, the reporting requirements on the designated judge are limited, and information about her operations is scarce.[42]

41. The inherent secrecy of the authorisation process heightens the need for independence of the designated judge. Structural mechanisms that are adequate to protect the independence of a court that operates openly, may be inadequate to secure the independence of a secret court.

42. The principle of *open justice* is central. This Court[43] and the Supreme Court of Appeal[44] have repeatedly endorsed the principle of open justice. Open court rooms are a powerful guarantee of fairness, but also of independence.

42.1. As Ponnan JA put it: "*The publicity of a trial usually serves as a guarantee that the matter will be determined independently and impartially. The glare of public scrutiny makes it far less likely that the courts will act unfairly.*"[45]

42.2. Or as Chief Justice Langa explained: "*The public is entitled to know exactly how the judiciary works and to be reassured that it always functions within the terms of the law and according to time-honoured standards of independence, integrity, impartiality and fairness.*"[46]

---

[42] R2K and PI's FA at paras 60-67. R2K and PI believe the limited reporting requirements and practice of the designated judge may well be unconstitutional, but accept that is not directly in issue in this application.

[43] *South African Broadcasting Corporation Limited v National Director of Public Prosecutions and Others* [2006] ZACC 15; 2007 (1) SA 523 (CC); *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services (Freedom of Expression Institute as Amicus Curiae) In re: Masetlha v President of the Republic of South Africa and Another* [2008] ZACC 6; 2008 (5) SA 31 (CC); *Shinga v The State and Another (Society of Advocates, Pietermaritzburg Bar as* Amicus Curiae*); O'Connell and Others v The State* [2007] ZACC 3; 2007 (4) SA 611 (CC). The principle derives from multiple constitutional rights, including the rights to freedom of expression, access to courts and access to information. It is also entrenched by the constitutional guarantees of judicial independence. Constitution ss 165 and 173.

[44] *City of Cape Town v South African National Roads Authority Limited and Others* [2015] ZASCA 58; 2015 (3) SA 386 (SCA); *Van Breda v Media 24 Limited and Others; National Director of Public Prosecutions v Media 24 Limited and Others* [2017] ZASCA 97; 2017 (2) SACR 491 (SCA).

[45] *City of Cape Town* (n 44) at para 17.

[46] *South African Broadcasting Corporation* (n 43) at para 32.

43. We insist on open court rooms because they ensure independence – and the perception of independence. Where judicial functions are performed in secret, the risk that they will not be performed independently is higher.

44. That requires even greater structural guarantees of independence. But while RICA demands secrecy, it secures less independence than an ordinary judge in an open courtroom. It requires direct executive appointment – with no involvement of the JSC – and term renewal at the Minister's discretion.

THE DANGER OF A RETIRED JUDGE

45. In addition to the obvious dangers of executive appointment and term-renewal, the designated judge must be a *retired* judge.[47] Combined with term renewal, that creates a clear financial incentive for the designated judge to seek re-appointment. Those financial incentives exist only because the judge is a retired judge.

46. Under the Judges' Remuneration and Conditions of Employment Act,[48] a judge who has been discharged from active service[49] continues to receive a salary[50] and a gratuity[51] calculated according to their active service salary and the length of their

[47] RICA s 1 defines the *"designated judge"* as *"any judge of a High Court discharged from active service under section 3(2) of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act 47 of 2001), or any retired judge, who is designated by the Minister to perform the functions of a designated judge for purposes of this Act"*

[48] Act 47 of 2001.

[49] RICA defines the "designated judge" to include both a *"retired judge"* and a judge discharged from active service. The Judges' Remuneration Act does not use the terminology "retirement", except with regard to judges who were governed by the Judges' Pension Act. While it permits what is in practice retirement, it does so under the rubric of discharge from active service. Whoever precisely the term *"retired judge"* in RICA is meant to cover, the same rules about payment for service after the end of active service seem to apply.

[50] Judges' Remuneration Act s 5.

[51] Judges' Remuneration Act s 6.

service.

