IN THE HIGH COURT OF SOUTH AFRICA

(GAUTENG DIVISION, PRETORIA)

Case number: 25978/17

In the matter between:

AMABHUNGANE CETRE 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 OF 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

---

PRINCIPAL SUBMISSIONS MADE ON BEHALF OF THE

2ND, 7TH, 8TH & 10TH RESPONDENTS

TABLE OF CONTENTS

A. THE ISSUE

1. This application, based on what appears to be a misconception of the purpose of the Regulation of Interception of Communication and Provision of Communication-Related Information Act 70 of 2002 ("RICA"), seeks to have certain provisions of RICA set aside on the basis that they are unconstitutional.

2. As one of its contentions, the applicants, while accepting that interception is an acceptable mechanism for national security[1], propose that the target of interception must be given notice of surveillance after it has been conducted. They seem to accept that pre-surveillance notice would defeat the very purpose of the legislative measure. But what a post-surveillance notice would achieve is hard to imagine. The applicants seem to suggest that it would enable the target of the surveillance to challenge a surveillance order that would have been unlawfully granted. But by then the question is academic and, in any event, surveillance for national security purposes is ordinarily not an event that starts and ends within a determinable time frame but tends to be an ongoing pursuit depending on the complexity of the dots that Intelligence Services need to join at any given period.

3. RICA regulates the interception of certain communications. Recognizing that interception amounts to some limitation of the right to privacy, RICA provides

---

1 Bundle, p, Founding Affidavit, para 12

various safeguards to ensure that such limitation is consistent with section 36 of the Constitution. It regulates the making of applications for, and the issuing of, directions authorising such interception.

4. At the outset, it is important to state that RICA provides for various safeguards to ensure that an appropriate balance is struck between the need to ensure national security and the right of citizens to privacy. These safeguards include the fact that no interception of communication is conducted without an application to a designated judge. They also include rigorous internal scrutiny conducted by the Agency's legal officers prior to an application for an interception. Section 16(2) of RICA sets out all the requirements that must be complied with when an application for interception is made. In addition, section 16(5) sets out high threshold criteria (or jurisdictional facts) that must be met in order to satisfy the designated judge that the intended interception is indeed consistent with the Bill of Rights.

5. Notwithstanding the safeguards inherent in RICA, the applicants challenge certain provisions of RICA and to some extent the National Strategic Intelligence Act, 39 of 1994 ("the NSIA") on the grounds that they are inconsistent with the Constitution of the Republic of South Africa Act, 108 of 1996 (**"the Constitution"**) in form, procedure and content.

6. This application is opposed as it is, with respect, ill-conceived and based on a misunderstanding of the relevant legislation. The grounds upon which it is based arise from a misunderstanding of the safeguards already contained in RICA.

7. Strikingly, the application calls for special treatment of journalists as distinct from the rest of society, thus requiring some form of higher standard for the surveillance of journalists and lawyers, or their exemption from the reasonable legislative mechanisms aimed at ensuring national security. This, we respectfully submit, is an instance of a misunderstanding of the applicable principles and standard. Not since the so-called "Sobukwe Clause" in 1963 has legislation been enacted specifically for an individual. Not since the dark days of repression in South Africa has legislation of general application been enacted to give special privileges to a section of society. There is no rational basis for the special privileges that the applicants want this Court to confer upon journalists and lawyers as there are sufficient safeguards in RICA and other laws to protect privileged and confidential information.

8. In any event, we shall show that this application is premature and seeks to involve the courts in matters that are policy-laden and fall outside judicial proficiency and, with respect, competence. The courts have no business second-guessing government policy on intelligence gathering for purposes of national security. The Constitutional Court has drawn a distinction between policy matters or considerations on the one hand, which fall outside the courts' reach,

and the implementation of policy matters on the other, which fall within the courts' competence. The applicants' attack focuses on policy matters in the realm of intelligence gathering for national security purposes. Such matters are, with respect, not within the proficiency of the Courts. The Constitutional Court, no less, has said so.

B. THE RELIEF SOUGHT

9. The applicants seek an order declaring:

9.1. Sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) of RICA to be inconsistent with the Constitution and accordingly invalid to the extent that they fail to prescribe procedure for notifying the subject of the interception direction (**"the first challenge"** – notification to the subject of an interception direction)[2];

9.2. The definition of "designated judge" in section 1 of RICA to be inconsistent with the Constitution and 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 (**"the second challenge"** – independence of the designated judge)[3];

---

2 Bundle, p 2, prayer 1.1
3 Bundle, p 2, prayer 1.4

9.3.

9.3.1. Section 37 of RICA to be 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 the interceptions[4];

9.3.2. Section 30(2)(a)(iii) of RICA to be inconsistent with the Constitution and accordingly invalid[5];

(**"the third challenge"** – safeguards regarding data obtained)

9.4. Section 16(5), 17(4), 19(4), 21(4)(a), 22(4)(b) of RICA to be 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 (**"the fourth challenge"** – the question of legal privilege and the confidentiality of journalists' sources)[6];

9.5.

7.5.1 RICA and the NSIA to be inconsistent with the Constitution and invalid to the extent that they fail to regulate properly or at all "bulk

---

4 Bundle, p 2, prayer 1.2
5 Bundle, p 2, prayer 1.3
6 Bundle, p 3, prayer 1.5

surveillance" and foreign signals interception undertaken by state officials, including by the National Communications Centre;[7] and

7.5.2 The bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre to be unlawful and invalid.[8]

(**"the fifth challenge"** – bulk & foreign signals surveillance)

C. SUMMARY OF BASES FOR OPPOSITION

10. The relief sought by the applicants is opposed on the following bases:

10.1. The application is **premature** because RICA is currently under review in respect of, among other things, **"the need to enhance governance, transparency and accountability mechanisms"**. These are the issues that form the basis for the applicants' complaint.

10.2. The courts should be slow to second-guess government's **policy-laden decisions** that do not infringe upon citizens' constitutional rights unwarrantedly.

---

7 Bundle, p 3, prayer 1.6
8 Bundle, p 3, prayer 1.7

10.3. The **jurisdictional facts** that an applicant must meet provide adequate safeguards against abuse of interception and other powers for which RICA provides.

10.4. In respect of **the first challenge** (notification to the subject of an interception direction), the applicants accept that prohibiting pre-surveillance notification is a justifiable limitation of the rights involved[9] but contend that there is no justification for the subject of an interception not to be notified after the surveillance has taken place. We respectfully submit that the applicants fail to appreciate that the nature of intelligence gathering is a process, not an event that starts and ends within a determinable time frame or that necessarily produces fool-proof results. Interception is necessitated by the demands of national security, is a measure of last resort and is done after leave has been obtained from a designated judge. The information gathered, if unassailable, ultimately assists in neutralising, pre-emptively or contemporaneously, threats to the security of the Republic and all her people. The designated judge has the institutional judgment and competence, as well as the statutory authority, to interrogate any perceived or unwarranted deviations that are inconsistent with the powers accorded to these intelligence services.

---

9 Applicants' HoA, p 37, para 86

10.5. As regards **the second challenge** (independence of the designated judge), the applicants raise two issues. First, they allege that RICA fails to secure the independence of the designated judge. Second, they allege that there is no adversarial process before the designated judge and that the other side of the case is never presented.

