IN THE HIGH COURT OF SOUTH AFRICA

GAUTENG DIVISION, PRETORIA

CASE NO: 25978/17

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 THE 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
MINISTER OF TELECOMMUNICATIONS AND POSTAL SERVICES	Eleventh Respondent

---

APPLICANTS' HEADS OF ARGUMENT

Table of Contents

OVERVIEW OF SUBMISSIONS

1 This application concerns the constitutionality of the regime for state surveillance of private communications between members of the South African public.

2 That regime is set out in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 ("RICA").

2.1 The default position under RICA is that the surveillance or interception of private communications is prohibited.

2.2 However, RICA then goes on to make express and wide-ranging provision for state agents to engage in the surveillance or interception of private communications, provided certain requirements are met. For example, where a state agent obtains an interception direction under RICA, this allows him or her to listen to and record private conversations and meetings and to read and retain emails and text messages.[1]

2.3 It is important to note that the applicants do not contend – and have at no stage contended – that state surveillance of private communications is inherently unconstitutional. Rather the applicants accept that state surveillance can serve legitimate and important purposes and is at times necessary.

---

[1] FA p 24 para 28.1

2.4 The question, however, is whether RICA allows for and regulates state surveillance in a manner that is consistent with the provisions of the Constitution. If not, RICA is unconstitutional and Parliament must be directed to fix its constitutional flaws.

3 In what follows, we begin by demonstrating that RICA limits constitutional rights.

3.1 Most obviously and acutely, RICA limits the right to privacy guaranteed by section 14 of the Constitution. Indeed, there can be no serious debate on this score, as the joint respondents are rightly constrained to recognise.[2]

3.2 But the limitations of rights occasioned by RICA go further. Its provisions limit various other rights, including the right of access to courts in section 34 of the Constitution, to freedom of expression and the media in section 16 of the Constitution and to the right of legal privilege protected by sections 34 and 35 of the Constitution.

4 The real debate before this Court is whether such limitations of fundamental rights are permissible, having regard to the requirements of section 36 of the Constitution. As we demonstrate, in a series of respects the limitations are not permissible.

4.1 Instead, there are available a range of "less restrictive means" that can be used to properly balance the legitimate interests of the state in

[2] Joint AA p 763 para 48.1

pursuing surveillance when necessary, on the one hand, and the rights of members of the public, on the other hand.

4.2 The failure to make use of these less restrictive means, without any proper explanation, renders RICA unconstitutional in a series of respects.

5 As we explain below, surveillance is particularly invasive when the subject is a journalist or lawyer with duties to keep information or sources confidential. The second applicant, Mr Sam Sole, is an investigative journalist and managing partner of the first applicant, amaBhungane.[3] He was the subject of an interception direction.[4] amaBhungane and its managing partners have been involved in various strategic litigation cases involving the media and access to information over the last ten years.[5] They have grave concerns about the surveillance of journalists in particular. The applicants are supported by the South African National Editors' Forum ("SANEF"),[6] a non-profit organisation, which stands in defence of media freedom and represents the senior leadership of the majority of media publications in the country.[7]

6 But the surveillance of private communications in South Africa is now a matter of concern for <u>all</u> members of the public:

---

[3] FA p 10 para 1

[4] FA p 27 – 36 paras 35 – 63

[5] *Brümmer v Minister for Social Development and Others* 2009 (6) SA 323 (CC); *City of Cape Town v South African National Roads Authority Limited and Others* 2015 (3) SA 386 (SCA); *Nova Property Group Holdings v Cobbett* 2016 (4) SA 317 (SCA); *M&G Centre for Investigative Journalism NPC and Another v Minister of Defence and Military Veterans and Another* [2017] ZAGPPHC 195; *Maharaj and Others v Mandag Centre of Investigative Journalism NPC, M&G Media Limited and Stephan Patrick "Sam" Sole* 2018 (1) SA 471 (SCA)

[6] RA3 at p 1114

[7] RA3 at p 1115 paras 3 and 5

6.1 In 2016, the United Nations Human Rights Committee found that South Africa's surveillance regime suffered from various serious difficulties.[8] It expressed concerns about: (a) the relatively low threshold for conducting surveillance; (b) the relatively weak safeguards and oversight; (c) the lack of remedies against unlawful interference with the right to privacy; (d) the wide scope of data retention under RICA; (e) reports of unlawful mass interception.

6.2 After the United Nations report, a joint statement was released by 41 concerned civil society organisations calling for urgent review of RICA.[9]

6.3 The applicants' concerns are not speculative. Quite the opposite – they have set out evidence of several serious abuses of RICA.[10]

6.4 RICA fails to satisfy the minimum safeguards set out by the European Court of Human Rights.[11]

6.5 In these proceedings the joint respondents have admitted that they are conducting bulk/mass surveillance on members of the public[12] – the applicants submit that there is no statutory basis for them to do so.

7 We deal with the following topics in these heads of argument:

---

[8] FA p 85 – 89 paras 181 – 192

[9] FA p 89 para 194; it stated: "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."

[10] FA p 83 – 85 paras 176 – 180

[11] *Weber v Germany* (2008) 46 EHRR SE5, [2006] ECHR 1173, 54934/00

[12] Joint AA p 799 para 143

7.1 First, we provide an overview of the scheme of RICA;

7.2 Second, we explain that state surveillance of communications necessarily limits the right to privacy;

7.3 Third, we deal with the approach to limitation of rights required by the Constitution;

7.4 Fourth, we deal with each of the specific constitutional challenges that the applicants have brought; and

7.5 Lastly, we deal with costs and miscellaneous issues.

THE STATUTORY SCHEME OF RICA

8 RICA regulates the interception of private communications and communication-related information. The term 'communications' is defined broadly including phone calls, face-to-face conversations, sms text messages and emails.

9 Communication-related information, by contrast, is what is commonly referred to as 'meta-data'.[13] Academic commentators helpfully distinguish between the following three concepts:

9.1 the 'communication' or content of a message (i.e. the actual message: the audio recording of a phone conversation or content of a text message);

[13] Section 1 of RICA. 'Communication-related information' is defined somewhat cumbersomely in section 1 as 'any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system'.

9.2 the ‘meta-data’ (information about which telephone numbers were involved in a call, and where the telephone calls were made from);

9.3 ‘subscriber data’ (data regarding the owner of an account involved in a communication).[14]

10 The starting point is section 2 of RICA, which sets out a general prohibition of intercepting communications and meta-data. Contravening section 2 is an offence accompanied by severe penalties, including a fine up to R2 000 000 or up to 10 years imprisonment.[15]

The forms of surveillance permitted by RICA

11 RICA provides a legal framework for targeted surveillance — not general mass surveillance of the public. RICA makes provision for six substantive applications, each with its own requirements.[16] Applicants may apply for:

11.1 First, an interception direction of communications;[17]

11.2 Second, a real-time meta-data direction;[18]

11.3 Third, an archived meta-data direction;[19]

---

[14] Vian Bakir, ‘“Veillant Panoptic Assemblage”: Mutual Watching and Resistance to Mass Surveillance After Snowden’ (2015) 3(3) *Media and Communications* 12, cited in Admire Mare with contributions by Jane Duncan, ‘An Analysis of the Communications Surveillance Legislative Framework in South Africa’ (Report, Media Policy and Democracy Project, November 2015) 21 <www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf>

[15] Section 49(1) read with section 51(1)(b)(i) of RICA

[16] Sections 16–19, 21–22 of RICA

[17] Section 16 of RICA

[18] Section 17 of RICA

[19] Section 19 of RICA

11.4 Fourth, a combined application for meta-data as well as an interception direction.[20] For convenience, two different kinds of applications, in relation to the same subject, may be brought as a combined legal process.

11.5 Fifth, an entry warrant, which enables an interception device to be installed on the premises.[21] An entry warrant may only be issued if the designated judge (a retired judge) is satisfied that, first, entry of the premises concerned is necessary for a purpose referred to in the definition of entry warrant and, secondly, that there are reasonable grounds to believe that the interception of communication — under the direction concerned — would be impracticable without the installation of an interception device on the premises.

11.6 Sixth, a decryption direction,[22] which is essentially an instruction to a communications provider to assist with the decryption of encrypted information.[23]

12 Sections 16(2), 17(2), 21(2) and 22(2) of RICA stipulate the required format and content of applications. The requirements have slight variations particular to each kind of application.

---

[20] Section 18 of RICA

[21] Section 22 of RICA

[22] Section 21 of RICA

[23] Section 21(4)(a) of RICA; the designated judge may issue a decryption direction if there are reasonable grounds to believe that the communication contains encrypted information, which cannot be accessed in an intelligible form, and which is essential to the purpose of the interception.

13 The general position is that the designated judge will only grant an interception direction following an application in writing. The applications must also contain relevant detail including, for example, the identity of the law enforcement officer, the identity of the person being intercepted, all supporting allegations regarding where and why interception is necessary and the period for which the direction is required.

14 The designated judge must be satisfied that there are reasonable grounds to believe that one of the grounds outlined in section 16(5)(a) exists (see below) and that there are reasonable grounds to believe that granting the interception direction will result in the interception of communications concerning the particular ground.[24]

15 The applicant must include a basis to support the belief that the interception applied for will result in obtaining evidence.[25] The applicant must also indicate whether other investigative procedures have been applied and failed to produce the required evidence and why other investigative means are unlikely to succeed or appear to be too dangerous.[26]

16 The grounds on which an interception direction may be issued are set out in section 16(5) of RICA. There must be reasonable grounds to believe that:

16.1 a serious offence (which is a defined term under RICA) has been, is being, or will likely be committed;[27]

---

[24] Section 16(5)(b)(i) of RICA

[25] Section 16(2)(d)(ii) of RICA

[26] Section 16(2)(e) of RICA

[27] Section 16(5)(i) of RICA. The term 'serious offence' is defined in section 1 of RICA to mean—

16.2 it is necessary to gather information concerning an actual threat to the public health or safety, national security or compelling national economic interests;[28]

16.3 it is necessary to gather information concerning a potential threat to the public health or safety, national security or compelling national economic interests;[29]

16.4 providing any assistance in the form of interception of communications relating to organised crime or terrorism-related offences is in the interests of international relations or obligations;[30] or

16.5 it is necessary to gather information concerning property that could be the instrumentality of a serious offence, or the proceeds of unlawful activity.[31]

(a) any offence mentioned in the Schedule to RICA (which lists various offences including: high treason; any offence which could result in the loss of, or serious risk to, a person's life; any offence relating to the illicit dealing in or possession of precious metals or precious stones; or any offence where the punishment may be imprisonment for life or a period of imprisonment exceeding five years without the option of a fine); or
(b) any 'offence that is allegedly being or has allegedly been or will probably be committed by a person, group of persons or syndicate—
    (i) acting in an organised fashion which includes the planned, ongoing, continuous or repeated participation, involvement or engagement in at least two incidents of criminal or unlawful conduct that has the same or similar intents, results, accomplices, victims or methods of commission, or otherwise are related by distinguishing characteristics;
    (ii) acting in the execution or furtherance of a common purpose or conspiracy; or
    (iii) which could result in substantial financial gain for the person, group of persons or syndicate committing the offence, including any conspiracy, incitement or attempt to commit any of the abovementioned offences.'

[28] Section 16(5)(ii) of RICA

[29] Section 16(5)(iii) of RICA

[30] Section 16(5)(iv) of RICA

[31] Section 16(5)(v) of RICA

17 RICA places restrictions on which state entities may bring applications on each of the grounds above.[32] These restrictions are not applicable for applications for the issue of an entry warrant or a decryption direction.

18 Of particular relevance for the applicants' case is that section 16(7) of RICA mandates that the designated judge *must* consider an application and issue an interception direction *without providing notice to the party to whom the application applies.* It is mandatory, irrespective of the circumstances, under RICA that the subject is not notified prior to the granting of the application.

19 The imperative in section 16(7) prohibiting notice, applies to every form of application under RICA: to the issuing of an entry warrant,[33] a direction in respect of real-time[34] and archived meta-data,[35] as well as combined applications under section 18,[36] decryption directions[37] and any amendments or extensions.[38]

---

[32] Section 16(3) of RICA. For example, where the grounds stated in an application are that a serious offence has, is or will likely be committed, RICA stipulates (section 16(3)(b)) that the applicant must either be an officer in the South African Police Service, acting with approval from a senior officer (as defined in section 1(a) of RICA) or be the Head of Directorate or authorised Investigating Director (section 1(b) of RICA) or be a member of the Directorate with written approval from the Executive Director (section 1(c) of RICA).

Where the grounds are that gathering information relating to organised crime or terrorism-related offices is in the interests of international obligations (under section 16(5)(a)(iii) of RICA) the application may only be brought by a member of the Intelligence Services, who is or who has obtained authority from an Agency member at the level of at least General Manager.

[33] Section 22(7) – except for section 16(3) – of RICA

[34] Section 17(6) of RICA

[35] Section 19(6) of RICA

[36] Section 18(3) of RICA

[37] Section 21(6) – except for section 16(3) – of RICA

[38] Section 20(6) of RICA

20 RICA also permits the interception of communications in two emergency scenarios. The emergency surveillance procedures may be divided into two categories.

20.1 The first category accommodates scenarios in which an application may be made orally. Section 23 of the Act permits an oral application to be made where it is not reasonably practicable to make a written application because of the urgent need to intercept the communication. The applicant must be of the opinion — and the designated judge must be persuaded — that a written application is not reasonably practical, having regard to the urgency of the case or the existence of exceptional circumstances.[39]

20.2 The second category of emergency surveillance provides for exceptional scenarios in which the police may proceed to intercept communications *without any prior authorisation* from the designated judge. These include, for instance, where a law enforcement officer has reasonable grounds to believe that a party to the communication has caused, or may cause bodily harm to another person,[40] or has threatened to take his or her own life.[41] Where this is so, the police must notify the designated judge as soon as is practicable following the

[39] Applications under section 19(1) of RICA for archived meta-data are not listed under section 23. The likely reason that is so is that, if a law enforcement officer is only applying for archived meta-data, then they will apply to any High Court judge or magistrate rather than to the designated judge. But combination applications under section 18, which include an application for archived meta-data as one of the applications, may be made orally to the designated judge.

[40] Section 7(a)(i) of RICA

[41] Section 7(a)(iii) of RICA

fulfilment of any other conditions stipulated in RICA,[42] such as furnishing the telecommunications provider concerned with a written confirmation of the request.[43]

The safeguards under RICA

21 RICA includes some safeguards:

21.1 First, there is a degree of administrative oversight by the designated judge under the Act – who is a judge retired from active service – and who must be satisfied that there are reasonable grounds to believe that the surveillance order is necessary to gather information in relation to various trigger events set out above.

21.2 Second, there must be reasonable grounds that the information sought *will actually be obtained* by the interception.

21.3 Third, other investigative procedures must have been attempted and failed to produce the required evidence (or would be unlikely to succeed if applied).

21.4 Fourth, the orders are only granted for a period of three months at a time.

22 The applicants contend, however, that these safeguards are insufficient to justify the significant infringement of four fundamental rights: the rights to privacy, freedom of expression and access to courts, and legal professional

[42] Sections 7(4) and 8(4)(b) of RICA

[43] Section 8(4)(a) of RICA

privilege.

SURVEILLANCE LIMITS THE RIGHT TO PRIVACY

23 As is now trite, the courts apply a two-stage test in order to determine whether legislation is constitutionally invalid.[44]

23.1 The first question is whether the impugned provisions limit any of the rights in the Bill of Rights.[45]

23.2 If so, the second question is whether the limitation can be justified in terms of section 36 of the Constitution, that is whether it is reasonable and justifiable in an open and democratic society, having regard to the factors specified in section 36.

24 In the present case, the applicants rely on four different constitutional rights:

24.1 The right to privacy in section 14 of the Constitution;

24.2 The right of access to courts in section 34 of the Constitution;

24.3 The right to freedom of expression and the media in section 16 of the Constitution; and

24.4 The right of legal privilege protected by sections 34 and 35 of the Constitution.

---

[44] *Johncom Media Investments Limited v M and Others* 2009 (4) SA 7 (CC) at para 22

[45] *Coetzee v Government of the Republic of South Africa; Matiso & Others v Commanding Officer, Port Elizabeth Prison & Others* 1995 (4) SA 631 (CC) at para 9. *Coetzee* was decided under the interim Constitution, but the same approach is applied under the final Constitution.