47. Judges who have been discharged from active service are also required to continue to perform "service" for up to three months per year until they reach the age of 75.[52] "Service" would include appointment as the designated RICA judge.[53] If a retired judge does not perform those three months of service, their salary is reduced. They may voluntarily perform more than three months' service, for which they are paid at a rate determined by the executive.[54]

48. As a result, the longer a retired judge serves as the designated judge, the more money she will make. That plainly undermines independence. It creates a financial incentive to secure the renewal of the judge's term.

49. 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 merely be part of their case load. It would also not be the case if the retired RICA Judge's term was not subject to renewal. There would be no possibility of future enrichment as a result of renewal. It is the combination of term-renewal with the requirement of retirement that eliminates independence.

---

[52] Judges' Remuneration Act s 7(1).

[53] "*Service*" is defined to include "*service as a chairperson or a member of a body or institution established by or under any law; or (d) any other service which the Minister may request him or her to perform*".

[54] Judges' Remuneration Act s 7(2). In the case of service as the designated RICA judge, the rate would be determined by the President. Judges' Remuneration Act s 7(2)(b). While we were unable to find the specific rate determined for the designated judge.

INTERNATIONAL AND COMPARATIVE LAW

50. RICA falls far short of international best practice. While there is certainly no uniformity between states, most provide more independence to the equivalent of the designated judge for two reasons.

51. First, the need for independent authorization of surveillance is required by international human rights law.

    51.1. According to the Special Rapporteur: "*Legislation must stipulate that State surveillance of communications must only occur … exclusively under the supervision of an independent judicial authority.*'[55]

    51.2. And following the OHCHR: "*Surveillance measures … should be authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after they have been terminated.*"[56]

52. Second, R2K and PI conducted a survey of other states' practice concerning the independence of the bodies authorising surveillance.[57] Many states require surveillance to be approved by a sitting member of the judiciary. In some of these countries the executive – either the police or the prosecutor – must approach an ordinary court to authorise the surveillance. In many European civil-law countries, it is the investigating judge who performs the role. In other countries, the sitting judge is part of a panel of judges who performs this role.

53. None of the countries R2K and PI considered provide for a single, retired judge,

---

[55] Report of Special Rapporteur (n 23) at 81.

[56] United Nations High Commissioner for Human Rights *Privacy in the Digital Age 2018* (n 22) at para 39 (emphasis added, citation omitted).

[57] R2K and PI FA at paras 76-84.

subject to executive appointment and term renewal to determine surveillance applications. This comparative practice supports the conclusion that RICA is an outlier. It must be amended to afford the designated judge adequate independence.

IV CONCLUSION

54. The prohibition on **post-surveillance notification** is a violation of the rights to privacy, access to court, and to a constitutional remedy. It is contrary to international law. It is not necessary to protect the state's interest in fighting crime, as comparative experience demonstrates. The High Court's First Order should be upheld.

55. The **designated judge** lacks independence. Every time she grants an interception directive, she limits privacy. She is compelled to do so in secret. Yet she lacks the same independence as ordinary judges acting in the open. The fact that she is retired creates an unfortunate financial incentive that is inconsistent with independence. International and comparative law demand real independence. The High Court's Second Order should be upheld.

MICHAEL BISHOP

PATRICK WAINWRIGHT

Counsel for Right2Know Campaign

Chambers, Cape Town

12 February 2020

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

CCT 278/19

In the application of:

AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC	First Applicant
SOLE, STEPHEN PATRICK	Second Applicant

and

MINISTER OF JUSTICE AND CORRECTIONAL SERVICES	First Respondent
NINE OTHERS	Second to Tenth Respondents

and

THE RIGHT2KNOW CAMPAIGN	Second *Amicus Curiae*
PRIVACY INTERNATIONAL	Third *Amicus Curiae*

SECOND AMICUS CURIAE'S TABLE OF AUTHORITIES

<u>Legislation</u>

1. Judges' Remuneration and Conditions of Employment Act 47 of 2001.

2. Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002.

<u>Cases</u>

1. *Bernstein and Others v Bester NO and Others* [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (CC).

2. *City of Cape Town v South African National Roads Authority Limited and Others* [2015] ZASCA 58; 2015 (3) SA 386 (SCA).

3. *Doctors for Life International v Speaker of the National Assembly and Others* [2006] ZACC 11; 2006 (12) BCLR 1399 (CC); 2006 (6) SA 416 (CC).