10.6. There is no merit in these contentions. Firstly, the process of applying for an interception direction is not presided over by some clerk in a government office armed with a rubber stamp and a political party membership card. It is a rigorous process that is validated by the institutional independence of the Designated Judge who performs a quasi-judicial function, is independent and impartial in his or her application of the law, and is appropriately qualified for such appointment. Secondly, the fact that the Designated Judge is appointed by the Minister without a Judicial Service Process does not detract from his or her independence and impartiality. Judges are often appointed to head Commissions of Inquiry, or to preside over Inquiries, without undergoing the JSC process. That does not detract from their impartiality or independence. Thirdly, the fault line that runs through the applicants' support for an adversarial process is inappropriate for the environment within which intelligence services operate.

10.7. In respect of **the third challenge** (i.e. safeguards regarding data obtained), the applicants allege that the storage of personal communications limits the right to privacy and that the length of time that the communications are kept aggravates this limitation. This is an overstatement of the applicants' case. RICA provides sufficient guidelines and safeguards in this regard. The impugned provisions relating to the storing of data are intended to discover and preserve evidence. The process is secured so as to ensure that only authorised persons with the requisite security clearance are in a position to access and copy the intercepted information.

10.8. **The fourth challenge** (the question of legal privilege and the confidentiality of journalists' sources) is extraordinary. It fails to appreciate that the limitations that apply to other rights in the Bill of Rights also apply to the rights exercised by lawyers and journalists. There is no rational basis for the contention that journalists and lawyers, as a distinct group of professionals, ought to be treated differently and with less vigilance in matters of national security and the protection of citizens from threats of terrorism and other dangers. The applicants' contention in this regard is no different from a contention that priests and other religious leaders should be treated differently and with less vigilance than other members of society in matters of sexual misconduct involving children. There are many non-profit organisations whose mission is to

promote access to information rights. If lawyers and journalists are exempted from the application of RICA, why should these organisations not be exempted too? And why not medical doctors in respect of information pertaining to their patients, teachers in respect of information pertaining to their students, accountants and auditors in respect of information pertaining to their clients, and so on? The contention is, with respect, not legally sound and may lead to unforeseen consequences that will render administration of RICA unmanageable.

10.9. The essence of **the fifth challenge** (bulk & foreign signals surveillance) is that bulk and foreign surveillance is being carried out without any safeguards at all. Once again, this contention simply fails to appreciate the nature of global threats and cyber-insecurity. The development of unconventional threats to peace and stability, technological advances and the pervasiveness of cybercrimes have compelled various jurisdictions to adopt mechanisms such as bulk surveillance in an effort to secure the well-being of their inhabitants[10]. South Africa is no different. Just like other jurisdictions, South Africa has institutionalised oversight mechanisms that are intended to provide checks and balances to ensure that the intelligence services execute their mandate within constitutional bounds.

---

[10] Bundle, p 794, SSA answering affidavit, para 128

10.10. The focus of bulk surveillance is the monitoring of transnational signals. It screens certain cue words or phrases in cyber space in order to have foreknowledge of possible transnational threats.[11]

11. For the reasons fully set out below, and which are largely uncontested in the affidavits, we respectfully submit that the impugned provisions do not constitute a violation of the Constitution. The limitations that accompany such provisions are all consistent with section 36 of the Constitution, if one has regard to the nature of the rights, the extent of the limitation and the security threats such limitations seek to prevent. As we demonstrate through an account of relevant legislation, the is no basis for the challenge mounted by the applicants.

12. It is trite that where there is a limitation of a constitutional right, the limitation must be reasonable and justifiable.

D. OVERVIEW AND STRUCTURE OF THESE SUBMISSIONS

13. These submissions are structured as follows:

13.1. Firstly, we set out the relevant **constitutional and legislative framework** that governs security/intelligence services, thereby placing the impugned provisions in their proper context.

---

[11] Bundle, p 795, SSA answering affidavit, para 130

13.2. Secondly, we demonstrate that the **application is premature** and should be dismissed.

13.3. Thirdly, we summarise the nature of intelligence services in order to show that the impugned legislation governs several **policy-laden issues** which do not fall within the terrain of the judiciary and that the applicants lack the sufficient appreciation of intelligence services.

13.4. Fourthly, we demonstrate how the **high jurisdiction facts threshold** serve as adequate safeguards against abuse of the powers provided for in RICA.

13.5. Fifthly, we deal with the evidence on which the applicants rely for their challenge and the **abstract nature of this application**.

13.6. Sixthly, we deal with the **limitation of rights** and show why the limitation is in accordance with section 36 of the Constitution.

13.7. Seventhly, we address each of the **challenges** that the applicants raise and demonstrate why each one of them is unmeritorious.

13.8. Finally, we deal with **appropriate remedy**.

E. THE CONSTITUTIONAL AND LEGISLATIVE FRAMEWORK

(i) The Constitution

14. Intelligence services are constitutionally regulated and are part of the Security Services in terms of Chapter 11 of the Constitution. This is addressed more fully in the SSA's answering affidavit.[12]

15. Section 198 of the Constitution provides that:

> "198 Governing principles
>
> The following principles govern national security in the Republic:
> (a) National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life.
> (b) The resolve to live in peace and harmony precludes any South African citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.
> (c) National security must be pursued in compliance with the law, including international law.
> (d) National security is subject to the authority of Parliament and the national executive."

16. Sections 209 and 210 of the Constitution deal specifically with Intelligence Services.

---

[12] Bundle, page 747, SSA answering affidavit, paras 24-70

17. Section 209 provides that:

> "209 Establishment and control of intelligence services
>
> (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."

18. Section 210 provides that:

> "210 Powers, functions and monitoring
>
> 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 coordination 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."

(ii) <u>The National Strategic Intelligence Act, 39 of 1994 ("the NSIA")</u>

19. The NSIA sets out the functions of members of the National Intelligence Structures and establishes a National Intelligence Co-ordinating Committee.

20. Section 1 of the NSIA, defines "National Intelligence Structures" as

20.1. The National Intelligence Co-ordinating Committee (**"NICOC"**);

20.2. The intelligence division of the National Defence Force, established under the Defence Act, 2002;

20.3. The intelligence division of the South African Police Service; and

20.4. The State Security Agency (**"the Agency"**).

21. The Agency is an entity created pursuant to the government review of intelligence structures in the domestic sphere. Its functions are, inter alia,

21.1. 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; and

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

21.2. to fulfil the national counter-intelligence responsibilities and for this purpose to conduct and coordinate 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;

(iv) supply intelligence relating to any such threat to the Department of Home Affairs for the purposes of fulfilment of any immigration function;

(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;

53.3. 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.

22. The Agency is also required to

22.1. 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; and

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

22.2. 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 cryptographic 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;

22.3. to liaise with intelligence or security services or other authorities, of other countries or intergovernmental forums of intelligence or security services;

22.4. to train and support users of electronic communications systems, products and related services;

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

22.6. to cooperate with any organisation in the Republic or elsewhere to achieve its objectives.

23. "Intelligence" is defined as any information obtained and processed by a National Intelligence Structure for the purposes of informing any government decision or policymaking process carried out in order to protect or advance the national security, and includes

23.1. counterintelligence;
23.2. crime intelligence;
23.3. departmental intelligence;
23.4. domestic intelligence;
23.5. domestic military intelligence;
23.6. foreign intelligence; and
23.7. foreign military intelligence.