25 We deal with the content of the last three of these rights further on in these heads, because they relate to particular challenges brought by the applicants.

26 However, the applicants' reliance on the right to privacy is relevant to the entire application. It is therefore appropriate to deal with it up front.

27 Section 14 of the Constitution guarantees everyone the right to privacy, including the right not to have their person or home searched, their property searched, their possessions seized, or the privacy of their communications infringed. The joint respondents are rightly constrained to recognise that this is the case.

28 That this is so is made both by the jurisprudence of our courts and that of foreign and international courts.

The position under our law

29 The Constitutional Court has found that the right to privacy is a significant right in a constitutional democracy and that there is a close link between the right to privacy and dignity in section 10 of the Constitution[46], which bolsters the right to privacy even further.[47] Privacy fosters dignity insofar as it protects an individual's entitlement to a sphere of private intimacy and autonomy.[48] Indeed, the Court has found that no sharp lines can be drawn between reputation,

---

[46] *Khumalo v Holomisa* 2002 (5) SA 401 (CC)

[47] *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* 2001 (1) SA 545 (CC) at para 18; *Thint (Pty) Ltd v NDPP* 2009 (1) SA 1 (CC) at para 77

[48] *Teddy Bear Clinic for Abused Children and Another v Minister of Justice and Constitutional Development and Another 2014 (2) SA 168 (CC)* at para 64

dignitas and privacy in giving effect to the value of human dignity in our Constitution.[49]

30 The scope of a person's privacy only extends to these aspects in relation to which a legitimate expectation of privacy can be harboured.[50] Ackerman J went on to say:

> *"A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individuals' activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation."*[51]

31 Importantly, the right to privacy extends beyond simply the inner sanctum of the home.[52] In *Magajane*, the Constitutional Court helpfully described it as "*what can be seen as a series of concentric circles ranging from the core most protected realms of privacy to the outer rings that would yield more readily to the rights of other citizens and the public interest*".[53]

32 The invasion of the right to privacy may take two forms: (i) an unlawful intrusion upon the personal privacy of another and (ii) the unlawful disclosure of private facts about a person.[54] The applicants submit that RICA occasions both forms of invasion.

---

[49] *Khumalo v Holomisa* at para 27

[50] *Bernstein and others v Bester and others NNO* 1996 (2) SA 751 (CC) at para 75

[51] *Bernstein v Bester* at para 77

[52] *Magajane v Chairperson, North West Gambling Board* 2006 (5) SA 250 (CC)

[53] *Magajane* at para 42

[54] *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* 1993 (2) SA 451 (A) at 462E – F

33 In *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another*[55] the Appellate Division held that telephone-tapping amounted to an unlawful intrusion into privacy:

> *"the telephone-tapping which occurred was manifestly an unlawful invasion of the privacy of Sage and its corporate executives and appellants did not seek to justify the tapping; nor is there any acceptable evidence on record which would possibly provide such justification."*[56]

34 That is virtually the same conduct being undertaken under RICA in terms of an interception direction. It follows that the act of interception is clearly an intrusion into privacy – that is, a limitation of the right to privacy. That is undoubtedly why Parliament has seen fit to include section 2 in RICA, which prohibits interception as a general rule.

35 The right to privacy covers certain private facts about which there is a legitimate expectation of privacy. Generally, the enquiry involves two questions.[57] First, there must at least be a subjective expectation of privacy. Second, the expectation must be recognised as reasonable by society.

36 Private facts have been held to include:

36.1 Information about a person's health or medical treatment. In *NM and Others v Smith*[58] the Constitutional Court held that an individual's HIV status was a private fact and, particularly within the South African context, deserved protection against indiscriminate disclosure, due to

---

[55] Ibid

[56] Ibid at 463B – C

[57] *Bernstein v Bester* at para 76

[58] *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae)* 2007 (7) BCLR 751 (CC)

the nature and negative social context of the disease, as well as the potential intolerance and discrimination that resulted from such a disclosure.[59]

36.2 Information about sexual orientation or sexual preferences. In *National Coalition for Gay and Lesbian Equality v Minister of Justice*[60] the inner sanctum of privacy was defined as including a person's family life, sexual preference, home environment. As a person moves into communal relations and activities such as business the scope of privacy shrinks.[61]

36.3 In *Case v Minister of Safety and Security,*[62] which dealt with the prohibition on the possession of pornography, Didcott J stated:

> *"What erotic material I may choose to keep within the privacy of my home, and only for my personal use there, is nobody's business but mine. It is certainly not the business of society or the State."*

36.4 Private financial information and sensitive business information of natural or juristic persons.[63] In *Financial Mail v Sage Holdings* the newspaper was interdicted from publishing private facts arising from a *"[s]trictly private and confidential"* internal company memorandum with

---

[59] See also *Tshabalala-Msimang and Another v Makhanya and Others* 2008 (3) BCLR 338 (W)

[60] *National Coalition for Gay and Lesbian Equality v Minister Of Justice* 1999 (1) SA 6 (CC) at para 31

[61] Ibid

[62] *Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others* 1996 (3) SA 617 (CC) at para 91

[63] See *Bernstein* at para 85 – though the company's right to privacy is certainly less expansive than a private individual it is still possible for a corporate entity to assert its right to privacy in certain instances. See, further, in *Tulip Diamonds FZE v Minister for Justice and Constitutional Development and Others* 2013 (10) BCLR 1180 (CC) while the Constitutional Court held that Tulip's belated reliance on privacy could not be entertained and that the privacy rights of juristic persons are not as "*intense as those of human beings*", the court did not find that juristic persons could never have claims to privacy rights.

restricted circulation, and unlawfully obtained tape recordings of telephone conversations between directors of the company and third parties. The Financial Mail had, however, not been party to the unlawful interception of the company's telephone calls.

36.5 Other communications that are private or confidential by their nature. We submit, and explain fully below, that the contents of private correspondence including communications with lawyers, or communications with journalists would fall into this category.

37 As the Constitutional Court explained recently, in upholding a challenge to the criminalisation of the private use of marijuana, "*it can legitimately be said that the right to privacy is a right to be left alone*".[64]

38 Understood in this way, there can be no question that having a state agent listen to a private person's calls, read their emails and so on limits the right to privacy.

38.1 This is especially because even if the state agent is seeking only, for example, conversations and correspondence about criminal conduct, the manner in which surveillance occurs under RICA will include interception of communications that have nothing to do with criminal conduct at all.

---

[64] *Minister of Justice and Constitutional Development and Others v Prince (Clarke and Others Intervening); National Director of Public Prosecutions and Others v Rubin; National Director of Public Prosecutions and Others v Acton* 2018 (6) SA 393 (CC) at para 45

38.2 Many of these will touch personal aspects of a person's life: listening to recordings of personal conversations with a spouse, reading private text messages between a person and a friend and tracking what websites they have been visiting.

38.3 The subject could be disclosing private information related to their sexual orientation or health status, phoning a journalist to disclose evidence of corruption or even speaking to a friend – who has nothing to do with the surveillance order – as they disclose extremely private details of their life. It is information that clearly carries a reasonable expectation of privacy.

38.4 There may well be information in the communications that is not known to the public, or even to their spouse or family.

39 There can thus be no doubt that the interception of such communications involves a limitation of privacy.

40 The various cases in the Constitutional Court dealing with warrants for search and seizures are also instructive on this score. Interception directions (or real-time communication-related directions etc.) under RICA are essentially no more than warrants to perform the particular form of surveillance.

40.1 In *Mistry*, the Constitutional Court emphasised the sanctity of the right to privacy and held that the existence of safeguards to regulate the way that state officials may enter the private domains of ordinary citizens is

one of the features that distinguishes a constitutional democracy from a police state.[65]

40.2 In *Gaertner*, the Court held that "*the right to privacy embraces the right to be free from intrusions and interference by the state and others in one's personal life*".[66]

40.3 In *Magajane,* the Court held that all statutorily authorised inspections limit the constitutional right to privacy.[67] The Court further explained that:

> *"The notion that an inspection constitutes an intrusion, albeit a less invasive one, invoking the right to privacy is consistent with our constitutional notion of concentric circles of the privacy right. Additionally, it would be undesirable to impose at the threshold inquiry an arbitrary demarcation line between degrees of intrusion that would invoke the constitutional right to privacy. Such line drawing would have the negative effect of placing certain administrative inspections beyond the reach of judicial review. I therefore conclude that section 65(1) limits the right to privacy entrenched in section 14 of the Constitution. It is now necessary to consider whether the limitation passes constitutional muster."*[68]

40.4 The Constitutional Court further held:

> *"A court has to consider an applicant's expectation of privacy and the breadth of the legislation, among other considerations. The expectation of privacy will be more attenuated the more the business is public, closely regulated and potentially hazardous to the public. Legislation may not be so broad as to have the real potential to reach into private homes."*[69]

---

[65] *Mistry v Interim National Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC) at para 25; cited in *Minister of Police and Others v Kunjana* 2016 (2) SACR 473 (CC) at para 18

[66] *Gaertner and Others v Minister of Finance and Others* 2014 (1) SA 442 (CC) at para 47

[67] *Magajane* at para 59

[68] *Magajane* at para 59

[69] *Magajane* at para 50

40.5 Again, we emphasise that RICA permits the state not only to reach into a private home but enables the state to access extremely private information that a person might only have disclosed with select trusted persons.

41 These arguments apply with equal, if not greater force, to RICA.

42 First, RICA draws no distinction between surveillance of private or business communications. There are no mechanisms in place for sorting through private communications with a spouse, obviously private photographs, legally privileged communications or messages that disclose that secret meetings have taken place with a journalist or confidential source.

43 Second, where searched premises included private homes the Constitutional Court held that expectation of privacy is greater as it is part of the “inner sanctum” of a person. We submit that even in the context of a private home there are spaces that might generally be visited by members of the public and more private spaces where confidential documents are kept. But an interception direction under RICA empowers the state to have complete access to all of a person’s calls on their private cellular phone – regardless of whether those calls have anything to do with the basis for the interception direction.

44 Third, RICA has no mechanism for protecting the rights of third parties that feature in the communications. The *Gaertner* Court found the wording '*any premises*' and '*any premises whatsoever*' so broad that it brought within its sweep not only the places of business and homes of people who are players in the customs and excise industry, but also the homes of their clients, associates,

service providers, and employees, their relatives, and anyone who may be linked to a player in the customs and excise industry.[70] The same is so with interception directions. It is an infringement of all persons who have communicated with the target. If one takes Mr Sole's communications as an example – during the period of the surveillance there may well have been numerous other calls with confidential sources regarding various other investigations that he was conducting. The participants to those calls plainly had a reasonable expectation of privacy.

The collection and examination of meta-data is no different

45 There is a suggestion in the respondents' papers that collecting and examining "*meta-data*" is a less invasive form of surveillance.[71] The applicants' papers make it clear that this contention is without merit.

46 Meta-data is different from the "content" of a message or call (the actual text of the message or the actual audio recording of a voice call). Rather, this is information about a message or voice call. For example, who sent the message to whom and when, or who made and received the call, as well as where the message was sent or a voice call was made. It also includes "subscriber data" (data regarding the owner of an account involved in a communication).

47 But this does not alter the fact that the collection and analysis of meta-data involves a limitation of the right to privacy.

---

[70] *Gaertner* at para 38
[71] 1st respondent's AA p 942 para 35

48 Being provided with meta-data of a person's communications is incredibly invasive. An analysis of meta-data provides almost a complete picture regarding:[72]

48.1 that person's movements and whereabouts at any given time;

48.2 who they are contacting; and

48.3 when they are doing so.

49 The applicants provide a detailed technical account in the papers of how this occurs. In effect cellular phones broadcast a constant stream of information about their users' locations and activities.[73]

50 Thus meta-data can expose an individual's:[74]

50.1 Social circles;

50.2 Intimate relationships;

50.3 Routines;

50.4 Religious beliefs (depending on how often they visit a religious institution); as well as

50.5 Interactions with protected sources or confidential clients.

51 Accordingly, we submit that there is simply no basis for the contention that accessing and storing a person's meta-data record is not invasive.

---

[72] RA p 1004 para 56

[73] RA p 1005 – 1006 para 59

[74] RA p 1009 para 66

The position in international and foreign law

52 That surveillance limits the right to privacy is also made clear from an analysis of international law and foreign law.

53 South Africa in a member country of the United Nations, and any resolutions taken by the General Assembly, have binding force on it.

54 Resolution No. 68/167 on the Right to Privacy in the Digital Age, adopted by the United Nations General Assembly on 18 December 2013, reads as follows:

> *"4. Calls upon all States:*
> *(a) To respect and protect the right to privacy, including in the context of digital communication;*
> *(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;*
> *(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;*
> *(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data".*

55 The European Court of Human Rights has found that telephony, facsimile and e-mail are covered by notions of *private life* and *correspondence* pursuant to Article 8.[75] And that the sphere of privacy under the European Convention is not to be narrowly construed. Rather it may extend to both professional and business activities when the case concerns protection against arbitrary interferences by public authorities.[76]

---

[75] *Liberty and others v the United Kingdom*, application no. 58243/00 at paras 69-70

[76] *Niemietz v. Germany*, application no. 13710/88 at paras 29-32

56 In *Malone v the United Kingdom*[77] – a case decided in 1984 – the European Court found that the Secretary of State issuing a warrant to intercept telephone conversations was unlawful because there was no sufficient regulatory system to supervise this form of warrants. Importantly, for present purposes, the Court held that the interception was an interference by a public authority with the right to privacy under the European Convention. Moreover, the Court emphasised that the requirement that limitations of rights occur in "accordance with law" was not an exercise that merely examined whether any domestic law on the subject existed – but a normative enquiry evaluating the quality of the law and whether it provided sufficient protection to citizens.

57 In *Weber v Germany,* the Government conceded that the impugned provisions, which permitted the monitoring of telecommunications and the use of data obtained from it, interfered with the secrecy of telecommunications protected by Article 8 of the European Convention. The European Court of Human Rights reiterated that:

57.1 Telephone conversations are covered by the notions of "private life" and "correspondence" under Article 8.[78]

57.2 The mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the

[77] *Malone v the United Kingdom* (1984) 7 EHRR 14, [1984] ECHR 10

[78] *Weber v Germany* at para 77. See also – *Klass and Others v Germany* (ECHR) application no. 5029/71; *Malone v the United Kingdom*)

telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.[79]

57.3 Thus, insofar as the provisions authorised the interception of telecommunications, they interfered with the right to respect for private life and correspondence.[80]

57.4 The European Court found, further, that "the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8".[81]

58 The Court has been consistent in its approach that the surveillance regimes limit the right to privacy and that the crux of the analysis turns on whether the provisions satisfy the European Convention's limitations analysis. Two recent decisions in this regard are *Zakharov v Russia*[82] and *Centrum för Rättvisa v Sweden*,[83] in which the Court recognised that while states generally enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security – the discretion afforded to them in operating an interception regime must necessarily be narrower.