4. *Fose v Minister of Safety and Security* 1997 (3) SA 786 (CC), 1997 (7) BCLR 851 (CC)

5. *Glenister v President of the Republic of South Africa and Others* [2011] ZACC 6; 2011 (3) SA 347 (CC).

6. *Government of the Republic of South Africa and Others v Grootboom and Others* [2000] ZACC 19; 2001 (1) SA 46 (CC).

7. *Government of the Republic of Zimbabwe v Fick and Others* [2013] ZACC 22; 2013 (5) SA 325 (CC); 2013 (10) BCLR 1103 (CC).

8. *Head of Department : Mpumalanga Department of Education and Another v Hoërskool Ermelo and Another* [2009] ZACC 32; 2010 (2) SA 415 (CC); 2010 (3) BCLR 177 (CC).

9. *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services (Freedom of Expression Institute as Amicus Curiae) In re: Masetlha v President of the Republic of South Africa and Another* [2008] ZACC 6; 2008 (5) SA 31 (CC).

10. *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit* NO *and Others* [2000] ZACC 12; 2001 (1) SA 545 (CC).

11. *Law Society of South Africa and Others v Minister for Transport and Another* [2010] ZACC 25; 2011 (1) SA 400 (CC); 2011 (2) BCLR 150 (CC).

12. *Minister of Safety and Security v Van der Merwe and Others* 2011 (5) SA 61 (CC).

13. *Motswagae and Others v Rustenburg Local Municipality and Another* [2013] ZACC 1; 2013 (3) BCLR 271 (CC); 2013 (2) SA 613 (CC).

14. *National Coalition for Gay and Lesbian Equality v Minister of Home Affairs & Others* 2000 (2) SA 1 (CC), 2000 (1) BCLR 39 (CC).

15. *NM and Others v Smith and Others* [2007] ZACC 6; 2007 (5) SA 250 (CC).

16. *President of the Republic of South Africa and Another v Modderklip Boerdery (Pty) Ltd* [2005] ZACC 5; 2005 (5) SA 3 (CC); 2005 (8) BCLR 786 (CC).

17. *Rail Commuters Action Group v Transnet Ltd t/a Metrorail* [2004] ZACC 20; 2005 (2) SA 359 (CC); 2005 (4) BCLR 301 (CC).

18. *Shinga v The State and Another (Society of Advocates, Pietermaritzburg Bar as* Amicus Curiae*); O'Connell and Others v The State* [2007] ZACC 3; 2007 (4) SA 611 (CC).

19. *South African Association of Personal Injury Lawyers v Heath and Others* [2000] ZACC 22; 2001 (1) SA 883; 2001 (1) BCLR 77 (CC).

20. *South African Broadcasting Corporation Limited v National Director of Public Prosecutions and Others* [2006] ZACC 15; 2007 (1) SA 523 (CC).

21. *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* [2008] ZACC 13; 2008 (2) SACR 421 (CC); 2009 (1) SA 1 (CC).

22. *Van Breda v Media 24 Limited and Others; National Director of Public Prosecutions v Media 24 Limited and Others* [2017] ZASCA 97; 2017 (2) SACR 491 (SCA).

International Treaties and Reports

1. *Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee,* U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016).

2. International Covenant of Civil and Political Rights

3. *Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age,* U.N. Doc. A/HRC/27/37 (30 June 2014).

4. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,* U.N. Doc. A/HRC/23/40 (17 April 2013)).

5. *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights* (2018) A/HRC/39/29.

6. UN Human Rights Committee (HRC) *General Comment no. 31, The Nature of the General Legal Obligation imposed on States Parties to the Covenant* (26 May 2004) CCPR/C/21/Rev.1/Add.13.

7. Universal Declaration of Human Rights

Foreign and International Cases

1. *Big Brother Watch & Others v United Kingdom* [2018] ECHR 722.

2. *Szabó and Vissy v Hungary* [2016] ECHR 579.

3. *Tele2 Sverige AB and C-698/15 Watson and Others* [2016] EUCJEU C-203/15.

4. *Zakharov v Russia* (2016) 63 EHRR 17.