24. The Agency therefore performs a critical role in the country. It exists in order to ensure peace and security of the State and its citizens. It can only do this if it

functions optimally and efficiently. RICA recognizes the importance of the Agency's ability to anticipate threats through interception, but creates sufficient safeguards to avoid unnecessary intrusion into the privacy of citizens. If one has regard to the impugned provisions together with those safeguards, it is clear that interception is the **last resort**. For example, the applicant must satisfy the designated judge that

> "other investigative procedures have been applied and have failed to produce the required evidence or must indicate the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence"[13].

25. And is done in circumstances in which the Agency reasonably suspects the existence of threats to the security of the South African State and its citizens. There is no room in RICA for interception that is not permitted by RICA. Any interception outside the boundaries of RICA is an offence for which there are criminal liabilities.

26. As we demonstrate below, the threshold, or jurisdictional fact, of **"reasonable grounds to believe"** is reasonably high. It is certainly much higher than the usual threshold such as *"in the opinion of"* or *"if the judge believes"* or *"if the judge is satisfied that"*. The high threshold is itself intended to serve as a reasonable safeguard against abuse of the admittedly invasive powers for which RICA provides.

---

13 For example, an applicant must indicate

27. The Electronic Communications Security Needs Analysis Regulations, 2014 prescribe the manner in which a head of an organ of state must submit to the Agency, or his or her delegate at its request, an analysis of the electronic communications security needs of the organ of state under his or her administration.

(iii) <u>The Intelligence Services Oversight Act, 40 of 1994 ("the ISOA")</u>

28. The ISOA establishes a Parliamentary Committee to be known as the Joint Standing Committee on Intelligence (**"the Joint Standing Committee"**), which, subject to the Constitution, performs the oversight functions set out in the Act –

(a) in relation to the intelligence and counter-intelligence functions of the Services, which include the administration, financial management and expenditure of the Services; and

(b) in respect of the administration, financial management and expenditure of the Office,

and report thereon to Parliament.

29. Section 3 sets out the functions of the Joint Standing Committee which include, among other things,

29.1. to obtain from any designated judge a report regarding the functions performed by him or her in terms of RICA, including statistics regarding such functions, together with any comments or recommendations which such designated judge may deem appropriate: Provided that such report shall not disclose any information contained in an application or direction referred to in that Act;[14]

29.2. to order investigation by, and to receive a report from, the Head of a Service or the Inspector-General regarding any complaint received by the Committee from any member of the public regarding anything which such member believes that a Service has caused to his or her person or property: Provided that the Committee is satisfied that such complaint is not trivial or vexatious or made in bad faith;[15]

29.3. to refer any matter in relation to a Service or intelligence activity which comes to its attention and which it regards as relevant to the promotion of, respect for, and protection of the rights entrenched in Chapter 2 of the

---

14 See s 3(a)(iii)
15 s 3(f)

Constitution to the South African Human Rights Commission, and to receive a report from such Commission concerning the matter[16].

30. Section 5 of the ISOA provides that:

> "5 Secrecy
>
> (1) The Committee shall conduct its functions in a manner consistent with the protection of national security.
>
> (2) No person shall disclose any intelligence, information or document the publication of which is restricted by law and which is obtained by that person in the performance of his or her functions in terms of this Act, except-
> (a) to the extent to which it may be necessary for the proper administration of any provision of this Act;
> (b) to any person who of necessity requires it for the performance of any function in terms of this Act;
> (c) with the written permission of the chairperson, which permission may be given only with the concurrence of the Head of a Service and the Inspector-General;
> (d) as prescribed by regulation."

31. Section 7 deals with the appointment of an Inspector-General of Intelligence (**"the Inspector-General"**).

32. Section 7(7) sets out the functions of the Inspector-General which include investigating complaints received from members of the public on alleged maladministration, abuse of power, transgressions of the Constitution, etc.

---

16 s 3(g)

(iv) <u>The Intelligence Services Act, 65 of 2002 ("the ISA")</u>

33. The ISA regulates the establishment, administration, organisation and control of the Agency and establishes and regulates the Intelligence Council on Conditions of Service.

34. Section 10(3) provides that:

> "(3) The Director-General may, in a prescribed manner, subject to the approval of the Minister and the provisions of this Act, issue functional directives applicable to-
>
> (a) physical security;
> (b) computer security;
> (c) communication security;
> (d) protection of classified information;
> (e) .....
> (f) any other matter that is necessary for the intelligence and counter-intelligence functions of the Agency."

35. Sections 10(4) and 10(5) provide that:

> "(4) The Director-General must, as far as is reasonably practicable, take steps to ensure that-
>
> (a) national security intelligence, intelligence collection methods, sources of information and the identity of members of the Agency, are protected from unauthorised disclosure;
>
> (b) neither the Agency nor any of its members may, in the performance of their functions-
>
> (i) prejudice a political party interest that is legitimate in terms of the Constitution; or
> (ii) further, in a partisan manner, any interest of a political party; and

(c) the powers of the Agency are limited to what is necessary for the purposes of the discharge of its functions in terms of the National Strategic Intelligence Act, 1994 (Act 39 of 1994), and the Secret Services Act, 1978 (Act 56 of 1978).

(5) (a) The Director-General must at the end of each financial year submit to the Minister a report on the activities of the Agency for the relevant financial year, that must-

(i) include information about any co-operation by the Agency with an authority of another country in planning or undertaking activities pertaining to the Agency's mandate; and
(ii) except for classified information, be publicly accessible.

(b) As soon as practicable after receipt of the report contemplated in paragraph (a), the Minister must table it in Parliament."

36. Section 11 sets out the powers and duties of members.

"11 Powers and duties of members

(1) A member must, in the performance of his or her functions, obey all lawful directions received from a person having the authority to give such directions.

(2) If a designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002), is satisfied, on the grounds mentioned in a written application complying with directives issued under subsection (5), that-

(a) there is on any premises information which has or could probably have a bearing on the functions of the Agency as contemplated in section 2 of the National Strategic Intelligence Act, 1994 (Act 39 of 1994), which information is of substantial importance and is necessary for the proper discharge of the functions of the Agency;

(b) such information cannot reasonably be obtained by other means, he or she may issue the Agency with a direction authorising any member when reasonably necessary-

(i) to enter such premises;
(ii) to search such premises with the purpose of

obtaining such information;

(iii) to examine, copy, photograph or transcribe any article, document or other material on such premises; and

(iv) to remove any article, document or other material from the premises, for as long as is reasonably necessary, for the purposes of examining, copying, photographing or transcribing it, as the case may be.

(3)(a) A direction referred to in subsection (2) must be issued for a specific period not exceeding three months.

(b) A direction referred to in paragraph (a) may be executed by a member of the Agency who is authorised to do so by a senior member of the Agency holding a post of at least a General Manager.

(c) A member who executes a direction or assists in the execution thereof must, not later than the date of expiry of the direction referred to in paragraph (a), return any article, document or other material that was removed in terms of subsection (2)(b)(iv) to the premises in question unless the judge referred to in subsection (2) is of the opinion that the return of the said article, document or material will prejudice the security of the Republic, in which case the judge may direct that it be destroyed or stored elsewhere.