---

[79] *Weber v Germany* at para 78

[80] *Weber v Germany* at para 78

[81] *Weber v Germany* at para 79

[82] *Zakharov v Russia* (2016) 63 E.H.R.R. 17

[83] *Centrum för Rättvisa v Sweden* (2019) 68 E.H.R.R. 2

THE APPROACH TO THE LIMITATIONS ANALYSIS

59 Once the limitation of the right has been established, the question is whether that limitation is justified in terms of the limitations clause. Once an applicant has demonstrated that legislative provisions limit constitutional rights, the onus shifts to the government to show that the limitations are justifiable under section 36.[84]

60 Section 36 (1) provides:

> *"The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including –*
> *(a) the nature of the right;*
> *(b) the importance of the purpose of the limitation;*
> *(c) the nature and extent of the limitation;*
> *(d) the relation between the limitation and its purpose; and*
> *(e) less restrictive means to achieve the purpose."*

61 The first requirement is that rights may only be limited by a law of general application. Thereafter, the court will consider all relevant factors (including those set out in paragraphs (a) to (e) in section 36) to determine whether the limitation is reasonable and justifiable. This second stage involves a proportionality analysis.[85]

62 The core question is whether the law strikes an appropriate balance between the purpose it seeks to achieve (combatting crime, for instance), on the one

---

[84] *Moise v Greater Germiston Transitional Local Council: Minister of Justice and Constitutional Development Intervening (Women's Legal Centre as Amicus Curiae)* 2001 (4) SA 491 (CC) at para 31; *Minister of Home Affairs v National Institute for Crime Prevention and the Reintegration of Offenders (NICRO) and Others* 2005 (3) SA 280 (CC) at paras 33-7; *Phillips and Another v Director of Public Prosecutions, Witwatersrand Local Division, and Others* 2003 (3) SA 345 (CC) at para 20

[85] *Johncom* at para 24

hand, and the right that is being limited, on the other (for example, the right to privacy, or freedom of expression).[86]

63 Where the limitations analysis "*rests on factual or policy considerations, the party seeking to justify the impugned law – usually the organ of state responsible for its administration – must put material regarding such considerations before the court*."[87]

64 As regards RICA's purpose, the South African government stated in its reply to issues, submitted as part of the International Covenant on Civil and Political Rights reporting process to the Human Rights Committee, that the purpose of RICA is:

> *"to provide for a mechanism to investigate and combat serious crimes which are planned, facilitated or executed through the use of electronic communications. Most constitutional democracies followed this route in order to investigate crime."*[88]

65 The long title of RICA sets out the following purposes:

> *"To regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information; to regulate the making of applications for, and the issuing of, directions authorising the interception of communications and the provision of communication-related information under certain circumstances; to regulate the execution of directions and entry warrants by law enforcement officers and the assistance to be given by postal service providers, telecommunication service providers and decryption key holders in the execution of such directions and entry warrants; to prohibit the provision of telecommunication services which do not have the capability to be intercepted; to provide for certain costs to be borne by certain telecommunication service providers; to provide for the establishment of interception centres, the Office for Interception*

---

[86] Ibid

[87] *Teddy Bear Clinic* at para 84

[88] South Africa's Further Written Responses to United Nations Human Rights Committee; annexure in respect of Issue No. 26 at 6 (available at: http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/ZAF/INT_CCPR_AIS_ZAF_23518_E.pdf)

Centres and the Internet Service Providers Assistance Fund; to prohibit the manufacturing, assembling, possessing, selling, purchasing or advertising of certain equipment; to create offences and to prescribe penalties for such offences; and to provide for matters connected therewith."

66 The applicants accept that the purpose is, generally, legitimate. However, at the same time, the rights discussed are all of fundamental importance and the limitations are significant (factors (a) and (c) in section 36(1) of the Constitution).

67 As is often the case in limitations analyses,[89] the focus then turns to factors (d) and (e) – the relation between the limitation and its purpose and less restrictive means to achieve the purpose.

68 In this regard we demonstrate below that the impugned provisions of RICA fall short of the limitations clause for two reasons:

68.1 First, the provisions are not rationally related to the purposes they seek to achieve. This enquiry evaluates the logical relationship between the purpose sought to be achieved by the provision and the means used.[90] The aim of the evaluation is not to determine whether some means will achieve the purpose better, only whether the selected measures could rationally achieve the same end.[91]

68.2 Second, there are less restrictive means available to achieve the same purposes. The Constitutional Court has made very clear that where a

---

[89] See, for instance, *Teddy Bear Clinic.*

[90] *Minister of Safety and Security v South African Hunters and Game Conservation Association* 2018 (2) SACR 164 (CC) at para 14

[91] Ibid

right is being limited, if there are less-restrictive means available by which the same end could be achieved, these less-restrictive means must be used. A statute is overbroad if, amongst other things, the extent of its invasion of fundamental rights is substantially disproportionate to its public purpose.[92] The Constitutional Court famously stated that a sledgehammer must not be used to crack a nut.[93] A provision which infringes constitutional rights must be "*appropriately tailored*" and "*narrowly focused*". [94]

THE FIRST CHALLENGE – FAILURE TO NOTIFY THE SUBJECT OF INTERCEPTION

69 It is mandatory under RICA that the subject of the surveillance is not notified prior to the granting of the application. Section 16(7)(a) of RICA provides:

> *"An application must be considered and an interception directive issued without any notice to the person or customer to whom the application applies and without hearing such person or customer."*

70 Section 16(7) applies, with necessary changes, to the issuing of an entry warrant,[95] a direction in respect of real-time[96] and archived meta-data,[97] as well as combined applications under section 18,[98] decryption directions[99] and any amendments or extensions.[100]

---

[92] *Mistry* at para 30

[93] *S v Manamela and Another (Director-General of Justice Intervening)* 2000 (3) SA 1 (CC) at para 34

[94] *Islamic Unity Convention v Independent Broadcasting Authority and Others* 2002 (4) SA 294 (CC) at para 51; *South African National Defence Union v Minister of Defence and Another* 1999 (4) SA 469 (CC) at para 18

[95] Section 22(7) – except for section 16(3) – of RICA

[96] Section 17(6) of RICA

[97] Section 19(6) of RICA

[98] Section 18(3) of RICA

71 The applicants submit that section 16(7) of RICA, and the other sections relying on it, are inconsistent with the Constitution and invalid for the following reasons.

71.1 They breach the rights of privacy and access to courts in terms of sections 14 and 34 of the Constitution; and

71.2 They impermissibly invert the constitutional principle of open justice – making blanket secrecy the default and effectively the permanent position.

72 Moreover, while administrative review may exist in principle, the subject of the surveillance may never find out that an order was even granted which renders this an entirely theoretical right.

Access to courts

73 For present purposes, the right to privacy must be understood together with the right of access to courts in section 34 of the Constitution.

74 Section 34 of the Constitution provides that:

> *"[e]veryone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum."*

75 There are a few key components captured in section 34. The decision-maker must be *independent*. The hearing must be *fair* (this captures notions of natural justice and, in particular, procedural fairness); and it must be *public*.

76 As we demonstrate below, RICA falls foul of each of these requirements.

---

[99] Section 21(6) of RICA — except for section 16(3)

[100] Section 20(6) of RICA

77 In relation to court hearings being public, in *R v Legal Aid Board, ex parte Kaim Todner (a firm)* Lord Woolf said:

> *"This is the reason it is so important not to forget why proceedings are required to be subjected to the full glare of a public hearing. It is necessary because the public nature of proceedings deters inappropriate behaviour on the part of the court. It also maintains the public's confidence in the administration of justice. It enables the public to know that justice is being administered impartially. It can result in evidence becoming available which would not become available if the proceedings were conducted behind closed doors or with one or more of the parties' or witnesses' identity concealed. It makes uninformed and inaccurate comment about the proceedings less likely. If secrecy is restricted to those situations where justice would be frustrated if the cloak of anonymity is not provided, this reduces the risk of the sanction of contempt having to be invoked, with the expense and the interference with the administration of justice which this can involve."*[101]

78 In *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services and another, In re: Masetlha v President of the Republic of South Africa and another*[102] the Constitutional Court dealt with an application for access to classified documents which formed part of an appeal record. The Constitutional Court confirmed that the default position is one of openness and disavowed an approach that proceeded from a position of secrecy, even in a case where the documents in question had been lawfully classified as confidential in the interest of national security.[103]

79 Secrecy must therefore be the exception, not the rule. The Supreme Court of Appeal recently underscored that without openness, the judiciary loses the legitimacy and independence it requires in order to perform its functions.[104]

---

[101] *R v Legal Aid Board, ex parte Kaim Todner (a firm)* [1998] 3 All ER 541 at 549J-550B

[102] *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services and Another, In re: Masetlha v President of the Republic of South Africa and Another* 2008 (5) SA 31 (CC)

[103] Ibid at paras 39 – 40

[104] *City of Cape Town v South African National Roads Authority Limited and Others* 2015 (3) SA 386 (SCA) at para 19

80 In *S v Shinga*,[105] the Constitutional Court considered the constitutionality of a law that allowed criminal appeals to be determined in chambers. It expressed alarm at the idea that court proceedings could, by default, be held in secret:

> *"The section makes dangerous inroads into our system of justice which ordinarily requires court proceedings that affect the rights of parties to be heard in public. It provides that an appeal can be determined by a judge behind closed doors. No member of the public will know what transpired; nobody can be present at the hearing. Far from having any merit, the provision is inimical to the rule of law, to the constitutional mandate of transparency and to justice itself. And the danger must not be underestimated. Closed court proceedings carry within them the seeds for serious potential damage to every pillar on which every constitutional democracy is based."*[106]

81 RICA is even more invasive. Section 16(7) significantly limits accountability and the right of access to courts as perpetual secrecy means that there is virtually no way to tell if there was an interception direction at all, or if the interception direction was correctly granted.

82 Accordingly, while a decision by the designated judge amounts to administrative action and is subject to the principle of legality – the subject is unable to review the decision because he or she will not even be informed under the Act that he or she was the subject of the interception or adequate particulars of the interception direction to review the decision.[107]

83 This is precisely what occurred in relation to the second applicant – Mr Sole. He only received confirmation that he had been surveilled when a transcript of his telephone calls was attached to court papers in another case.[108]

---

[105] *S v Shinga (Society of Advocates (Pietermaritzburg)) as Amicus Curiae), S v O'Connell and Others* 2007 (4) SA 611 (CC)

[106] *S v Shinga* at para 25

[107] FA p 40 para 73.5

[108] "SPS 12.1" to FA at p 156 – 163

84 We note too that the European Court of Human Rights in *Zakharov*[109] found that the Russian law regarding surveillance was insufficient because it did not provide:

84.1 An effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject (the same argument that some of the respondents sought to raise in this case).[110]

84.2 Effective remedies to a person who suspects that he or she has been subjected to secret surveillance. By depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law eschewed an important safeguard against the improper use of secret surveillance measures.[111]

Respondents' contentions on notification

85 The respondents contend that absolute and invariable secrecy is required – forever, regardless of the circumstances. However, this is with respect to miss the point.

86 For the purposes of this application the applicants accept that prohibiting pre-surveillance notification is a justifiable limitation of the rights involved. However, there is no justification for the blanket and invariable secrecy contended for by the respondents, after the surveillance has taken place.

---

[109] *Zakharov v Russia*

[110] *Zakharov v Russia* at para 298

[111] *Zakharov v Russia* at para 300

87 The joint respondents claim that notification of the subject would defeat the purpose of RICA since the subject might conduct communications in a manner that evades any interception direction and prevents the authorities from discovering the truth.[112] That may well be true in relation to notification before surveillance but it does not deal with notification after surveillance. In particular, the Joint Affidavit does nothing to rebut the applicants' arguments regarding post-surveillance notification.[113]

88 The Minister of Police accepts that there may be "*rogue elements*" within the SAPS who unlawfully intercept and monitor communications,[114] but argues that any evidence gathered outside RICA's constraints "*is tainted in legal proceedings*".[115]

88.1 But this too is to miss the point. The notion that evidence gathered in contravention of RICA will be excluded as evidence misconstrues the applicants' case.[116]

88.2 By the time that the interception has been done, the breach of rights and damage has already been done. If there was no legitimate basis for the interception in the first place there will never be any civil or criminal proceedings – where evidence might be interrogated.[117]

---

[112] RA p 761 – 762 paras 47.4 – 47.5

[113] RA p 993 para 26.1

[114] 5th respondent's AA p 940 para 31

[115] 5th respondent's AA p 940 para 31

[116] RA p 996 para 996

[117] Ibid

89 It is thus only the first respondent that seeks to deal with the true issue. He contends that post-surveillance notification is "*inimical to the efficacy of the interception of a communication*" because the investigation of criminal conduct is often an on-going process to which there is no definitive end-point. Alerting the subject may compromise the investigation that may flow from it.[118]

90 The first respondent also claims that if there is any limitation of the right of access to courts, it is reasonable and justifiable because:

90.1 If the subject comes to know of the surveillance he/she is free to approach a court for appropriate relief.[119]

90.2 The subject of the surveillance has the right to challenge the validity of the interception direction and the admissibility of evidence if criminal proceedings are instituted.[120]

90.3 The constitutionality of RICA must not be decided on the basis that some unscrupulous individual acting outside of the scope of legislation may abuse it or can abuse it.[121]

91 It must be noted that the first respondent's case is inherently speculative and cannot possibly justify the absolutist stance that post-surveillance notification is never permitted.

---

[118] 1st respondent's AA p 646 para 85

[119] 1st respondent's AA p 642 para 73

[120] 1st respondent's AA p 642 para 73

[121] 1st respondent's AA p 645 para 82

The limitation fails to meet the requirements under section 36

92 We therefore submit that the limitation fails to meet the requirements of section 36 for two reasons.

93 First, the limitation is not rationally connected to the purpose the provision seeks to achieve.

93.1 While depriving the subject of any knowledge of the surveillance directive may be argued to be rationally connected to a legitimate purpose (at least before and during the actual surveillance), it precludes notification of the subject even after the interception directive has lapsed, and even after any investigation has been concluded. In all of those instances, once the evidence has been gathered, the continued secrecy is not rationally linked to any legitimate purpose.

93.2 Even at a completely non-sensitive stage of an investigation the subject is completely unaware that she was at one stage under surveillance and whether the interception direction was granted lawfully, or at all.

94 Second, there are clearly less-restrictive means of achieving the purpose of intercepting communications, which better balance accountability and transparency. Secrecy should be the exception, not the rule. Making post-surveillance notification the default position, and any further secrecy the exception, accords with the principle of open justice.

95 The subject should be notified as a matter of course in each case, once the surveillance has run its course, and be provided with the record of the application for surveillance.

96 The only circumstances in which the subject should not receive post-notification surveillance is where, on the facts of that case, the state organ persuades the designated judge to depart from the default position of post-surveillance openness. Yet RICA contains no such provision or mechanism.

97 Various other jurisdictions have such systems in place, which require that the subject of the interception must be notified that there was such an order within a certain amount of days of the expiry of the order.

98 For example, section 196 (1) of the Criminal Code of Canada provides as follows:

> *"The Attorney General of the province in which an application under subsection 185(1) was made or the Minister of Public Safety and Emergency Preparedness if the application was made by or on behalf of that Minister shall, within 90 days after the period for which the authorization was given or renewed or within such other period as is fixed pursuant to subsection 185(3) or subsection (3) of this section, notify in writing the person who was the object of the interception pursuant to the authorization and shall, in a manner prescribed by regulations made by the Governor in Council, certify to the court that gave the authorization that the person has been so notified."*
> (Emphasis added)

99 Similarly, the Procedure for interception of wire, oral, or electronic communications in the United States (18 U.S. Code § 2518) states:

> *"8(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518 (7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—*
> *(1) the fact of the entry of the order or the application;*
> *(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and*
> *(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.*

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed."
(Emphasis added.)

100 Equally, in Japan the Act on Interception of Communications for Criminal Investigation requires that the subject is given notice of the interception within 30 days of the surveillance directive expiring.[122]

101 As regards notification of subjects of surveillance, *The International Principles on the Application of Human Rights to Communications Surveillance*,[123] also known as the "Necessary and Proportionate Principles" state:

"User notification

Those whose communications are being surveiled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation.

Delay in notification is only justified in the following circumstance:

1. Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life; and

2. Authorisation to delay notification is granted by a Competent Judicial Authority; and

3. The User affected is notified as soon as the risk is lifted as determined by a Competent Judicial Authority.

The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request."

---

[122] Dale McKinley "The surveillance state – communications surveillance and privacy in South Africa", March 2016, at 23 <http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf>

[123] "SPS 13" to FA at p 168 – 182; available at: https://necessaryandproportionate.org/principles

102 These principles, though not law, were put together (during 2012 and 2013) by a group of approximately 40 privacy and security experts. The ultimate product was a set of principles, which were launched at the UN Human Rights Council in Geneva in September 2013. These principles have been adopted by more than 400 organisations throughout the world.