(4) The judge referred to in subsection (2) may, upon a written application complying with the directives issued under subsection (5), extend the period of validity of the direction for a further period not exceeding three months at a time, if the extension is necessary for a reason mentioned in subsection (2).

(5) The Judges President of the several Divisions of the High Court of South Africa may jointly issue directives to uniformly regulate the manner and procedure of applications in terms of subsection (2)."

(v) ***The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 ("RICA")***

37. Section 2 of RICA provides that, subject to RICA, 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. Thus, the default position in RICA is that interceptions are impermissible.

38. Section 3 of RICA specifically provides that:

> "3 Interception of communication under interception direction
>
> Subject to this Act, any
> (a) authorised person who executes an interception direction or assists with the execution thereof, may intercept any communication; and
> (b) postal service provider to whom an interception direction is addressed, may intercept any indirect communication,
> to which that interception direction relates."

39. "Interception direction" is defined as a direction issued under section 16(4) or 18(3)(a) and which authorises the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission, and includes an oral interception direction issued under section 23(7).

40. Section 16(1) provides that an applicant may apply to a designated judge for the issuing of an interception direction.

41. An "applicant" is defined as

41.1. an officer referred to in section 33 of the South African Police Service Act, if the officer concerned obtained in writing the approval in advance of another officer in the Police Service with at least the rank of assistant commissioner and who has been authorised in writing by the National Commissioner to grant such approval;

41.2. an officer as defined in section 1 of the Defence Act, if the officer concerned obtained in writing the approval in advance of another officer in the Defence Force with at least the rank of Major General, and who has been authorised in writing by the Chief of the Defence Force to grant such approval;

41.3. a member as defined in section 1 of the Intelligence Services Act, if the member concerned obtained in writing the approval in advance of another member of the Agency, holding a post of at least General Manager;

41.4. the head of the Directorate or an Investigating Director authorised thereto in writing by the head of the Directorate;

41.5. a member of a component referred to in paragraph (e) of the definition of 'law enforcement agency', authorised thereto in writing by the National Director; or

41.6. a member of the Independent Directorate, if the member concerned obtained in writing the approval in advance of the Executive Director.

42. A "designated judge" is defined as any judge of a High Court discharged from active service under section 3(2) of the Judges' Remuneration and Conditions of

Employment Act, 47 of 2001, or any retired judge, who is designated by the Minister to perform the functions of a designated judge for purposes of RICA.

43. A designated judge therefore performs duties related to national security. The judiciary is already an independent branch and the challenge whose essence is to question the independence of a designated judge is a challenge to the independence of the judiciary. Accordingly, the applicants' contentions regarding a designated judge are without merit. In any event, the designated judge is not the only oversight body that holds the intelligence services accountable[17]. Parliament and the Inspector-General of Intelligence are also structures designed to ensure that there is no unlawful intrusion into the citizens' right to privacy in the manner in which the Agency performs its functions.

44. The applicants complain that because the interception is issued without notice to the person to whom the application applies, it is therefore intrusive or constitutes a breach of the right of access to courts because there is no means of testing the evidence placed before the designated judge. It is simply not true that an *ex parte* application of this nature is necessarily a breach of the right of access to courts.

45. The applicants incorrectly rely on cases like *My Vote Counts, John v Rees, NDPP and Another v Mohamed NO and Others* to make a case of *audi alteram partem.*[18] Again, the applicants' reliance on these cases is misplaced. There is

---

17 Bundle, p 777, SSA answering affidavit, paras 83-84

18 Applicants' HoA, p 47, paras 112 - 117

no doubt that the principle of *audi* is a trite principle of our administrative law. However, relying on it in matters where it would undermine the very purpose of preventing security threats is entirely misplaced. The issue of prevention of security threats makes RICA interception a unique regime designed to deal with unique circumstances in which intelligence services seek to detect threats before they occur. It is precisely for this reason that RICA provides that applications to intercept must be considered by a designated judge. It is a recognition that without such an intervention, it would indeed exacerbate what is already some form of intrusion.

46. A designated judge is guided by the relevant provisions setting out the necessary averments to be made in order for the designated judge to grant an application for interception. The applicants' contention that an introduction of a public advocate would necessarily guarantee more independence is misplaced. In fact, this suggestion would prolong the process, which by its very nature requires a prompt response to security threats. It would also add a risk of security leaks and lapses as a result of an adversarial process and thus compromise the very prompt investigation it is designed to achieve[19].

47. Section 16(2) lists the necessary averments to be included in the application for interception, thus eliminating the possibility of the intrusion the applicants are complaining about.

---

[19] Bundle, p 782-783, SSA answering affidavit

48. Section 16(5) provides that:

"(5) An interception direction may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that:

(a) there are reasonable grounds to believe that:

(i) a serious offence has been or is being or will probably be committed;
(ii) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;
(iii) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;
(iv) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in -
(aa) accordance with an international mutual assistance agreement; or
(bb) the interests of the Republic's international relations or obligations; or

(v) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary;

(b) there are reasonable grounds to believe that –

(i) the interception of particular communications concerning the relevant ground referred to in paragraph (a) will be obtained by means of such an interception direction; and

(ii) subject to subsection (8), the facilities from which, or the place at which, the communications are to be intercepted are being used, or are about to be used, in connection with the relevant ground referred to in paragraph (a) are

commonly used by the person or customer in respect of whom the application for the issuing of an interception direction is made; and

(c) in respect of the grounds referred to in paragraph (a) (i), (iii), (iv) or (v), other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner: Provided that this paragraph does not apply to an application for the issuing of a direction in respect of the ground referred to in paragraph (a) (i) or (v) if the –

(i) serious offence has been or is being or will probably be committed for the benefit of, at the direction of, or in association with, a person, group of persons or syndicate involved in organised crime; or

(ii) property is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities."

(our emphasis)

49. In terms of section 16(6), an interception direction may specify conditions or restrictions relating to the interception of communications and may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein.

50. Section 16(7) provides that:

"(7) (a) An application must be considered and an interception direction issued without any notice to the person or customer to whom the application applies and without hearing such person or customer.

(b) A designated judge considering an application may require the applicant to furnish such further information as he or she deems necessary."

51. Section 17 provides for the application for, and issuing of, real-time communication-related direction.

52. "Real-time communication-related information" is defined as communication-related information which is immediately available to a telecommunication service provider -

(a) before, during, or for a period of 90 days after, the transmission of an indirect communication; and

(b) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates.

53. In terms of section 17(4),

"A real-time communication- related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that <u>there are reasonable grounds to believe</u> that -

(a) a serious offence has been or is being or will probably be committed;
(b) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;
(c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in –

(i) accordance with an international mutual assistance agreement; or
(ii) the interests of the Republic's international relations or obligations; or

(e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary, and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information."

54. Like section 16, section 17 lists

54.1. the necessary averments that must be made in the application,

54.2. the justification grounds that must be met for the issue of a direction,

54.3. that the direction may specify conditions or restrictions to which it is subject,

54.4. that the direction may be issued for a period not exceeding three months at a time, and

54.5. the period for which it has been issued must be specified therein.

55. Section 16(7) applies to section 17, with the necessary changes, in respect of an application for, and the issuing of, a real-time communication-related direction. That is, the application is considered and a direction is made without prior notice.

56. Section 19 deals with applications for, and issuing of, archived communication-related directions.

57. "Archive communication-related information" is defined as any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30(1)*(b)* for the period determined in a directive referred to in section 30(2)*(a)*, beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates.

58. Section 19(1) provides that if only archived communication-related information is required, an applicant may apply to a judge of the High Court, a regional court magistrate or a magistrate for the issuing of an archived communication-related direction.

59. Section 19(4) states that:

> "An archived communication-related direction may only be issued if it appears to the judge of a High Court, regional court magistrate or magistrate concerned, on the facts alleged in the application concerned, that <u>there are reasonable grounds to believe</u> that
>
> (a) a serious offence has been or is being or will probably be committed;
> (b) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in

(i) accordance with an international mutual assistance agreement; or

(ii) the interests of the Republic's international relations or obligations; or

(e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary,

and that the provision of archived communication-related information is necessary for purposes of investigating such offence or gathering such information."

(our emphasis)

60. Section 16(7) applies to section 19, with the necessary changes. That means the application is considered and a direction is made without prior notice.

61. Section 18 deals with combined applications for, and issuing of, interception direction, real-time communication-related direction and archived communication-related direction.

62. Section 18(1) provides that:

"(1) If the –

(a) interception of an indirect communication and the provision of communication-related information, whether real-time or archived or both; or

(b) provision of real-time and archived communication-related information, are required, an applicant may, subject to sections 16(2) and (3), 17(1) and (2) and 19(1) and (2), in a combined application, apply to a designated judge for the simultaneous issuing of any combination of directions referred to in those sections."

63. Like section 16, 17 and 19, the application is considered and a direction is made without prior notice.

64. Existing directions may be amended or extended. Section 20 provides that the applicant who made the application in respect of an existing direction or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the existing direction concerned, but before the expiry of the period for which it has been issued, apply to a designated judge for an amendment thereof or the extension of the period for which it has been issued. An existing direction may only be amended or the period for which it has been issued, may only be extended, if the designated judge is satisfied, on the facts alleged in the application, that the amendment or extension is necessary for purposes of achieving the objectives of the direction concerned, provided that the period for which an existing direction has been issued may only be extended for a further period not exceeding three months at a time. The application is considered and a direction is made without prior notice.

65. Section 21 provides for application for, and issuing of, a decryption direction. A "decryption direction" means a direction issued under section 21(3) in terms of which a decryption key holder is directed to

65.1. disclose a decryption key; or

65.2. provide decryption assistance in respect of encrypted information, and includes an oral decryption direction issued under section 23(7).

66. A 'decryption key' means any key, mathematical formula, code, password, algorithm or any other data which is used to (a) allow access to encrypted information or (b) facilitate the putting of encrypted information into an intelligible form.

67. "Encrypted information" is defined as any electronic data which, without the decryption key to that data (a) cannot, or cannot readily, be accessed or (b) cannot, or cannot readily, be put into an intelligible form.

68. Section 21(4) provides that:

"(4) A decryption direction may only be issued –

(a) if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that <u>there are reasonable grounds to believe</u> that –

(i) any indirect communication to which the interception direction concerned applies, or any part of such an indirect communication, consists of encrypted information;

(ii) the decryption key holder specified in the application is in possession of the encrypted information and the decryption key thereto;

(iii) the purpose for which the interception direction concerned was issued would be defeated, in whole or in part, if the decryption direction was not issued; and

(iv) it is not reasonably practicable for the authorised person who executes the interception direction concerned or assists with the execution thereof, to obtain possession of the encrypted information in an intelligible form without the issuing of a decryption direction; and

(b) after the designated judge concerned has considered –

(i) the extent and nature of any other encrypted information, in addition to the encrypted information in respect of which the decryption direction is to be issued, to which the decryption key concerned is also a decryption key; and

(ii) any adverse effect that the issuing of the decryption direction might have on the business carried on by the decryption key holder to whom the decryption direction is addressed."

69. Section 16(7) also applies to section 21, with the necessary changes, in respect of the issuing of a decryption direction. That means the application is considered and a direction is made without prior notice.

70. Section 22 provides for the application for, and issuing of, an entry warrant. An entry warrant may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that (a) the entry of the premises concerned is necessary for a purpose referred to in the definition of 'entry

warrant'; or (b) there are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception direction concerned otherwise than by the use of an interception device installed on the premises. The application is considered and a direction is also made without prior notice.

71. Section 22(4) provides that:

"An entry warrant may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that –

(a) the entry of the premises concerned is necessary for a purpose referred to in the definition of 'entry warrant'; or

(b) there are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception direction concerned otherwise than by the use of an interception device installed on the premises."

72. Section 24 provides that the designated judge who issued a direction or an entry warrant may at the issuing thereof or at any stage before the date of expiry thereof, in writing require the applicant who made the application in respect of the direction or entry warrant concerned to report to him or her in writing –

(a) at such intervals as he or she determines, on (i) the progress that has been made towards achieving the objectives of the direction or entry warrant concerned; and (ii) any other matter which the designated judge deems necessary; or

(b) on the date of expiry of the entry warrant concerned, on whether the interception device has been removed from the premises concerned and, if so, the date of such removal.

73. Section 25 provides for the cancellation of a direction or entry warrant if –

(a) the applicant concerned fails to submit a report in terms of section 24, if applicable; or

(b) he or she, upon receipt of a report submitted in terms of section 24, is satisfied that the

(i) objectives of the direction or entry warrant concerned have been achieved; or

(ii) ground on which the direction or the purpose for which the entry warrant concerned was issued, has ceased to exist.

74. Chapter 6 makes provision for the establishment of interception centres and the Office for Interception Centres.

75. Section 37 provides as follows:

"37 Keeping of records by heads of interception centres and submission of reports to Director

(1) The head of an interception centre must 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).

(2) (a) The head of an interception centre must on a quarterly basis, or as often as the Director requires, submit a written report to the Director on –

(i) the records kept by him or her in terms of subsection (1);
(ii) any abuses in connection with the execution of directions which he or she is aware of;
(iii) any defects in any telecommunication system or in the operation of the interception centre which have been discovered; and
(iv) such activities at the interception centre or on any other matter relating to this Act which the Director requests the head of the interception centre to deal with in such report.

(b) Notwithstanding paragraph (a), a head of an interception centre may at any stage submit a report to the Director on any matter which, in the opinion of the head concerned, should urgently be brought to the attention of the Director.

(3) The Director must, upon receipt of a report contemplated in subsection (2)(a), submit a copy of that report to the Minister and the Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994)."

76. Telecommunication service providers also have a duty to store communication-related information. In terms of section 30(2) of RICA, the Minister of Communications, in consultation with the Minister of Justice and Constitutional Development, and the other relevant Ministers and after consultation with the Independent Communications Authority of South Africa ("ICASA") 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, issue a directive.

77. The directive sets outs, among other things,

77.1. security, technical and functional requirements of the facilities and devices to be acquired by the telecommunication service provider or category of telecommunication service providers to enable

(a) interception of indirect communications in terms of RICA

(b) storing of communication related information

77.2. type of communication-related information which must be stored and the period for which such information must be stored.