103 There may be instances in which, exceptionally, the state is justified in delaying notifying the subject. As McKinley notes "*[w]here an on-going investigation might be compromised by such notice, a district court judge can extend the period of time within which the subject must be notified*."[124]

104 Thus, a practical less restrictive mechanism exists to achieve the purpose. There is no evidence that the integrity of investigations under RICA will be compromised by this mechanism. Where it is necessary to limit access to court records or court proceedings, the limitation must be as narrow as necessary to achieve the purpose.[125] We accept that in some instances notification may well need to be delayed. The issue in this case, however, is whether complete secrecy is required as an invariable and immutable feature, which permits of no qualification, regardless of the circumstances of each particular case. Post-surveillance notification should be the default rule, further secrecy the exception.

---

[124] Ibid

[125] *Independent Newspapers* at para 45; see also para 181 of Van der Westhuizen J's minority judgment: "*Even if it is shown that national security requires non-disclosure, it must be shown that the non-disclosure that is specifically being sought is the least restrictive method to achieve the purpose. A court will look favourably upon alternatives to full disclosure, or absolute non-disclosure, for example redaction of highly sensitive materials, or summaries of documents that allow the public to understand the substance if not the specifics of the material.*"

Conclusion on the first challenge

105 Importantly, the respondents have made out cases against pre-surveillance notification and post-surveillance notification – but none made out any case regarding post-surveillance notification with the possibility of motivating for a delay.

105.1 Where there are risks or an investigation is at a sensitive stage the state must demonstrate this to the designated judge.[126] The risks fall away – there would be no risk of publication if the subject had not yet been notified.[127]

105.2 If the state is unable to demonstrate than an investigation is sensitive then the state should not be permitted to rely on the exception.

105.3 Parliament might well decide that in some instances when the interception documents are provided to the subject of the surveillance, certain information could be redacted.[128]

106 There are plainly less restrictive means to achieve the purpose: a general rule of post-surveillance notification with the possibility of the state entities motivating to delay the notification. Notification should be the rule with secrecy being the exception.[129] In an exceptional case then the respondents should motivate why notification of the subject should be delayed.[130] All relevant facts

---

[126] RA p 995 para 31.1

[127] RA p 995 para 31.2

[128] RA p 995 para 31.2

[129] RA p 994 para 30

[130] RA p 994 para 30

should be pleaded and interrogated – not merely assumed on a blanket basis.[131] After an interception direction has expired the state must make out a strong case demonstrating why the subject should not be notified.[132]

107 Once that is so, the provision fails the limitations analysis in terms of section 36.

Remedy on the first challenge

108 This Court's remedial powers are set out in section 172(1) of the Constitution which provides:

> *"(1) When deciding a constitutional matter within its power, a court—*
>
> *(a) must declare that any law or conduct that is inconsistent with the Constitution is invalid to the extent of its inconsistency; and*
>
> *(b) may make any order that is just and equitable, including -*
>
> *(i) an order limiting the retrospective effect of the declaration of invalidity; and*
>
> *(ii) an order suspending the declaration of invalidity for any period and on any conditions, to allow the competent authority to correct the defect."*

109 In the event that this Court upholds the first challenge, it must declare RICA invalid to this extent. That is required by section 172(1)(a) of the Constitution.

110 However, this Court is then also empowered by section 172(1)(b) to suspend the operation of this declaration of invalidity and grant any order that is just equitable.

---

[131] RA p 994 para 30

[132] RA p 994 para 30

110.1 The general approach of the Constitutional Court in this regard is to suspend the declaration of invalidity for two years, but direct than an "interim reading-in" take place during this period.

110.2 This has the advantage of vindicating the rights concerned immediately, while still allowing Parliament to fix the defect more permanently as it deems fit. As the Constitutional Court has explained, in a case about a statute that unconstitutionally failed to respect the right to privacy of persons being searched:

> *"With interim reading-in, there is recognition of the Legislature's ultimate responsibility for amending Acts of Parliament: reading-in is temporary precisely because the Court recognises that there may be other legislative solutions. And those are best left to Parliament to contend with."*[133]

111 In the present case, therefore, the order that should be granted in respect of the first challenge is:

> *"It is declared that:*
>
> *(a) RICA, including sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe procedure for notifying the subject of the interception;*
>
> *(b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and*
>
> *(c) Pending the enactment of legislation to cure the defect, RICA shall be deemed to read to include the following additional sections 16(11) and (12):*
>
> *'(11) The applicant that obtained the interception direction shall, within 90 days of its expiry, notify in writing the person who was the subject of the interception and shall certify to the designated judge that the person has been so notified.*

---

[133] *Gaertner* at para 84

> *(12) The designated judge may in exceptional circumstances and on written application made before the expiry of the 90 day period referred to in sub-section (11), direct that the obligation referred to in sub-section (11) is postponed for a further appropriate period, which period shall not exceed 180 days.'"*

SECOND CHALLENGE – INADEQUACIES RELATING TO THE DESIGNATED JUDGE

Lack of any adversarial process

112 Section 16(7)(a) of RICA provides that an application must be considered and granted "*without any notice to the person or customer to whom the application applies and without hearing such person or customer*." Section 16(7)(a) also applies, with necessary changes, to the issuing of an entry warrant,[134] a direction in respect of real-time meta data,[135] a direction in respect of archived meta data,[136] as well as a combined application under section 18,[137] any amendment or extension[138] and to a decryption direction,[139]

113 As set out above, section 34 of the Constitution requires that hearings be *fair*. The principle of *audi alteram partem* – to hear the other side – is axiomatic to the South African legal system (and most other common law legal systems). The rationale is that a party should be given an opportunity of being heard

---

[134] Section 22(7) of RICA

[135] Section 17(6) of RICA

[136] Section 19(6) of RICA

[137] Section 18(3)(a) of RICA

[138] Section 20(6) of RICA

[139] Section 21(6) of RICA

before an order is made that might adversely affect their rights. Its importance was ably captured by the oft-quoted passage in *John v Rees*:

> *"As everybody who has anything to do with the law well knows, the path of the law is strewn with examples of open and shut cases which, somehow, were not; of unanswerable charges which, in the event, were completely answered; of inexplicable conduct which was fully explained; of fixed and unalterable determination that, by discussion, suffered a change."*[140]

114 In *My Vote Counts*, the majority of the Constitutional Court endorsed the passage in *John v Rees* and emphasised that "*even in an apparent 'open and shut' case, an affected party must be given an opportunity to meet the case advanced by an adversary*."[141]

115 The Constitutional Court has made clear that *audi* is one of the main pillars of the section 34 right to a fair-hearing.[142] Like the other principles of natural justice, the enforcement of *audi* "*serves as a lesson for future administrative action. But more than that, and whatever the merits of any particular case, it is a denial of justice in itself for natural justice to be ignored*."[143]

116 The principle of *audi* is especially important when the order being sought is one that will result in significant incursion into a fundamental right – as is the case here. There can thus be no question that the granting of a surveillance order against someone, without that person being heard, is a limitation of the right of access to courts and the right to privacy.

---

[140] *John v Rees* [1970] Ch 345 at 402

[141] *My Vote Counts NPC v Speaker of the National Assembly and Others* [2015] ZACC 31, majority judgment at para 176

[142] *National Director of Public Prosecutions and Another v Mohamed NO and Others* 2003 (4) SA 1 (CC) at para 36

[143] Lawrence Baxter "Administrative Law" (Juta, 1984) at 540

117 The real question again is whether this limitation is permissible. That is, does it meet the requirements of section 36 of the Constitution?

The public advocate is a less restrictive means

118 The applicants accept that it will not be possible for the subject of the interception to appear personally before the Judge prior to the order being granted.[144] This is because the subject's knowledge of the application could undermine the effectiveness of granting the interception direction in the first place.[145] The granting of the application in the absence of the party is, therefore, in our view rationally connected to the purpose of effective surveillance.

119 However, in relation to the less-restrictive means test, we submit that there are various mechanisms that could be utilised which would better balance the competing interests.

119.1 The real difficulty with interception directions under RICA is that there is no opportunity for the subject to contest the order granted before it is implemented. Where other extraordinary *ex parte* remedies such as an Anton Pillar order are granted under South African law these are generally done on an interim basis.[146] The Supreme Court of Appeal has made it clear (in the context of a warrant in terms of section 46 of the Competition Act) that any order given *ex parte* is by nature

[144] FA p 49 para 92

[145] FA p 49 para 92

[146] FA p 49 para 93

provisional, irrespective of the form that it takes.[147] Once it is contested and the matter is reconsidered by a court, the applicant for that *ex parte* order (in that case the Competition Commission) is in no better position in other respects than it was when the order was first sought.[148]

119.2 Yet in the present case, there is no provisional order, nor an interim order. An interception order is granted without the subject being heard, carried out without the subject being heard and fully carried out and completed without the subject being heard. (Indeed, the subject does not even get notice of the order.)

120 An obvious less-restrictive means to address this issue would be for RICA to make provision for a forum such as a public advocate.

120.1 As Duncan notes "*the granting of directions is an inherently one-sided process, which means that the judge has to take the information that is given to him on trust*".[149]

120.2 The appointment of a public advocate would be a key step towards addressing this dilemma. The public advocate would be a practising legal representative and would be statutorily and ethically bound to represent and advance the interests and rights of the subject of

---

[147] *Pretoria Portland Cement and Another v Competition Commission and Others* 2003 (2) SA 385 (SCA) at paras 44 – 47

[148] *Pretoria Portland Cement* at paras 44 – 47

[149] Jane Duncan, 'Communications Surveillance in South Africa: The Case of the *Sunday Times* Newspaper' in 'Global Information Society Watch 2014: Communications Surveillance in the Digital Age' (Report, Association for Progressive Communications and the Humanist Institute for Development Cooperation, 2014) www.giswatch.org/sites/default/files/communications_surveillance_in_south_africa.pdf at 226

surveillance in order to test the propositions put forward by the law enforcement agencies.

120.3 In other words, the subject of the interception would still have no knowledge of the matter. But he or she would still have the benefit of a public advocate advancing his or her case before the designated judge.

120.4 We submit that a public advocate is plainly a less-restrictive means of achieving the purposes of the Act, while posing less of an infringement on the rights of access to courts and privacy.

121 The applicants submit that even if the applicants' submission (regarding retrospective notification as a matter of course) finds favour with this Court, section 16(7) will remain unconstitutional in the absence of some form of system such as the public advocate. That is so because a review, by its nature, is retrospective and unable to avert or undo future harm.[150] Retrospective notification places the subject in a position to review a decision after the fact, and the public advocate system is intended to test the veracity of applications for interception directions before the designated judge grants them.[151]

122 The applicants submit that the public-advocate system and the notice system are complementary.[152] Both are required to remedy the unconstitutionality of section 16(7) of RICA.[153]

---

[150] FA p 50 para 96

[151] FA p 50 para 96

[152] FA p 51 para 96

[153] FA p 51 para 96

Respondents' contentions

123 The joint respondents argue that the public advocate system would cause lengthy application processes and undermine the security services capacity to act promptly in the interests of national security.[154]

124 Moreover, they contend it could lead to information being leaked because the circle of people with knowledge of the surveillance has been expanded,[155] or lead to security leaks.[156]

125 The respondents' claims are all bald and completely devoid of any factual foundations. The Constitutional Court has rejected such approaches. It held:

> *"no evidence, direct or inferential, was adduced to establish likelihood of detriment… In effect we are invited to find a probability of material economic detriment to the respondent's marks of well-entrenched repute on conjecture alone. We must decline the invitation."*[157]

126 Importantly, it is the party seeking to justify a limitation of constitutional rights that bears the burden of doing so.[158] We submit that none of the respondents placed sufficient evidence before this Court to demonstrate that some form of public advocate system would be unworkable. As regards delays, there is no reason why fit and proper persons from the legal profession (who would be bound to keep matters completely confidential) could not take up the task.

---

[154] Joint AA p 782 para 97

[155] 1st respondent's AA p 657 para 105

[156] Joint AA p 782 para 97

[157] *Laugh It Off Promotions CC v South African Breweries International (Finance) BV t/a Sabmark International and Another* 2006 (1) SA 144 (CC) at paras 58-59

[158] *Prophet v National Director of Public Prosecutions* 2006 (2) SACR 525 (CC) at para 33; see also *Prince v President, Cape Law Society and Others* 2001 (2) SA 388 (CC) at para 21; *Rail Commuters Action Group and Others v Transnet Ltd t/a Metrorail* 2005 (2) SA 359 (CC) at para 43; and *S v Shaik and Others* 2008 (2) SA 208 (CC) at paras 17-23

127 The respondents cannot seriously be contending that the designated judge would not need to be familiar with the facts or conduct research regarding the application. Thus, any public advocate system would actually make the system more productive since it would release the burden off the designated judge.

128 Lastly, if there is a truly urgent need for a particular interception direction then there are the emergency provisions in place. But the general position should be that there is some form of adversarial system so that the state agencies can be tested on their versions, members of the public advocate would become well-versed with the applications and the kinds of questions that need to be asked. For instance, the state entities should be made to prove that the telephone numbers that they wish to surveil are in fact the people that they claim. That is not a difficult aspect to prove since the cellular telephone numbers would in any event be registered to people's names in terms of RICA.

Remedy in relation to the absence of an adversarial process

129 RICA, and particularly section 16(7) thereof, therefore falls to be declared invalid because it fails to make provision for any form of public advocate system. However, we accept that it is not easily practical to fashion an interim remedy in this regard.

130 The order that should be granted in respect of this part of the case is therefore simply as follows.

"It is declared that:

(a) RICA, including sections 16(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to provide for a system for a public advocate or other appropriate

safeguards to deal with the fact that the orders in question are granted ex parte; and

(b) *The declaration of invalidity is suspended for two years to allow Parliament to cure the defect."*

Lack of independence safeguards for the designated judge

131 Section 1 of RICA 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 No. 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".*

132 The applicants contend that the designated judge must plainly be independent and that the principles set out by the Constitutional Court in relation to structural protections that are required to ensure independence apply with equal force in respect of the designated judge.[159]

133 Accordingly, the appointment process and term of the designated judge's appointment must protect the designated judge's independence. The applicants submit that the present appointment process and term fail to do so.[160]

134 The applicants submit that RICA fails to secure the independence of the designated judge in two respects.[161]

134.1 First, there is no term specified under RICA. The present term for a designated judge is generally one year, with the option for renewal.[162] But there is no restriction on how many renewals there can be.

---

[159] FA p 55 para 108

[160] FA p 55 para 108

[161] FA p 51 para 99

[162] FA p 51 para 99.1

134.2 Second, the designated judge is simply appointed at the instance of a member of the executive (the Minister).[163]

135 The "overriding consideration" is whether the autonomy-protecting features in the legislation enable the members of the entity required to be independent (e.g. the designated judge or the investigative unit) to carry out their duties vigorously, without any inhibitions or fear of reprisals.[164]

136 Further, the appearance or perception of independence plays an important role in evaluating whether independence in fact exists. As the Court explained:

> *"[P]ublic confidence in mechanisms that are designed to secure independence is indispensable. Whether a reasonably informed and reasonable member of the public will have confidence in an entity's autonomy-protecting features is important to determining whether it has the requisite degree of independence. Hence, if Parliament fails to create an institution that appears from the reasonable standpoint of the public to be independent, it has failed to meet one of the objective benchmarks for independence. This is because public confidence that an institution is independent is a component of, or is constitutive of, its independence."*[165]

<u>The designated judge's term</u>

137 There is no term specified under RICA for the designated judge. A term of one year has emerged as a matter of practice.[166] We submit that the short duration

---

[163] FA p 51 para 99.2

[164] *Helen Suzman Foundation v President of the Republic of South Africa and Others; Glenister v President of the Republic of South Africa and Others* 2015 (2) SA 1 (CC) at para 32; *Glenister v President of the Republic of South Africa and Others* 2011 (3) SA 347 (CC) ("*Glenister II*") at para 222

[165] *Glenister II* majority judgment, para 207, with reference to *S v Van Rooyen* 2002 (5) SA 246 (CC) at para 32; and *Valente v The Queen* [1986] 24 DLR (4th) 161 (SCC) at 172. Also restated in *Helen Suzman Foundation (CC)* at para 31

[166] FA p 52 para 100; see also the 2011 JSCI Report (at p 28 para 17) which states that "*[t]he appointment is usually for a period of a year renewable*".

and renewability of the designated judge's term has the potential to undermine the independence of the designated judge.[167]

138 The extension of a term of office, particularly one conferred by the Executive or by Parliament, may be seen as a benefit.[168] The judge or judges upon whom the benefit is conferred may be seen as favoured by it.