78. RICA is a law of general application. So are the other laws discussed in brief above. Clear guidance is given in these enactments as to the scope of powers accorded to the Services, their monitoring and oversight. The safeguards and the purpose for which these laws have been enacted are such that it is incorrect to contend, as the applicants do, that these provisions in any way constitute an unconstitutional limitation of the rights enshrined in the Bill of Rights. Invasive they are, but not unconstitutionally so. We shall demonstrate this below.

F. **PREMATURITY**

79. It is common cause that RICA is currently the subject of review specifically in relation to the need to enhance governance, **transparency and accountability mechanisms** in order to oversee the interception of communications[20]. These are the very issues that form the pith and marrow of the applicants' attack. Their denial that the Minister has announced amendment of RICA in these respects is puzzling and, with respect, incomprehensible.

80. This application is thus premature. The applicant's intention, and the effect of the orders that they seek, will be to rush Parliament into hurriedly producing amendments that government is in any event considering.

81. At worst, the applicants want this Court to legislate from the bench on State policy-laden issues the content of which they want to dictate. This, with respect, is impermissible and in any event sets its face against the jurisprudence of the Constitutional Court in these matters.[21]

82. That brings us to a related subject of judicial deference in matter such as those with which this case is concerned.

---

[20] Bundle, pp 800-801; pp 907-909

[21] Minister of Defence and Military Veterans v Motau NO and Others 2014 (5) SA 69 (CC)

G. JUDICIAL DEFERRENCE ON POLICY-LADEN ISSUES

83. In **Minister of Environmental Affairs and Tourism and Others v Phambili Fisheries (Pty) Ltd; Minister of Environmental Affairs and Tourism and Others v Bato Star Fishing (Pty) Ltd** 2003 (6) SA 407 (SCA) the Court, in a review setting, made the need for judicial deference on matters outside judicial proficiency quite clear when it said:

> "Judicial deference is particularly appropriate where the subject-matter of an administrative action is very technical or of a kind in which a Court has no particular proficiency."[22]

84. On appeal to the Constitutional Court, in **Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Tourism and Others** 2004 (4) SA 290 (CC), the principle of judicial deference was endorsed in these words:

> "The use of the word 'deference' may give rise to misunderstanding as to the true function of a review Court. This can be avoided if it is realised that the need for Courts to treat decision-makers with appropriate deference or respect flows not from judicial courtesy or etiquette but from the fundamental constitutional principle of the separation of powers itself."[23]

85. The Constitutional Court continued:

> "In treating the decisions of administrative agencies with the appropriate respect, a Court is recognising the proper role of the Executive within the Constitution. In doing so a Court should be careful not to attribute to itself superior wisdom in relation to matters entrusted to other branches of

---

22 At paragraph [53]
23 At paragraph [46]

> government. A Court should thus give due weight to findings of fact and policy decisions made by those with special expertise and experience in the field. The extent to which a Court should give weight to these considerations will depend upon the character of the decision itself, as well as on the identity of the decision-maker. A decision that requires an equilibrium to be struck between a range of competing interests or considerations and which is to be taken by a person or institution with specific expertise in that area must be shown respect by the Courts . . ."[24]

86. National security, and the intelligence function designed for that purpose, is a policy-centric matter. While its implementation may be reviewed by courts at the instance of those who feel aggrieved by the effects of its implementation, it is not the role of Courts to decide matters that involve the balancing of complex factors and sensitive subject matter relating to national security and intelligence services.

87. What the applicants are seeking is not the review and setting aside of the conduct of officials in the implementation of RICA; they want this Court to second-guess government on policy matters that inform policy framework by which RICA is underpinned for purposes of national security. This they are not entitled to do, and the Court is not empowered to entertain.

---

[24] At paragraph [48]

H. HIGH THRESHOLD JURISDICTIONAL FACTS AS SAFEGUARDS

88. The jurisdictional fact that an applicant is required to meet in order to secure a direction is sufficiently high to serve as adequate safeguard against abuse of the powers provided for in RICA.

89. The legal position as regards jurisdictional facts or administrative triggers for the exercise of public power is clear. The *locus classicus* on jurisdictional facts in our law in the sphere of Administrative Law, which has now become infused into our supreme law, remains **South African Defence and Aid Fund and Another v Minister of Justice** 1967 (1) SA 31 (C) (**"the Defence and Aid Fund case"**) where the Court said:

> "Upon a proper construction of the legislation concerned, a jurisdictional fact may fall into one or other of two broad categories. It may consist of a fact, or state of affairs, which, objectively speaking, must have existed before the statutory power could validly be exercised. In such a case, the objective existence of the jurisdictional fact as a prelude to the exercise of that power in a particular case is justiciable in a Court of law. If the Court finds that objectively the fact did not exist, it may then declare invalid the purported exercise of the power (see e.g. *Kellerman v Minister of Interior,* 1945 T.P.D. 179; *Tefu v Minister of Justice and Another*, 1953 (2) SA 61 (T)). On the other hand, it may fall into the category comprised by instances where the statute itself has entrusted to the repository of the power the sole and exclusive function of determining whether in its opinion the pre-requisite fact, or state of affairs, existed prior to the exercise of the power. In that event, the jurisdictional fact is, in truth, not whether the prescribed fact, or state of affairs, existed in an objective sense but whether, subjectively speaking, the repository of the power had decided that it did. In cases falling into this category the objective existence of the fact, or state of affairs, is not justiciable in a Court of law. The Court can interfere and declare the exercise

of the power invalid on the ground of a non-observance of the jurisdictional fact only where it is shown that the repository of the power, in deciding that the pre-requisite fact or state of affairs existed, acted mala fide or from ulterior motive or failed to apply his mind to the matter."

90. In **President of the Republic of South Africa and Others v South African Rugby Football Union and Others** 2000 (1) SA 1 (CC) (**"SARFU"**) the Constitutional Court said **the Defence and Aid Fund case** remains the leading authority on jurisdictional facts in our law.[25]

91. Some 10 years after **SARFU**, in **Kimberley Junior School and Another v Head, Northern Cape Education Department and Others** 2010 (1) SA 217 (SCA) at paras [12]-[13] the Supreme Court of Appeal said:

"[12] … . As was pointed out by the Constitutional Court in *President of the Republic of South Africa and Others v South African Rugby Football Union and Others* … the judgment of Corbett J in *South African Defence and Aid Fund and Another v Minister of Justice* 1967 (1) SA 31 (C) remains the leading authority on jurisdictional facts in our law. In that judgment Corbett J … identified two categories of jurisdictional facts that can be encountered in empowering legislation. The first category, described as 'objective jurisdictional facts', includes the type of fact or state of affairs that must exist in an objective sense before the power can validly be exercised. Here the objective existence of the fact or state of affairs is justiciable in a court of law. If the court finds that objectively the fact or state of affairs did not exist, it will declare invalid the purported exercise of the power.

[13] In the second category, that of subjective jurisdictional facts, the empowering statute has entrusted the repository of the power itself with the function to determine whether in its subjective view the prerequisite fact or state of affairs existed or not. Expressions often used by the legislature to express this intent are, eg 'in his or her opinion' or 'if he or she is satisfied that' the particular fact or state of affairs exists. In this event the question is

[25] at para [168] footnote 132

> not whether the prescribed fact or state of affairs existed in an objective sense. The court can only interfere where it is shown that the repository of the power, in forming the opinion that the fact or state of affairs existed, had failed to apply its mind to the matter. Whether a particular jurisdictional fact can be said to fall within the one category or the other, will depend on the interpretation of the empowering statute."

92. In **Democratic Alliance v President of the RSA and Others** 2012 (1) SA 417 (SCA), the Supreme Court of Appeal acknowledged the distinction between subjective and objective jurisdictional facts, and the proper approach in relation to each, and found the clause there in issue to be of the objective variety.[26]

93. Thus, the distinction between subjective and objective discretionary clauses is still very much part of our law on jurisdictional facts. The plain language of the impugned provisions connotes an **objective discretionary power** the exercise of which can be set aside on review if the aggrieved party (such the applicants) can show that the designated judge's grounds for granting surveillance orders are unreasonable or irrational or otherwise unlawful. These jurisdictional facts carry a higher standard of proof or a higher threshold. They include, for example

93.1. section 16(5): **"satisfied . . . that there are reasonable grounds to believe"** in relation to the issuing of an interception direction;

---

[26] At para [118]

93.2. section 17(4): **"it appears that . . . there are reasonable grounds to believe"** in relation to the issuing of real-time communication-related direction;

93.3. section 19(4): **"it appears that . . . there are reasonable grounds to believe"** in relation to the issuing of an archived communication-related direction;

93.4. section 21(4): **"satisfied . . . that there are reasonable grounds to believe"** in relation to the issuing of a decryption direction;

93.5. section 22(4): **"satisfied . . . that there are reasonable grounds to believe"** in relation to the issuing of an entry warrant;

93.6. section 23(4)(a)(i): **"satisfied . . . that there are reasonable grounds to believe"** in relation to the issuing of an oral direction or oral entry warrant in urgent circumstances.

94. These carry a higher threshold or standard of proof than **subjective discretionary power** denoted by phrases like **"in his or her opinion"** or **"if he or she is satisfied"** or **"if he or she believes"** which can only be set aside on grounds that the decision-maker was actuated by bad faith or by an ulterior

motive or failed to apply his or her mind to the matter. Examples of these **subjective discretionary power** jurisdictional facts are found in

94.1. section 20(4): **"if the designated judge concerned is satisfied"** in relation to the amendment of an existing direction; and

94.2. section 25(1)(b): **"if [the designated judge concerned] is satisfied"** in relation to the cancellation of a direction or entry warrant.

95. In fact, the objective discretionary power denoted by the phrase **"reasonable grounds to believe"** is the equivalent of **"high degree of probability"** that the applicants want employed in respect of journalists and lawyers specifically in their fourth challenge. We submit that their demand in this regard probably stems from their lack of appreciation of the current South African jurisprudence in relation to jurisdictional facts.

96. Strikingly, the threshold for the cancellation of a direction or entry warrant is lower than the threshold for the granting thereof. This is not fortuitous. It is deliberate because the legislature appreciates acutely the invasive nature of these instruments. That is why the granting of a new direction or entry warrant requires a higher standard than the amendment of an existing direction or cancellation of a direction or entry warrant.

97. There are other provisions in RICA that set the threshold even higher than the objective jurisdictional fact itself suggests. For example,

97.1. The designated judge may cancel a direction or entry warrant if the person at whose instance it was granted fails to submit a report detailing the progress that has been made towards achieving the objectives of the direction or entry warrant concerned and any other matter which the designated judge considers necessary to report on, or (on the date of expiry of the entry warrant concerned) on whether the interception device has been removed from the premises concerned and, if so, the date of such removal.[27]

97.2. The designated judge may cancel a directive or entry warrant if he or she is satisfied, upon receiving a progress report, that the objectives of the direction or entry warrant have been achieved, or that the purpose for which the direction or entry warrant had been issued has ceased to exist.[28]

97.3. If an entry warrant has been cancelled, the person at whose instance it had been issued must, as soon as practicable after having been informed of such cancellation, remove any interception device which had been installed under the entry warrant.[29]

---

27 s 25(1)(a)
28 s 25(1)(b)
29 s 25(4)

97.4. If a direction is cancelled, the contents of any communication intercepted under that direction will be inadmissible as evidence in any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 121 of 1998, unless the court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise be detrimental to the administration of justice.[30]

98. Clear from these provisions is that

98.1. the designated judge not only issues directions and entry warrants but also monitors that they are used for the purpose for which they had been sought;

98.2. once the purpose for which the direction or entry warrant had been issued has been achieved, it is cancelled and does not require the target's application for cancellation or setting aside;

98.3. the designated judge ensures removal of the interception device when the entry warrant has reached its expiry date without the need for the target to approach him or her on application;

---

30 s 25(5)(a)

98.4. by the monitoring powers conferred upon him or her, the designated judge ensures that the directions and/or entry warrants are not abused thus making it unnecessary for the target to run to court for the review and setting aside of the direction or entry warrant;

98.5. the fact that information gathered under direction cannot be used in evidence in any court proceedings after cancellation is yet another safeguard in the protection of the target's rights.

99. All these point to the fact that notice of the issue of a direction or entry warrant is self-evidently unnecessary under the scheme of RICA as it guards against abuse and wanton invasion.

100. Attention may be drawn to two judgments of the High Court – one from the Pietermaritzburg High Court (**Valuline CC and Others v Minister of Labour and Others** 2013 (4) SA 326 (KZP)) and another from the North Gauteng High Court (**Freedom Under Law v NDPP** 2014 (1) SA 254 (GNP)) – and a Constitutional Court judgment in **Walele v City of Cape Town and Others** 2008 (6) SA 129 (CC) for the proposition that all jurisdictional facts are now objectively determinable and that the **Defence and Aid Fund** standard no longer holds sway.

101. But upon a proper consideration of these cases one soon realises that none of them detracts from the **Defence and Aid Fund** bifurcated approach to jurisdictional facts. Certainly, in none of them has the **Defence and Aid Fund** approach been jettisoned as no longer forming part of our law.

102. The legislative provision that called for consideration in **Valuline** was differently phrased than the residual clause in the impugned provisions in this case. While we are here concerned with the standard of **"reasonable grounds to believe"**, **Valuline** was concerned with the Minister's **"satisfaction"**. The provision in question was s 32(3)(c) of the Labour Relations Act, 66 of 1995 which says:

> "(3) A collective agreement may not be extended in terms of subsection (2) unless the Minister is satisfied that-
> (a) …
> (b …
> (a) the members of the employers' organisations that are parties to the bargaining council will, upon the extension of the collective agreement, be found to employ the majority of all the employees who fall within the scope of the collective agreement"

103. In any event, the basis for the setting aside of the Minister's decision in **Valuline** was not that the **Defence and Aid Fund** bifurcated approach no longer forms part of our law. It was rather that the Minister had – in merely relying upon a certificate as being conclusive of the issue to which she was required to apply her mind – failed to apply her mind properly to the determination of that issue. That is one of the bases recognised in the **Defence and Aid Fund case** for the

review of a subjective jurisdictional fact. Thus, **Valuline** does not represent a departure from the **Defence and Aid Fund** approach.