139 Security of tenure requires protection against termination of employment or suspension at the discretion and behest of the Executive. The importance of security of tenure in ensuring the independent functioning of the agency was explained by Moseneke DCJ and Cameron J as follows:

> *"While it is not to be assumed, and we do not assume, that powers under the SAPS Act will be abused, at the very least the lack of specially entrenched employment security is not calculated to instil confidence in the members of the DPCI that they can carry out their investigations vigorously and fearlessly. In our view, adequate independence requires special measures entrenching their employment security to enable them to carry out their duties vigorously".*[169]

140 Non-renewability fosters public confidence in the institution of the judiciary as a whole, since its members function with neither threat that their terms will not be renewed nor any inducement to seek to secure renewal.[170]

141 In *Helen Suzman Foundation v President of the Republic of South Africa; In Re: Glenister v President of South Africa*[171] the High Court summarised the

---

[167] FA p 53 para 104. See also S v *Van Rooyen* as well as *Justice Alliance of South Africa v President of Republic of South Africa, Freedom Under Law v President of Republic of South Africa, Centre for Applied Legal Studies v President of Republic of South Africa* 2011 (5) SA 388 (CC) at para 73 where the Constitutional Court held that the renewability of the term of the Chief Justice would undermine independence.

[168] *Justice Alliance of South Africa* at para 75

[169] *Glenister II* majority judgment, at para 222

[170] *Justice Alliance of South Africa* at para 73

Constitutional Court's jurisprudence on the issue and held that renewability of a term would undermine independence:

> *"[R]enewability of the term at the behest of the Minister is intrinsically inimical to independence. It is clear from the CC's judgments in Glenister 2 and JASA that it is renewability as such, rather than the insufficiency of conditions or constraints imposed on renewability, which jeopardises independence. Renewability thus has no valid place in the scheme of a unit that is constitutionally required to be adequately independent."*

142 The Joint Standing Committee reports have called for the term of the designated judge to be extended on numerous occasions (albeit for different reasons).[172]

143 We submit that it is clear that the designated judge needs stronger security of tenure as well as a longer non-renewable term in order to curb any fears that reappointment could be used as a benefit. RICA's provisions do not provide any form of Parliamentary oversight to secure the designated judge's tenure. This is particularly concerning when combined with the manner in which the designated judge is appointed.

Appointment

144 The applicants contend that permitting a member of the executive to select one judge without any other process in place for such a sensitive constitutional function undermines the public confidence in the designated judge's

---

[171] *Helen Suzman Foundation v President of the Republic of South Africa and Others; In re: Glenister v President of South Africa and Others* 2014 (4) BCLR 481 (WCC) at para 68

[172] FA p 52 paras 101 – 103

independence and accordingly the constitutional requirement of independence.[173]

144.1 A sensitive post should not merely be left to one judge and should be handled by a panel of judges.[174] The role performed by the designated judge is significant – it involves the curtailment of an individual's rights – where the person is not able to present his side of the case before the decision is taken. These matters are complex and different judges might well reach different conclusions. The panel of judges would provide a greater margin for human error – that is precisely why appellate courts around the world are staffed by panels of judge rather than merely a single judge.[175]

144.2 The designated judge must be selected following a proper public interview process before the Judicial Services Commission.[176] That is precisely the position for judges for the Electoral Court.[177] The appointment of the designated judge requires at least as many safeguards for independence as the judges for the Electoral Court.[178]

---

[173] FA p 53 para 105

[174] FA p 53 para 106.1

[175] RA p 1013 para 78

[176] FA p 53 para 106.2

[177] FA p 53 para 106.2

[178] FA p 53 para 106.2

Respondents' contentions

145 The Joint Affidavit provides that the integrity of the current process is validated by the institutional independence of the designated judge.[179] The first respondent claims that there is no basis to question the designated judge's independence since judges are appointed in terms of an open and transparent process before a body established in terms of the Constitution. But that is not correct. The designated judge is not appointed by the Judicial Services Commission.

146 We emphasise that whenever a person who is already a judge seeks a promotion to higher office there is a fresh process held before the JSC (even though that person became a judge following an open and transparent process).

Remedy in relation to independence safeguards

147 The applicants submit that viewed cumulatively there is no doubt (following the decisions in *Justice Alliance*, *Glenister II* and *Helen Suzman*) that there is insufficient protection for the designated judge's independence. We emphasise that, if anything, the role of the designated judge is more contentious than many matters that the ordinary High Court judge might deal with. It is a position of supreme constitutional importance and like the Electoral Court will be dealing with very politically contentious matters. It follows that a similar appointment process should be undertaken.

[179] RA p 781 para 95

148 In this case, it is possible to fashion an interim reading in order. The order that should be granted in respect of this part of the case is therefore as follows:

"It is declared that:

(a) RICA, including the definition of 'designated judge' in section 1, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe an appointment mechanism and terms for the designated judge which ensure the designated judge's independence;

(b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and

(c) Six months after the date of this order and pending the enactment of legislation to cure the defect, "designated judge" in RICA shall be deemed to read as follows:

> *'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 appointed by the Judicial Service Commission for a non-renewable term of two years to perform the functions of a designated judge for purposes of this Act'."*

THIRD CHALLENGE – INADEQUATE SAFEGUARDS REGARDING THE DATA OBTAINED

Failure to prescribe any procedure for examining, using and storing the data obtained

The nature of the problem

149 RICA fails to prescribe the procedure to be followed for examining, using and storing the data obtained from the surveillance.

150 Three of the minimum safeguards set out by the European Court of Human Rights in *Weber v Germany* deal with the manner in which the data that are obtained via interception are managed and aim to protect the privacy of the data subject:

150.1 The procedure to be followed for examining, using and storing the data obtained;[180]

150.2 The precautions to be taken when communicating the data to other parties;[181] and

150.3 The circumstances in which recordings may or must be erased.[182]

151 RICA fails to include provisions adequately dealing with any of these three aspects.[183]

151.1 Section 35(1)(f) of RICA sets out various responsibilities of the Director of the interception centres. These include that the Director:

> *"must prescribe the information to be kept by the head of an interception centre in terms of section 37, which must include particulars relating to–*
>
> *(i) applications for the issuing of directions and the directions issued upon such applications which is relevant to the interception centre of which he or she is the head; and*
>
> *(ii) (the results obtained from every direction executed at that interception centre)".*[184]

151.2 Section 37(1) requires the head of an interception centre to keep or cause to be kept proper records of such information as may be prescribed by the Director in terms of section 35(1)(f). The head must submit written reports on a quarterly basis to the Director setting out the

---

[180] FA p 44 para 77.1

[181] FA p 44 para 77.2

[182] FA p 44 para 77.3

[183] FA p 44 para 79

[184] FA p 44 para 80

records kept by him or her, any abuses in relation to the execution of the directions.[185]

152 RICA fails to incorporate safeguards dealing with how the interception directions should be executed. Such safeguards are normally present in statutory authorisation of these types of legislative provisions, for instance in statutes relating to arrest warrants.[186]

153 In the English case of *R (Davis and Others) v Secretary of State for the Home Department (Open Rights Group and others intervening)*[187] there was a challenge to the validity of the Data Retention and Investigatory Powers Act on the basis that it was inconsistent with European Union law.

154 The court held that the UK legislation was indeed inconsistent with European Union law on the grounds that it did not, inter alia, lay down clear and precise rules providing for access to and use of communications data retained to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences.[188]

155 RICA fails to include provisions adequately dealing with these key aspects. In this regard, there is no proper provision made in RICA regarding:

155.1 where intercepted information is stored;

---

[185] FA p 44 – 45 para 81

[186] See, for example, section 29 of the Criminal Procedure Act 51 of 1977.

[187] *R (Davis and Others) v Secretary of State for the Home Department (Open Rights Group and others intervening)* [2015] EWHC 2092 (Admin)

[188] Ibid at para 114

155.2 who may have access to it and under what conditions;

155.3 whether any access has to be recorded/registered;

155.4 whether copies may be made;

155.5 whether the fact of the number and distribution of copies has to be recorded in any way;

155.6 whether access or copies may be shared within the intelligence or security community and if so what documentation of this sharing takes place;

155.7 whether the material must be or may be destroyed at any time and if so when/under what conditions;

155.8 if and how extraneous or irrelevant material that is gathered must be separated and destroyed and whether this is documented.

156 These difficulties have been recognised by the Inspector General in South Africa. The 2011 Joint Standing Committee on Intelligence Report stated that:

> *"The IG further noted that there was a lacuna/gap in the* RICA *Act (dealing with the handling of intercept material)."*[189]

157 Even assuming that a lawful interception direction were to be granted in respect of a particular person in relation to issue X, there is no indication under RICA what happens to information relating to any other issues (issues Y and Z) which are not related to the interception direction.[190] A person will, for example, use

[189] 2011 JSCI Report to Parliament at 26 para 16

[190] FA p 46 para 84

the same telephone for many conversations - personal, business and otherwise.[191]

Respondents' contentions

158 The first respondent claims that the correct question is whether the existing measures in RICA can effectively safeguard abuse[192] and the first respondent claims that they can.[193] In other words, the fact that the European Court of Human Rights has set down other minimum safeguards which RICA does not have – does not lead to RICA being declared unconstitutional.

159 In *Weber v Germany* the European Court emphasised that, notwithstanding its general approach of granting the implementing state a margin of appreciation,[194] "*in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse*".[195]

160 The joint respondents contend that RICA, read with other legislation and the Constitution, provides sufficient measures for how intercepted material is dealt with.

---

[191] Joint AA p 766 paras 51 - 52

[192] RA p 1001 para 46

[193] RA p 1001 para 46

[194] In other words, the court is less stringent than a domestic court might be – on the basis that national authorities should be given a wide margin for determining how to implement provisions in their own state (reasons for the doctrine include comity).

[195] *Weber v Germany* at para 106

160.1 Section 37(2) of RICA provides detailed regulation regarding the submission of reports on where the records are kept and abuses. The reports need to be submitted to the Minister and the Chair of the JSCI.[196] These oversight mechanisms read with sections 35(1) and 36 of the Constitution "*comply with the prevailing constitutional standards*".[197]

160.2 Section 26 of RICA, further, limits the scope for abuse as it provides that only the person who applied for the interception direction (or a law enforcement officer or person authorised by the applicant in writing) can execute the interception direction.

160.3 Section 10(4) of the Intelligence Services Act 65 of 2002 enjoins the Director-General to:

> *"take steps to ensure that (a) national security intelligence collection methods, sources or information, and the identity of members of the Intelligence Service are protected from unauthorised disclosure".*[198]

161 However, in truth none of these provisions provides adequate protection. The purpose of section 10(4) of the ISA is to curb unauthorised disclosure – for instance publishing the material in the press or providing the information to persons outside the state entity. But it does nothing to restrict: how authorised persons must treat the material; who authorised persons may delegate the power to access the material to; how relevant surveillance data is separated from irrelevant personal information.

---

[196] Joint AA p 766 paras 51 - 52

[197] Joint AA p 766 para 52

[198] Joint AA p 767 para 56

162 The submission of reports requires state entities to demonstrate how they have been complying with RICA's provisions. In this instance, RICA fails to set out any procedure that needs to be followed

163 Restricting certain individuals to execute the interception direction does not limit what that person may do with the material or how it should be stored and accessed or sorted. For example, when the Competition Commission seizes material from a firm's premises – the electronic material is first sorted using random keyword searches performed by independent IT experts. Thereafter, the firm's legal representatives are entitled to ensure that this material does not contain any legally privileged material before the electronic information is provided to the Commission.

164 The first respondent relies on the Protection of Personal Information Act 4 of 2013 ("POPI"), aimed at protecting and regulating the collection and retention of personal information and when it is "functionally implemented" it will afford additional protection to the sharing of personal information obtained by surveillance.[199]

165 These fall to be rejected for two reasons.

165.1 First, the substantive provisions of POPI have not yet been brought into force.

[199] 1st respondent's AA p 658 para 106

165.2 Second, and in any event, section 6(1)(c) of POPI provides that the Act does not apply to the processing of personal information, by or on behalf of a public body:

> *"(i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety: or*
>
> *(ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures,*
>
> *to the extent that adequate safeguards have been established in legislation for the protection of such personal information"*

166 In other words, if the safeguards under RICA are adequate then POPI does not apply. It is only if RICA's safeguards are inadequate that POPI would apply.[200] Seeking to rely on POPI does not assist in answering the applicants' challenge: whether the safeguards in RICA are adequate or not.[201]

167 The fifth respondent details various internal systems that SAPS has in place to regulate the procedure for any officer applying for an interception direction.[202]

167.1 SAPS introducing internal procedures in order to plug the hole left by RICA might be laudable, but it is irrelevant to the question whether RICA is unconstitutional.[203] There is nothing in law preventing SAPS from adopting less rigorous standards.[204]

---

[200] RA p 1000 para 43

[201] RA p 1000 para 44

[202] 5th respondent's AA p 945 – 950 paras 43 – 50

[203] RA p 1002 para 48.1

[204] RA p 1002 para 48.2

167.2 SAPS's need for internal measures cuts the other way – it shows that SAPS deemed it necessary to supplement the 'safeguards' set out by RICA.[205]

Limitations analysis

168 As regards the limitations analysis, we submit that there is no rational relationship between the purposes sought to be achieved by RICA and the lack of any provisions regarding the manner in which the information is dealt with under the Act.

169 As set out above, the purpose of RICA is to achieve its crime-fighting purpose with as little impact on the subject's rights as possible: to protect the right to privacy and to minimise, disincentivise and deter abuse. That is why RICA creates requirements for the applications to be made and executed as well as offences for failing to comply with its provisions. A complete failure to deal with key principles about how and who may access intercepted material – leaves it to chance and bears no rational relationship to the purpose.

170 Second, there are plainly less restrictive means of achieving the purpose. As set out above, private telephone calls are among the most private communications a person can have. Failing to set out any framework for how the intercepted material must be dealt with by the state officials – means there is no rational link whatsoever between the means and the purpose.

[205] RA p 1002 para 48.1

171 The European Court of Human Rights' list detailed the minimum safeguards to protect against abuse. These minimum safeguards demonstrate that there are less restrictive means of achieving RICA's purpose.

Mandatory data retention by telecommunications service providers

172 Section 30(1)(b) of RICA provides that – notwithstanding any other law – telecommunications service providers must store communication-related information.

173 Section 30(2) provides in relevant part:

> *"The Cabinet member responsible for communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and the telecommunication service provider or category of telecommunication service providers concerned, must, on the date of the issuing of a telecommunication service licence under the Electronic Communications Act, to such a telecommunication service provider or category of telecommunication service providers*
> *(a) issue a directive in respect of that telecommunication service provider or category of telecommunication service providers, determining the-*
>
> *(iii) 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".*

174 The European Court of Justice has declared that an analogous mandatory data retention regime infringed the right to privacy and entailed a "*wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data*".[206]

[206] Judgment in Joined Cases *Digital Rights Ireland* C-293/12; and *Seitlinger and Others* C-594/12 (2014)

175 The storage of personal communications limits the right to privacy.[207] Importantly, the length of time that the communications are kept aggravates this limitation.[208]

176 The applicants submit that there are two difficulties with these provisions in RICA.

176.1 First, the minimum period of three years is impermissibly long.[209] The state bears the onus to demonstrate why a period of two years is not sufficient as a minimum. Similarly – the state must demonstrate using evidence why a maximum period of five years is constitutionally justifiable.[210]

176.2 Second, and more significantly, RICA is under-inclusive as there are no oversight mechanisms required by section 30(2)(a)(iii) of RICA.[211] 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.[212] On this score, we submit that all of the flaws set out in detail above (at *inter alia* paragraph 155 above) apply equally in this context, where the private sector has control over an individual's private information. Thus, the

---

[207] FA p 48 para 88

[208] FA p 48 para 88

[209] FA p 48 para 89.1

[210] FA p 48 para 89.1

[211] FA p 48 para 89.2

[212] FA p 48 para 89.2

lengthy three to five year period is exacerbated by a complete absence of any mechanisms to prevent abuse. We submit that there are plainly less restrictive methods of achieving RICA's purposes in this regard. First, RICA needs to have a detailed set of requirements regarding the storage and handling of the data by the telecommunications service providers. Second, RICA should provide audit and inspection mechanisms to verify that the telecommunications companies are complying with the safeguards.

177 The United Nations Human Rights Committee Report stated that South Africa should take all necessary measures to ensure that its surveillance activities conform to its obligations under the ICCPR, including Article 17 thereof. Among the reform it requested it stated:

> *"consider revoking or limiting the requirement for mandatory retention of data by third parties. … The State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies."*[213]

Respondents' contentions

178 The first respondent states that RICA provides for a retention of communication-related information for a period between three and five years and the Cabinet member responsible for telecommunications and postal services has, by Government Notice, prescribed three years.[214]

---

[213] FA p 86 para 185

[214] 1st respondent's AA p 662 para 121

179 The joint respondents contend that the 3-year period is consistent with the practice in other jurisdictions, including the European Court of Human Rights.[215]

180 The first respondent notes that the period in Australia is two years and also argues that the "*length of time for which the information may be necessary will differ from case to case*."[216] The first respondent claims that *"[t]he peculiar circumstances of the case would determine the duration for which the data should be stored*".[217] Moreover, that various countries determine different periods for the preservation of meta-data which range from 6 months to two years.[218]

181 Significantly, the first respondent also states that typically the law enforcement agencies in South Africa ordinarily request communication-related information spanning less than 19 months.[219]

182 Ironically, this argument also cuts against the first respondent's claim. This is because the three-year retention period is mandatory, in all instances, and it is not variable according to the range of factors that the first respondent lists (for example, the nature and extent of crime to be investigated and to which the RICA applies).[220]

---

[215] Joint AA p 771 para 67

[216] 1st respondent's AA p 662 para 122

[217] 1st respondent's AA p 663 para 125.5

[218] 1st respondent's AA p 667 para 132

[219] 1st respondent's AA p 668 para 133.2

[220] RA p 1004 para 54.1

183 The first respondent has conceded that in some instances three years will be far too excessive. This amounts to a concession that the Acts fails to meet the standards set by the limitations clause, on the basis that:

183.1 In some instances the limitation will not be rationally related to the purpose – since there might have been no reason or basis to keep the information for longer than 6 months but the regime requires the communications to be kept for three years irrespective of the circumstances;

183.2 Second, the Australian and other systems demonstrate that the purpose can ably be served within a period of one or two years. Thus, the mandatory period of three years is not the least restrictive means of fulfilling the purpose. On this score, we note that various other jurisdictions including Belgium, Denmark, Finland, Germany, Spain have retention periods of approximately a year.

184 The first respondent's arguments cut against the respondents and show why RICA's provisions do not satisfy the limitations clause.

184.1 There is no discretion when there should be;[221]

184.2 Two years is the period generally thought to be adequate (with some other states – opting for periods as low as 6 months);[222]

184.3 The information requested is generally only for 19 months.[223]

---

[221] RA p 1011 para 70.1

[222] RA p 1011 para 70.2

185 The only claim outside of the general rule that is put up are claims relating to organised crime[224] and transnational investigations.[225] But there are three difficulties with these claims.

185.1 First, the information is hearsay. The applicants pointed out in their replying affidavit that the information amounted to hearsay as there is no indication regarding how the deponent was aware of the information – or any confirmatory affidavits from persons who provided the first respondent with the information.

185.2 Second, and in any event, the claims are speculative and not supported by any empirical research or facts.[226] The first respondent puts the argument no higher than "it tends to take longer", "it can take time to discover this" and "there are often delays in the investigations".

185.3 The first respondent has not pleaded any facts regarding what proportion of investigations the organized crime or transnational investigations amount to. The first respondent does not specify how much lower than 19 months the ordinary request is for.

186 The first respondent seeks to clarify that the ordinary period (some duration less than 19 months) is for crimes that are "*easily detectable and unrelated to*

---

[223] RA p 1011 para 70.3

[224] 1st respondent's AA p 668 para 133.3

[225] 1st respondent's AA p 669 para 133.6

[226] RA p 1011 para

any other crime/s".[227] There are two further problems with the claim made by the first respondent:

186.1 First, the first respondent does not specify what crimes or range of crimes are considered "easily detectable";

186.2 Second, and more importantly, the first respondent does not explain why RICA is needed at all when these crimes are "easily detectable" since RICA is a measure of last resort (which the respondents accept).

187 Put differently, the question is whether there is a less restrictive means than mandatory data retention for 3 years.

187.1 The first respondent has not made out a case justifying access to meta-data for a period of 3 years as the general rule. On the first respondent's version – the general period is 19 months – 1 ½ years i.e. even shorter than the Australian period.

187.2 At best for the respondents, then, there could be two separate regimes according to which even if the mandatory period of retention was 3 years there should be a higher threshold for accessing the data where it exceeds the 19-month period.

188 The applicants submit that the mandatory three-year period fails to satisfy the requirements of the limitations clause.

---

[227] 1st respondent's AA p 668 para 133.2

Remedy on the third challenge

189 In the circumstances, it is plain that RICA fails to provide adequate safeguards for the examining, copying and storage of data obtained through surveillance. This is severely exacerbated by the provision requiring the mandatory retention of information by telecommunication service providers for three years.

190 We submit that the appropriate remedy to be granted in this regard is as follows:

> *"It is declared that:*
> *(a) RICA, including section 37 thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe the proper procedure to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions;*
>
> *(b) Section 30(2)(a)(iii) of RICA is inconsistent with the Constitution and accordingly invalid; and*
>
> *(c) The declarations of invalidity are suspended for two years to allow Parliament to cure the defects."*

FOURTH CHALLENGE – INTERCEPTION OF COMMUNICATIONS WHERE SUBJECTS HAVE A SOURCE-PROTECTION DUTY

191 Section 16(5) of RICA sets out the requirements for an interception direction to be granted. These requirements do not deal with scenarios in which an interception direction may be granted against subjects with a duty to protect the confidentiality of the communications with sources and/or clients.[228]

[228] FA p 56 para 110

192 The applicants contend that the circumstances in which an interception direction may be granted against journalists or lawyers should be different in at least the following respects:

192.1 A stricter threshold for granting an application;

192.2 An independent intermediary should screen the information and pass any relevant information on to the state agency that sought the direction.

Stricter threshold for subjects with a source-protection duty

193 There is a less restrictive means to achieve the purpose. The applicants submit that the position should be analogous to the principles set out in Article XV of the Declaration of Principles of Freedom of Expression in Africa (relating to the protection of sources).[229]

193.1 The interception of the journalist or lawyer must be necessary for the investigation or prosecution of a serious crime, or the defence of a person accused of a criminal offence;

193.2 The information or similar information leading to the same result cannot be obtained elsewhere; and

193.3 The public interest in disclosure (to investigators of confidential source or client communications) outweighs the harm to freedom of expression and/or the right to legal privilege.

[229] FA p 56 para 111.1

194 Part of the difficulty with RICA lies in the fact that the threshold set by section 16(5) of RICA is too low. Section 16(5) requires that there are "reasonable grounds to believe" that the particular ground exists, and that there are "reasonable grounds to believe" that interception of particulars communications concerning the relevant ground will be obtained by the interception direction.[230]

195 The Necessary and Proportionate Principles (referred to above) instead use the standard of a "*high degree of probability*".[231] The applicants submit that such a higher threshold should be used in respect of surveilling journalists or lawyers, because the extent of the infringement to the right to privacy becomes amplified. That is so because the person interacting with the journalist or the lawyer has a heightened expectation that the information being exchanged is going to be kept highly confidential:

195.1 The media's sources could also be compromised or endangered by their participation in communications with journalists;

195.2 During a conversation with a lawyer, a person may disclose legally privileged facts.

Journalists

196 Section 16(1) of the Constitution provides that everyone has the right to freedom of expression, which includes:

> *"(a) freedom of the press and other media;*
> *(b) freedom to receive or impart information or ideas;*
> *(c) freedom of artistic creativity; and*
> *(d) academic freedom and freedom of scientific research."*

[230] Section 16(5)(b)(i) of RICA

[231] Ibid.

197 The right to freedom of expression, which comprises the right to an independent media, is jealously guarded in South Africa. This is particularly so because of the strident attempts by the apartheid government to control the media as well as the population's consumption of any art and literature that was considered immoral or improper.

198 The Constitutional Court has firmly enunciated the importance of the right to freedom of expression on numerous occasions. It has held that:

198.1 freedom of expression lies at the heart of democracy;[232]

198.2 is one of a "web of mutually supporting rights that hold up the fabric of the constitutional order";[233]

198.3 It has affirmed the media's role as the watchdog of society keeping the public informed of matters of public interest;

198.4 The very ability of each citizen to be a responsible and effective member of society "depends on the manner in which the media carry out their constitutional mandate."[234] Accordingly, "[t]he media thus rely on freedom of expression and must foster it."[235]

199 Examples of similarly powerful and elegant dicta upholding the importance of the free press in South Africa abound.

---

[232] *South African National Defence Union v Minister of Defence and Another* 1999 (6) BCLR 615 (CC)

[233] *Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others* 1996 (3) SA 617 (CC) at para 27

[234] *Khumalo v Holomisa* at paras 21 – 23

[235] Ibid

200 What is particularly important in relation to the surveillance of journalists is that inherent in section 16 of the Constitution is the principle that members of the media are entitled to keep their sources confidential. The importance of this entitlement cannot be overstated. In *British Steel Corporation v Granada Television Ltd*[236] Lord Denning, for example, stated:

> *"(I)f [newspapers] were compelled to disclose their sources, they would soon be bereft of information which they ought to have. Their sources would dry up. Wrongdoing would not be disclosed. Charlatans could not be exposed. Unfairness would go unremedied. Misdeeds in the corridors of power, in companies or in government departments would never be known."*[237]

200.1 In *Government of the Republic of South Africa v The Sunday Times Newspaper and Another*[238] the High Court held:

> *"It is the function of the press to ferret out corruption, dishonesty and graft wherever it may occur and to expose the perpetrators. The press must reveal dishonest mal- and inept administration… It must advance the communication between the governed and those who govern."*[239]

201 In *Goodwin v United Kingdom*[240] the European Court of Human Rights emphasised that –

> *"Protection of journalistic sources is one of the basic conditions for press freedom … Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure*

---

[236] [1981] AC 1096

[237] Ibid at 1129

[238] *Government of the Republic of South Africa v The Sunday Times Newspaper and Another* 1995 (2) BCLR 182 (T)

[239] Ibid at 188, endorsed by the Constitutional Court in *Khumalo v Holomisa*

[240] *Goodwin v United Kingdom* [1996] 22 E.C.H.R 123

cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest…"[241]

202 The South African courts have followed suit. In *Bosasa*[242] the court held:

"If indeed freedom of the press is fundamental and sine qua non for democracy, it is essential that in carrying out this public duty for the public good, the identity of their sources should not be revealed, particularly, when the information so revealed, would not have been publicly known. This essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded."[243]

203 Accordingly, any provisions of RICA which compromise the media's entitlement to keep its sources confidential will infringe the right to freedom of expression and the enquiry will turn to whether that infringement may be justified under the limitations clause.

204 We emphasise that the applicants' concerns about the surveillance of journalists are based – in part – on numerous practical examples of interception that has occurred, without any basis for it. The applicants set out these examples in the papers:

204.1 While journalists Stephan Hofstatter & Mzi wa Afrika were investigating major corruption scandals in the SAPS, the SAPS' Crime Intelligence Division tapped their phones. Copies of the RICA warrant which ordered that their phones numbers should be tapped. According to the RICA authorisation under which their phones were tapped, the SAPS had told the designated judge that the numbers belonged to ATM bombing

---

[241] Ibid at para 39

[242] *Bosasa Operation (Pty) Ltd v Basson and Another* 2013(2) SA 570 (GSJ)

[243] Ibid at para 38

suspects. The SAPS were ostensibly authorised perform real-time interception of their calls and text messages, as well as of their meta-data;[244]

204.2 Journalist Athandiwe Saba's phone records had been seized in 2016 in terms of a warrant by section 205 of the CPA, and such records may have been unlawfully provided by the SAPS and the NPA to a third party private investigator;[245]

204.3 A private investigator illegally accessed the private phone records of business press editors Peter Bruce and Rob Rose, apparently for the benefit of a Gupta-family linked propaganda campaign;[246]

204.4 The erstwhile Mpumalanga Premier David Mabuza announced in January 2015 that he was receiving briefings from State Security on the movements of journalists in the province journalist, singling out Tom Nkosi, who is the founder and publisher of Mpumalanga investigative newspaper Ziwaphi, who Mr Mabuza alleged had met with Mr Mabuza's "enemies" within the ANC;[247]

204.5 Journalist Sipho Masondo, who was working on a series of investigations involving corruption in South Africa's water delivery

---

[244] RA p 1019 para 96.1

[245] RA p 1019 para 96.2

[246] RA p 1019 para 96.3

[247] RA p 1020 para 96.4

projects, was informed by a source in SAPS's Crime Intelligence that somebody was listening to his calls;[248] and

204.6 Members of the so-called 'SABC 8', being a group of journalists and editors who spoke out against censorship and managerial interference under former SABC boss Hlaudi Motsoeneng in 2016, were informed that their communications were being intercepted.[249]

205 The applicants also provide various international examples which demonstrate that surveillance and bulk surveillance in particular pose significant threats to journalists and press freedom.[250]

Lawyers

206 The same defects apply where the interception direction is granted against a lawyer or a lawyer's client.[251]

207 Legal privilege began as a general rule of common law, which protects communications between a lawyer and his client from disclosure.[252] The following elements must be present:[253]

207.1 The legal advisor must be an advisor in a professional capacity;

207.2 The communication must have been made in confidence;

---

[248] RA p 1020 para 96.5

[249] RA p 1020 para 96.6

[250] RA p 1020 – 1021 paras 97 – 98

[251] FA p 62 para 129

[252] FA p 62 para 130

[253] FA p 62 para 131

207.3 The communication has to be made either for the purposes of giving legal advice or litigation;

207.4 The advice must not facilitate the commission of a crime or fraud; and

207.5 The privilege must be claimed.

208 The Constitutional Court has made it clear that legal privilege is now a fundamental constitutional right.[254] Members of the public must be able to make full and frank disclosure to their legal advisers (for the purpose of obtaining advice or giving instructions) without fear that this information will subsequently be disclosed.[255]

209 Foreign jurisdictions have equally emphasised the importance of legal privilege holding that without legal privilege the long-term tendency would be for law enforcement authorities to press for extra-judicial methods of investigation and decision-making.[256]

210 Critically, a general principle of maintaining privilege is that privileged communications must be kept confidential.[257] Once confidentiality is lost then, in the vast majority of cases, legal privilege is also lost.[258]

211 As regards a means of filtering intercepted communications – there should be some system according to which keywords are used to search within the

---

[254] *Thint* at para 184, in the context of criminal proceedings.

[255] FA p 62 para 132

[256] *Baker v Campbell* (1983) 153 CLR 52

[257] *South African Airways Soc v BDFM Publishers (Pty) Ltd and Others* 2016 (2) SA 561 (GJ) at para 49

[258] Ibid

communications so that all of the journalist's or lawyer's communications are not monitored.

212 These measures are particularly important in the context of the media because of a journalist's duty to protect confidential sources and if sources are aware that they may indirectly be the target of surveillance while divulging confidential information to the press – this will undoubtedly have a chilling effect on sources coming forward.

213 The European Court of Human Rights found that surveillance would affect the right to freedom of expression under Article 10 of the European Convention on Human Rights and that:

> *"there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or deterred from calling or providing information by telephone...the transmission of data to other authorities, their destruction and the failure to notify the first applicant of surveillance measures could serve further to impair the confidentiality and protection of information given to her by her sources."*[259]

214 Indeed, because of the nature of the job performed by journalists, sources will often deal with journalists on a confidential basis when they are fearful to come forward on the record.

215 The proposition that targeted surveillance harms the media is not, moreover, mere conjecture. The harm to journalism has been reflected in empirical research done in South Africa and abroad.

215.1 For instance, in 2014 Human Rights Watch published a report on how large-scale surveillance is harming journalism, law, and American

[259] *Weber v Germany* at para 145

democracy.[260] Journalists surveyed in the study stated that officials are substantially less willing to be in contact with the press (even in relation to unclassified matters or personal opinions) than they were even a few years ago.[261]

215.2 In South Africa a recent report by Mare found that journalists now found it "*difficult to cultivate reliable sources in various spheres of local, provincial and national government for fear of being surveilled by the security apparatuses*."[262] Mare's subjects revealed that technology was now something that was feared rather than celebrated since "*while the mobile phone was generally hailed as a tool which has brought efficiency and effectiveness to the journalism profession, it has brought them into the 'dragnet'*".[263]

215.3 Journalists interviewed by Mare revealed that various strategies have been adopted in order to circumvent communication surveillance, including: end-to-end encryptions email and messaging tools, coded language (with sources), face-to-face communication; and drop-off (people come and drop off documents at newsroom reception).[264]

---

[260] Human Rights Watch, 'With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy' (2014) <https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and>

[261] Ibid at 3

[262] Admire Mare "A qualitative analysis of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa" *Media Policy and Democracy Project*, March 2016, at 26 <http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/duncan_2_comm_surveillance.pdf>.

[263] Ibid at 26

[264] Ibid at 27- 28

Duncan also notes, for instance, that in an attempt to protect sources some journalists will carry two phones:

> *"one with a SIM card that has been registered in terms of* RICA *and one with a card that has been registered by someone other than themselves. "Pre-RICA'd" SIM cards – SIM cards that are registered before they are bought – can be bought fairly easily in South Africa, and cannot be traced back to their users as they are not registered in their names."*[265]

216 Surveillance unquestionably has a chilling effect on the media. In summary – surveillance of journalists may have a chilling effect upon sources coming forward and therefore affects access to crucial information for journalists. The Supreme Court of Appeal has recently held:

> *"Access to information is crucial to accurate reporting and thus to imparting accurate information to the public. Interference with the ability to access information impedes the freedom of the press. The right to freedom of expression is not limited to the right to speak, but includes the right to receive information and ideas. Preventing the press from reporting fully and accurately, does not only violate the rights of the journalist, but it also violates the rights of all the people who rely on the media to provide them with 'information and ideas."*[266]

The limitations analysis

217 The current threshold for granting applications against journalists or lawyers under RICA fails to meet the less-restrictive means requirement.[267] The state needs to demonstrate that less-restrictive means would not achieve the purpose of the provision. A higher threshold for granting the applications necessarily implies a lesser restriction on the rights to privacy and freedom of expression. Even if the court were to be persuaded that the threshold for granting applications in relation to ordinary subjects meets constitutional muster

---

[265] J Duncan 'Communications surveillance in South Africa: The case of the Sunday Times newspaper' at 224

[266] *Nova Property Group Holdings v Cobbett* [2016] ZASCA 63 at para 37

[267] Under section 36(e) of the Constitution

– the threshold in relation to journalists and lawyers should still be higher in order to avoid the disastrous consequences outlined by Mare:

> *"The Crime Intelligence Division of the South African Police Service (SAPS) also took advantage of the low threshold of targeted surveillance as set out in* RICA *to obtain judicial approval to intercept the mobile phones of two Sunday Times journalists (Stephan Hofstätter and Mzilikazi wa Afrika) in 2010 by giving fictional names and suggesting such interception was needed to investigate a criminal syndicate. Subsequently, the Sunday Times took the case to court and two officers were charged with violations of* RICA*. This incident has fueled fears that other applications to tap the communications of journalists and public figures may have been granted under false pretences."*[268]

218 Indeed, the respondents' contentions on the papers support the relief sought by the applicants.

218.1 The respondents claim that the designated judge has a discretion to take the fact than an application affects journalists into account or specify conditions or impose restrictions relating to the interception of communications.[269] There is no basis for that claim under the Act. Nor any indication about what those conditions should be.

218.2 The joint respondents concede that "*the fact that the subject of the interception is a journalist must be brought to the attention of the designated judge*".[270]

218.3 The joint respondents accept that it is legally significant and must be disclosed to the designated judge.[271]

---

[268] Mare at 19

[269] RA p 674 para 151

[270] RA p 792 para 122

[271] RA p 1021 para 100

219 But there is nothing in RICA that requires an applicant to disclose whether a person affected by the interception direction is a journalist or lawyer. Both arguments support the applicants' contention that there should be a higher threshold where an interception direction is going to be granted against journalists and lawyers.

Remedy on the fourth challenge

220 We submit that the fourth challenge is again one in respect of which an interim reading-in order can be crafted while Parliament resolves the matter more permanently.

221 Therefore, the appropriate order is as follows:

> *"It is declared that:*
>
> *(a) Sections 16(5), 17(4), 19(4), 21(4)(a), 22(4)(b) of RICA are inconsistent with the Constitution and accordingly invalid to the extent that they deal with an application related to a subject who is a journalist or a lawyer;*
>
> *(b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and*
>
> *(c) Pending the enactment of legislation to cure the defect, RICA shall be deemed to include an additional section 16A, which provides as follows:*
>
> > *"16A Where an order in terms of sections 16(5), 17(4), 19(4), 21(4)(a), 22(4)(b) is sought against a subject who is a journalist or practising legal practitioner:*
> >
> > *(a) The application for the order concerned must disclose and draw to the designated judge's attention that the subject is a journalist or practising legal practitioner;*
> >
> > *(b) The designated judge shall only grant the order sought if satisfied that the order is necessary and appropriate, notwithstanding the fact that the subject is a journalist or practising legal practitioner; and*

> *(c) If the designated judge grants the order sought, the designated judge may include such further limitations or conditions and he or she considers necessary in view of the fact that the subject is a journalist or practising legal practitioner."*

FIFTH CHALLENGE – BULK & FOREIGN SIGNALS SURVEILLANCE

222 This leaves us with the fifth and final challenge. This concerns the bulk surveillance and foreign signal surveillance that (it is common cause) are taking place – without any regulation by RICA.

223 As set out above, in South Africa, the general position is that the surveillance of communications and meta-data is prohibited. RICA provides a legal framework for targeted surveillance — that is: separate, particular applications to surveil particular subjects. RICA, however, makes no provision for general bulk/mass surveillance of the public.

The nature of the problem

224 It is trite that the exercise of all public power must comply with the Constitution and principle of legality;[272] and organs of state may only perform functions and exercise powers conferred on them by law.[273] Where an organ of state fails do so then its conduct is *ultra vires* and unconstitutional.[274]

---

[272] *Fedsure Life Assurance Ltd & Others v Greater Johannesburg Transitional Metropolitan Council & Others* 1999 (1) SA 374 (CC)

[273] *President of the Republic of South Africa and Others v South African Rugby Football Union and Others* 2000 (1) SA 1 (CC); 1999 (10) BCLR 1059 (CC) at para 48

[274] *Pharmaceutical Manufacturers Association of South Africa and Another: In re Ex Parte President of the Republic of South Africa and Others* 2000 (2) SA 674 (CC) at para 20

225 Therefore, if a form of surveillance is being carried out, but RICA (or some other legislative provision) does not provide the statutory power to do so, then it is unlawful and unconstitutional.

226 We emphasise that only the joint respondents deal with the challenges relating to bulk surveillance and foreign signals surveillance. The joint respondents have confirmed that bulk surveillance and foreign signals surveillance are taking place.[275]

227 The applicants therefore make two submissions, in the alternative:

227.1 First, the bulk surveillance and/or foreign signals surveillance that has taken place is *ultra vires* the statutory provisions that the joint respondents seek to rely on. Accordingly, no bulk surveillance and/or foreign signals surveillance may lawfully take place until new legislation is enacted which incorporates sufficient safeguards.

227.2 In the alternative, and only in the event that this Court finds that RICA and/or the National Strategic Intelligence Act 39 of 1994 do empower bulk surveillance and/or foreign signals surveillance, then the applicants submit that RICA and/or the NSIA are unconstitutional for their failure to provide any statutory safeguards for these invasive forms of surveillance.

[275] Joint AA p 799 para 143

Primary submission – bulk surveillance and foreign signals surveillance are ultra vires

228 Bulk or mass surveillance is the ongoing monitoring, recording and storage of communications of large sections of the population.[276] The joint respondents claim that the applicants have "*misconstrued the nature and purpose of 'bulk surveillance*'".[277] It summarises bulk surveillance as follows:

> *"Bulk surveillance is an internationally accepted method of strategically monitoring transnational signals, in order to screen them for certain cue words or key phrases. The national security objective is to ensure that the State is secured against transnational threats.*
> *It is basically done through the tapping and recording of transnational signals, including, in some cases, undersea fibre optic cables."*[278]

229 Foreign Signals Intelligence, according to the joint respondents refers to:

> *"intelligence obtained from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals. It also includes any communication that emanates from outside the borders of the Republic (in this case, South Africa) and passes through or ends in the Republic"*[279]

230 Importantly, as the applicants explain in the affidavits before this Court – the 'foreign signals' in certain instances may well be communications between two South African citizens: the interception of communications that flow through services such as Gmail, Yahoo! Whatsapp and Skype, where the servers of the particular company are located outside of the Republic, are not regulated by any law (even if both the sender and the receiver are in South Africa).[280]

---

[276] FA p 64 para 139

[277] Joint AA p 794 para 129

[278] Joint AA p 795 paras 130 -131

[279] Joint AA p 795 para 132

[280] FA p 74 para 155

231 The applicants set out various other allegations of abuse by the NCC in relation to bulk surveillance in their papers.[281]

231.1 The United Nations Human Rights Committee stated in recent Concluding Observations regarding South Africa's surveillance regime that it was concerned about allegations of illegal mass surveillance taking place in South Africa.[282]

231.2 Right2Know — the amicus in this matter, is a respected South African NGO dealing with information law and freedom of expression — and has noted that:

> *"The 2008 Matthews Commission found that the intelligence agencies were doing bulk monitoring through a second facility called the National Communications Centre (NCC) without any legal oversight."*[283]

232 The joint respondents maintain their stance in their answering affidavit: that the Agency "*indeed conducts lawful bulk interception*". The joint respondents claim

---

[281] FA p 64 para 141; see also "SPS 14" a copy of the Inspector-General's Report relating to Mr Saki Macozoma.

[282] United Nations Human Rights Committee, 'Concluding Observations on the Initial Report of South Africa', 3258th mtg, CCPR/C/ZAF/CO/1, 23 March 2016, [42] <http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en>. Paragraphs 42 and 43 deal with the right to privacy and interception of private communications.

[283] Right2Know, 'Big Brother Exposed, Activists Handbook: Stories of South Africa's Intelligence Structures Monitoring and Harassing Activist Movements' (Report, Right2Know) <http://bigbrother.r2k.org.za/wp-content/uploads/Big-Brother-Exposed-R2K-handbook-on-surveillance-web.pdf>.

The Matthews Commission was a commission of inquiry established in 2006 by the erstwhile Minister of Intelligence Services, Ronnie Kasrils. The Commission was officially named the Ministerial Review Commission on Intelligence and became known as the Matthews Commission as it was chaired by Joe Matthews (a former deputy Minister). The Commission's mandate was, inter alia, examining whether and to what extent the intelligence services in South Africa were infringing constitutional rights, as well as to strengthen oversight mechanisms in order to minimise the potential for abuses of power. A copy of the Commission's Report can be found at Right2Know, *The Matthews Commission, the GILAB, and Why We're Worried About SA's Spies* (11 February 2013) <www.r2k.org.za/2013/02/11/matthews-commission-gilab-south-africa-spies/> in which the Commission identified various aspects of the intelligence services over which there was insufficient oversight to prevent abuses of power and infringements of constitutional rights.

that they are empowered to do so in terms of RICA read with section 2 of the National Strategic Intelligence Act 39 of 1994 ("the NSIA").[284]

233 But the provisions they rely upon do nothing of the sort. The long title of the NSIA provides:

> *"To define the functions of members of the National Intelligence Structures; to establish a National Intelligence Co-ordinating Committee and to define its functions in respect of intelligence relating to the security of the Republic; and to provide for the appointment of a Co-ordinator for Intelligence as chairperson of the National Intelligence Co-ordinating Committee, and to define his or her functions; and to provide for matters connected therewith."*

234 Section 2 of the National Strategic Intelligence Act provides:

> *"**2 Functions relating to intelligence***
>
> *(1) The functions of the Agency shall, subject to section 3, be-*
>
> *(a) to gather, correlate, evaluate and analyse domestic and foreign intelligence (excluding foreign military intelligence), in order to-*
> *(i) identify any threat or potential threat to national security;*
> *(ii) supply intelligence regarding any such threat to Nicoc;*
>
> *(b) to fulfil the national counter-intelligence responsibilities and for this purpose to conduct and co-ordinate counter-intelligence and to gather, correlate, evaluate, analyse and interpret information regarding counter-intelligence in order to-*
> *(i) identify any threat or potential threat to the security of the Republic or its people;*
> *(ii) inform the President of any such threat;*
> *(iii)supply (where necessary) intelligence relating to any such threat to the South African Police Service for the purposes of investigating any offence or alleged offence; and*
> *(iv) supply intelligence relating to any such threat to the Department of Home Affairs for the purposes of fulfilment of any immigration function; and*
> *(ivA) supply intelligence relating to any such threat to any other department of State for the purposes of fulfilment of its departmental functions; and*
> *(v) supply intelligence relating to national strategic intelligence to Nicoc;*

[284] Joint AA p 798 para 141, p 799 para 143

(c) to gather departmental intelligence at the request of any interested department of State, and, without delay to evaluate and transmit such intelligence and any other intelligence at the disposal of the Agency and which constitutes departmental intelligence, to the department concerned and to Nicoc.

(2) It shall, subject to section 3, also be the functions of the Agency-

(a) to gather, correlate, evaluate and analyse foreign intelligence, excluding foreign military intelligence, in order to-

(i) identify any threat or potential threat to the security of the Republic or its people;

(ii) supply intelligence relating to any such threat to Nicoc;

(b) in the prescribed manner, and in regard to communications and cryptography-

(i) to identify, protect and secure critical electronic communications and infrastructure against unauthorised access or technical, electronic or any other related threats;

(ii) to provide crypto-graphic and verification services for electronic communications security systems, products and services used by organs of state;

(iii) to provide and coordinate research and development with regard to electronic communications security systems, products and services and any other related services;

(c) to liaise with intelligence or security services or other authorities, of other countries or inter-governmental forums of intelligence or security services;

(d) to train and support users of electronic communications systems, products and related services;

(e) to develop, design, procure, invent, install or maintain secure electronic communications systems or products and do research in this regard; and

(f) to cooperate with any organisation in the Republic or elsewhere to achieve its objectives.

(2A) When performing any function referred to in subsection (2) (b) the Agency is exempted from any licensing requirement contemplated in-

(a) the Broadcasting Act, 1999 (Act 4 of 1999); and
(b) the Electronic Communications Act, 2005 (Act 36 of 2005).

(3) It shall be the function of the South African Police Service, subject to section 3-

(a) to gather, correlate, evaluate, co-ordinate and use crime intelligence in support of the objects of the South African Police Service as contemplated in section 205 (3) of the Constitution;

(b) to institute counter-intelligence measures within the South African Police Service; and
(c) to supply crime intelligence relating to national strategic intelligence to Nicoc.

(4) The National Defence Force shall, subject to section 3-

(a) gather, correlate, evaluate and use foreign military intelligence, and supply foreign military intelligence relating to national strategic intelligence to Nicoc, but the National Defence Force shall not gather intelligence of a non-military nature in a covert manner;

(b) gather, correlate, evaluate and use domestic military intelligence excluding covert collection, except when employed for service as contemplated in section 201 (2) (a) of the Constitution and under conditions set out in section 3 (2) of this Act, and supply such intelligence to Nicoc; and

(c) institute counter-intelligence measures within the National Defence Force."

235 The joint respondents have not even attempted to explain how these provisions empower them to undertake bulk or foreign signals surveillance. However, and fatally for the respondents, section 2A(5) provides:

"The relevant members of the National Intelligence Structures may, in the prescribed manner, gather information relating to-
(a) criminal records;
(b) financial records;
(c) personal information; or
(d) any other information which is relevant to determine the security clearance of a person:

Provided that where the gathering of information contemplated in paragraphs (c) and (d) requires the interception and monitoring of the communication of such a person, the relevant members shall perform this function in accordance with the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002".
(Emphasis added)

236 Thus, gathering of information that requires interception and monitoring relating to any personal information expressly requires the provisions of RICA to be complied with. However, RICA is not designed to surveil the general populous – it only provides a regime for targeted surveillance upon individual applications that are approved by the designated judge.

237 Indeed, the joint respondents even concede that "*bulk surveillance is not directed at individuals*".[285] Once that is so, then it cannot be that RICA is the empowering statute.[286] The joint respondents admit that the two forms of surveillance are distinct with different purposes.[287]

238 The joint respondents do not isolate or identify the particular provisions in RICA that empower them to conduct these forms of surveillance. We submit that this is because there is no such provision in RICA. Even the most generous contextual reading of RICA cannot ignore the language used in the provisions.[288]

239 It follows that there is no applicable statutory regime raised by the joint respondents. It follows that these forms of surveillance are *ultra vires* and unlawful. The danger is that the applicants' understanding is that when the respondents carry out these forms of surveillance they do so without any

---

[285] RA p 1073 at 187.2

[286] RA p 1073 at 187.2

[287] RA p 1073 at para 187.2

[288] *The City of Tshwane Metropolitan Municipality v Blair Atholl Homeowners Association* [2018] ZASCA 176 (3 December 2018) at para 64

statutory framework whatsoever and accordingly there are no safeguards whatsoever employed in order to protect the rights of citizens.[289]

Alternative submission – the lacunae in RICA are unconstitutional

240 In *My Vote Counts*, the applicants alleged that Parliament had failed to fulfil a constitutional obligation because information on private funding of political parties was required to exercise the constitutional right to vote under section 19(3) of the Constitution and Parliament had not passed legislation that gives effect to the right of access to this information under section 32(2) of the Constitution.[290]

241 *My Vote Counts* argued that PAIA was not the only legislation that gave effect to section 32 and referred to various other pieces of legislation that made provision for access to information.[291]

242 The Constitutional Court found that PAIA is the national legislation contemplated in section 32(2) of the Constitution and should have been challenged.[292] While other pieces of legislation do make provision for access to information, the main focus was some other subject, where the right of access to information was "touched on" in a sparse manner – incidental to the legislation's main focus.[293]

---

[289] RA p 1074 para 187.2

[290] *My Vote Counts*, minority judgment of Cameron J at para 2

[291] *My Vote Counts*, majority judgment at para 149

[292] *PFE International Inc (BVI) and Others v Industrial Development Corporation of South Africa Ltd* 2013 (1) SA 1 (CC) at para 4; see also *Koalane and Another v Senkhe and Others* [2012] ZAFSHC 165 at para 7

[293] *My Vote Counts*, majority judgment at para 149

243 We submit that RICA is the legislation intended to regulate interception and monitoring. Accordingly, to the extent that this Court finds that RICA and/or the NSIA do empower the respondents to undertake bulk and/or foreign signals surveillance, then the applicants submit that these provisions are unconstitutional on the basis that they fail to set out any coherent regime or safeguards to protect significant limitations of the right to privacy.

244 Section 199 of the Constitution provides in relevant part:

> *"(4) The security services must be structured and regulated by national legislation.*
> *(5) The security services must act, and must teach and require their members to act, in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic.*
> *(6) No member of any security service may obey a manifestly illegal order."*

245 Chapter 11 of the Constitution, headed 'Security Services' provides:

> *"Establishment and control of intelligence services*
>
> *209. (1) Any intelligence service, other than any intelligence division of the defence force or police service, may be established only by the President, as head of the national executive, and only in terms of national legislation.*
>
> *(2) The President as head of the national executive must appoint a woman or a man as head of each intelligence service established in terms of subsection (1), and must either assume political responsibility for the control and direction of any of those services, or designate a member of the Cabinet to assume that responsibility.*
>
> *…*
> *Powers, functions and monitoring*
>
> *210. National legislation must regulate the objects, powers and functions of the intelligence services, including any intelligence division of the defence force or police service, and must provide for—*
>
> *(a) the co-ordination of all intelligence services; and*
> *(b) civilian monitoring of the activities of those services by an inspector appointed by the President, as head of the national executive, and*

approved by a resolution adopted by the National Assembly with a supporting vote of at least two thirds of its members."

246 "[I]ntercept" in section 1 of RICA means:

> *"the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the-*
>
> *(a) monitoring of any such communication by means of a monitoring device;*
> *(b) viewing, examination or inspection of the contents of any indirect communication;*
> *and*
> *(c) diversion of any indirect communication from its intended destination to any other destination".*

247 The prohibition of interception of communications in section 2 of RICA is broadly framed:

> *"Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."*

248 The applicants submit that RICA's prohibition makes it clear that if bulk surveillance and/or foreign signals surveillance is to take place then it must take place in accordance with RICA. Thus, while RICA – like PAIA – provides a '*once-off upon request*' regime, it may still be constitutionally vulnerable for failing to provide a legislative regime for bulk and/or foreign signals surveillance to take place.[294]

249 On this score, in *Mazibuko v Sisulu*,[295] the Constitutional Court held that:

---

[294] *My Vote Counts*, majority judgment at para 128

[295] *Mazibuko v Sisulu and Another* 2013 (6) SA 249 (CC)

> *"where legislation has been enacted to give effect to a right, a litigant should rely on that legislation in order to give effect to the right or alternatively challenge the legislation as being inconsistent with the Constitution."*

250 Similarly:

> *"[i]n our view, a reading of the Rules as a whole reveals that there is indeed a lacuna in the Rules regulating the decision-making and deadlock-breaking mechanism of the Programme Committee charged with the power to arrange the programme of the Assembly. To the extent that the Rules regulating the business of the Programme Committee do not protect or advance or may frustrate the rights of the applicant and other members of the Assembly in relation to the scheduling, debating and voting on a motion of no confidence as contemplated in section 102(2), they are inconsistent with section 102(2) and invalid to that extent."*[296]

251 Thus, to the extent that this Court finds that RICA and/or the NSIA do empower the respondents to undertake bulk and/or foreign signals surveillance, then the applicants submit that these provisions are unconstitutional because the provisions plainly and significantly limit constitutional rights but the respondents have failed to explain how these provisions operate in practice or satisfy the requirements of the limitations clause. We submit that it follows, in the alternative, that these provisions are unconstitutional (as they fail to set out any coherent regime or safeguards to protect significant limitations of the right to privacy).

Remedy on the fifth challenge

252 The applicants' primary argument is that the government is not empowered to carry out these forms of surveillance and accordingly this Court should declare that it may not do so.

---

[296] *Mazibuko v Sisulu* at para 61

252.1 The state would need to enact empowering legislation and provide sufficient safeguards which alleviate the significant limitations on each member of the public's right to privacy.

252.2 In that event the order granted should be:

> *"It is declared that the bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid."*

253 The applicants' alternative argument is that the RICA and the NSIA are unconstitutional for their failure to provide any statutory safeguards for these invasive forms of surveillance. In that event, the order granted should be:

> *"It is declared that:*
>
> *(a) RICA and the National Strategic Intelligence Act 39 of 1994 are inconsistent with the Constitution and invalid to the extent that they fail to regulate properly or at all "bulk surveillance" and foreign signals interception undertaken by state officials, including by the National Communications Centre; and*
>
> *(b) The bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid."*

POSSIBLE AMENDMENTS TO RICA ARE NO BAR TO THIS APPLICATION

254 Lastly, the Deputy Minister of Justice has filed an affidavit contending that RICA is presently being reviewed by Parliament. Accordingly, so the argument goes, this Court should not determine whether RICA is unconstitutional because separation of powers demands that this Court should leave it to the executive and Parliament to fix RICA if and where they deem it appropriate to do so.[297]

---

[297] RA p 984 para 15.2.1

255 There are four reasons why the Deputy Minister's argument is incorrect.

256 First, the fact that RICA may be reviewed in the future is no bar to this Court making a declaration of invalidity. In *Mazibuko v Sisulu*[298] the Constitutional Court rejected substantially similar contentions regarding the National Assembly's rules. The majority of the Court held:

> *"[67] … [The Speaker] also argued that there was no need for this Court to make an order even if it found for the applicant on the lacuna in the Rules because the Assembly was reforming its Rules to correct the defect. He in effect argued that the exercise of jurisdiction would offend the separation of powers doctrine in light of the ongoing negotiations within the Assembly.*
>
> *[69] … [T]here are fundamental differences between the applicant and Chief Whip on whether the Rules are constitutionally deficient and therefore what the Rules should provide for in relation to a motion of no confidence in the President. If this dispute is not resolved by this Court, the differences are likely to persist, to the detriment of a member of the Assembly who wishes to exercise the right envisaged in section 102(2).*
>
> *[70] I am therefore unable to agree with the contention of the Speaker that because the parties are in the process of remedying the alleged lacuna in the Rules the direct access application should be dismissed. First, the differences between the applicant and Chief Whip make it most improbable that the lacuna will be corrected. Second, once we have found, as we have, that the Rules regulating the business of the Programme Committee are unconstitutional, we must so declare. An order of constitutional invalidity is not discretionary. Once the Court has concluded that any law or conduct is inconsistent with the Constitution, it must declare it invalid.'*[299]

257 Second, the applicants seek declaratory relief. There is no intrusion into the separation of powers. In *Mazibuko v Sisulu* the Constitutional Court held:

> *"An order of constitutional invalidity would not be invasive because it is declaratory in kind. The Court would not be formulating Rules for the Assembly. The Court would be properly requiring the Assembly to*

---

[298] *Mazibuko v Sisulu* at paras 67 – 70

[299] Section 172(1)(a) of the Constitution

remedy the constitutional defect that threatens the right of members of the Assembly".[300]

258 Third, the respondents start from the premise that RICA in its present form is constitutional.[301] The Deputy Minister claims that RICA should be reviewed because of 'technological advances' that might have left the legislation out of step.[302] Indeed, the Deputy Minister states:

> *"Over the period of 15 years since its promulgation, the balance between using the RICA as an effective tool to fight crime, and the related limitation on a person's right to privacy, may very well have shifted unfavourably towards the limitation of a person's privacy".*[303]

258.1 The respondents have not even pleaded, let alone adequately explained, the bases upon which RICA is being reviewed and what features should be "*updated*". There is no evidence that the review process will address the defects highlighted by the applicants, either at all – or sufficiently.

258.2 By contrast, it will benefit Parliament and the public to have a judicial assessment of what is constitutionally permissible *before* more time is spent finalising and publishing draft legislation for public comment.

259 Fourth, these proceedings were launched in April 2017.[304] There have not been any new Bills published dealing with RICA since this litigation began. There is also no indication regarding how long the review process would likely take before any amendments would be law.

---

[300] *Mazibuko v Sisulu* at para 71

[301] Deputy Minister of Justice's AA at p 734F paras 8 – 9

[302] Deputy Minister of Justice's AA at p 734F paras 9 – 12

[303] Deputy Minister of Justice's AA at p 734F para 11

[304] FA p 1

COSTS AND CONCLUSION

260 For the reasons set out above, the applicants submit that RICA is unconstitutional and invalid in the respects identified above. We attach a draft order, which consolidates all of the orders explained and set out above.

261 In accordance with the principles of *Biowatch,*[305] if the applicants succeed, they are entitled to an order for costs. Given the complexity of the matter and the voluminous nature of the papers we submit that it would be appropriate for the order to include the costs of three counsel, where three counsel have been employed.

STEVEN BUDLENDER

STUART SCOTT

ITUMELENG PHALANE

Counsel for the applicants

Chambers, Sandton

11 February 2019

[305] *Biowatch Trust v Registrar, Genetic Resources, and Others* 2009 (6) SA 232 (CC) at paras 21-25

IN THE HIGH COURT OF SOUTH AFRICA

GAUTENG DIVISION, PRETORIA

CASE NO: 25978/17

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 THE 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
MINISTER OF TELECOMMUNICATIONS AND POSTAL SERVICES	Eleventh Respondent

---

APPLICANTS' DRAFT ORDER

---

1. It is declared that:

    (a) RICA, including sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe procedure for notifying the subject of the interception;

    (b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and

    (c) Pending the enactment of legislation to cure the defect, RICA is deemed to read to include the following additional sections 16(11) and (12):

        "(11) The applicant that obtained the interception direction shall, within 90 days of its expiry, notify in writing the person who was the subject of the interception and shall certify to the designated judge that the person has been so notified.

        (12) The designated judge may in exceptional circumstances and on written application made before the expiry of the 90-day period referred to in sub-section (11), direct that the obligation referred to in sub-section (11) is postponed for a further appropriate period, which period shall not exceed 180 days."

2. It is declared that:

    (a) RICA, including sections 16(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to provide for a system for a public advocate or other appropriate

safeguards to deal with the fact that the orders in question are granted ex parte; and

(b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect;

(c) RICA, including the definition of "designated judge" in section 1, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe an appointment mechanism and terms for the designated judge which ensure the designated judge's independence;

(d) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and

(e) With effect from six months after the date of this order and pending the enactment of legislation to cure the defect, “designated judge” in RICA shall be deemed to read as follows:

“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 <u>appointed by the Judicial Service Commission for a non-renewable term of two years</u> to perform the functions of a designated judge for purposes of this Act”.

3. It is declared that:

(a) RICA, including section 37 thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to

prescribe the proper procedure to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions;

(b) Section 30(2)(a)(iii) of RICA is inconsistent with the Constitution and accordingly invalid; and

(c) The declarations of invalidity are suspended for two years to allow Parliament to cure the defects.

4. It is declared that:

(a) Sections 16(5), 17(4), 19(4), 21(4)(a), 22(4)(b) of RICA are inconsistent with the Constitution and accordingly invalid to the extent that they deal with an application related to a subject who is a journalist or a lawyer;

(b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and

(c) Pending the enactment of legislation to cure the defect, RICA shall be deemed to include an additional section 16A, which provides as follows:

"16A Where an order in terms of sections 16(5), 17(4), 19(4), 21(4)(a), 22(4)(b) is sought against a subject who is a journalist or practicing legal practitioner:

(a) The application for the order concerned must disclose and draw to the designated judge's attention that the subject is a journalist or practicing legal practitioner;

(b) The designated judge shall only grant the order sought if satisfied that the order is necessary and appropriate, notwithstanding the fact that the subject is a journalist or practicing legal practitioner; and

(c) If the designated judge grants the order sought, the designated judge may include such further limitations or conditions and he or she considers necessary in view of the fact that the subject is a journalist or practicing legal practitioner."

5. It is declared that:

(a) The bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid; and

(b) RICA and the National Strategic Intelligence Act 39 of 1994 are inconsistent with the Constitution and invalid to the extent that they fail to regulate properly or at all "bulk surveillance" and foreign signals interception undertaken by state officials, including by the National Communications Centre.

6. The first, second, fourth, fifth, seventh, eighth, and tenth respondents are ordered, jointly and severally, to pay the applicants' costs, including the costs of three counsel, where three counsel have been employed.