104. The **Freedom Under Law** case had to do with a challenge to decisions made by an assortment of persons within the country's policing and prosecution cluster, including a decision to withdraw criminal and disciplinary charges against Lieutenant-General Mdluli. At issue was whether Courts have the power to review decisions of the prosecuting authority to discontinue a prosecution. The Court said yes and proceeded to set aside the decision to discontinue the prosecution of Lieutenant-General Mdluli on numerous grounds including irrationality, illegality, unreasonableness, consideration of irrelevant factors and material errors of law[31]. Nowhere was any suggestion made that the **Defence and Aid Fund** approach is no longer good law. There was also no suggestion in that case that the provisions pursuant to which prosecution was discontinued were of a subjective sort. The three reasons apparently advanced for the discontinuation of the prosecution seem not to spring from any legislative provision evincing a subjective or objective jurisdictional fact; they seem rather to spring from the decision-maker's own perception.[32]

105. **Walele** was concerned with a provision of the National Building Regulations and Building Standards Act, 103 of 1977, which required the **"satisfaction"** (not **"reasonable grounds to believe"**) of the local authority that the building to

---

31 See paras [167], [176] and [186]
32 See paras [171] and [175]

which the application relates would probably be unsightly or objectionable, or dangerous to property or life, or derogate from the value of adjoining or neighbouring properties, before refusing approval for the erection of a building. But the provision in **Walele** went further and required that the local authority **"give written reasons for such refusal"**.[33] Thus, quite apart from the fact that the provision in **Walele** is differently worded, the requirement in the section that the decision-maker gives written reasons for his decision constitutes an internal objective review mechanism.

106. In any event, nowhere in **Walele** is the **Defence and Aid Fund** approach jettisoned whether expressly or by necessary implication.

107. The applicants, with respect, fail to appreciate the nature of the jurisdictional fact by which their rights are safeguarded in RICA.

I. THE EVIDENCE THE APPLICANTS RELY ON AND THE ABSTRACT NATURE OF THIS APPLICATION

108. The deponent to the founding affidavit ("the second applicant"), places much reliance on public reports that he admits do not fall within his personal knowledge. He seeks the admission of such reports in terms of the Law of Evidence Amendment Act 45 of 1988.[34]

---

33 See para [50] of **Walele**

34 Bundle, p 10, para 3 see also p 76-90

109. There are, however, no allegations in the founding affidavit that support the admission of the hearsay evidence that the applicants seek to have admitted.

110. These reports include:

110.1. The Joint Standing Committee of Intelligence Reports;

110.2. The Annual Report by Justice Mokgoro; and

110.3. The United Nations Human Rights Committee Report.

111. We respectfully submit that it will not be in the interests of justice for such evidence to be admitted. The admission of such evidence prejudices the respondents in that the true probative value of the evidence is questionable.[35]

112. The applicants also refer to certain "examples" such as Stephen Hofstätter, Mzilikazi wa Afrika, Paul Scheepers.[36] But nothing more is said. The applicants lay no factual basis in respect of these examples. So too with those listed under bulk communications surveillance and in reply.

113. To the extent that the reports and examples are relied on solely to demonstrate perceived problems with RICA, we respectfully submit that these cannot and do not sustain an argument that the provisions of RICA and/or the NSIA are unconstitutional.

---

35 Bundle, p 820, para 167.9

36 Bundle, p 83, para 176-177

114. As regards the second applicant's own experience, he states that during 2008 he suspected that he was being monitored and that his communications were being intercepted. He links this to a story he had been investigating in relation to the Arms Deal.[37]

115. He confirms that a complaint was made by the *Mail & Guardian* (his employer at the time) to the Inspector-General in May 2009 in terms of section 7 of the ISOA.[38] The complaint related to:

115.1. The alleged surveillance of *Mail & Guardian* journalists;

115.2. The alleged monitoring and interception of communications between *Mail & Guardian* journalists and their sources;

115.3. Other forms of alleged covert action against *Mail & Guardian* journalists which has taken place over a period of 6 years;

115.4. The alleged dissemination by members of the Intelligence Services of false and damaging allegations about some of the *Mail & Guardian* journalists (including the second applicant).

---

37 Bundle, p 28, para 37
38 Bundle, p 97

116. On 14 September 2009, the Inspector-General responded to the complaint.[39] The response was, among other things, that:

116.1. *"We take cognisance of the constitutional rights to freedom of expression and that of privacy highlighted by you and wish to add that we share your sentiments of the importance of these rights in protecting our democracy. However at the same time one should not lose sight of the fact that the right to freedom of expression is not absolute and in this case must be balanced by the constitutional obligation of government to maintain national security."*;

116.2. The complaint was dealt with in terms of the Intelligence Services Oversight Act;

116.3. Internal policies set out investigation methodologies;

116.4. In the conduct of all investigations, relevant documents are requested from the Service concerned and perused to verify and corroborate the veracity of explanations provided therein;

116.5. Particular reference is had to a judicial direction and its supporting documentation as prescribed by section 16 of RICA which would in all

39 Bundle, p 122

cases involving the Intelligence Services be classified and protected from disclosure;

116.6. To request sight of these documents as proof of findings will serve to compromise intelligence methods and sources protected by legislation;

116.7. Sight of classified information would entail declassification in circumstances that warrant it. The complaint does not warrant such declassification;

116.8. Police investigations are protected from disclosure until such time that criminal charges are preferred. Disclosing the information requested not only serves to compromise and undermine these investigations but also has the potential of infringing constitutional rights of individuals involved which far exceeds that bounds of right of access to information;

116.9. In cases where criminal charges are later preferred against an individual arising from a police investigation, the law governing criminal procedure sets out parameters for disclosure and discovery of evidentiary material between the parties to the proceedings;

116.10. Following extensive investigations on all the complaints, it was found that at all stages both the National Intelligence Agency and the crime intelligence division acted within the regulatory framework governing the activities of the Intelligence Services, which includes acting within the prescripts set out in RICA.

117. This response is consistent with the legal prescripts that govern Intelligence Services. It is inappropriate to second guess

117.1. the Inspector-General; and

117.2. the designated judge who granted the interception directions.

118. The second applicant simply contends that *"there could not have been any lawful basis under RICA according to which the interception direction against me could have been granted. I submit that the conversations between Mr Downer and journalists (such as myself) plainly would not have satisfied any of the grounds under RICA. Moreover, even if RICA in its present form permitted the interception of my communications under these circumstances, then I submit that this is simply a further indication that RICA is not constitutionally compliant."*[40]

119. What the second applicant fails to understand is that:

---

40 Bundle, p 35, para 60

119.1. A duty is placed on the designated judge (as a member of the judiciary) to ensure that an application to intercept is for a lawful purpose and is not open to abuse;

119.2. The involvement of a Judge is precisely to ensure that the rights of the subject of interception are protected;

119.3. There are institutionalised oversight mechanisms that are built into the legislation and are intended to provide checks and balances;

119.4. The nature of intelligence gathering is a process, not an event that starts and ends within a determinable time frame, or that necessarily produces fool-proof results;

119.5. Such certainty, as sought by the applicants, is simply not consistent with the nature of the business of state security and intelligence.

120. The applicants have failed to set out any facts that support a finding that:

120.1. The subject of an interception direction must be notified;

120.2. The independence of the designated judge is questionable;

120.3. That the storage of personal communications limits the right to privacy and that the length of time that the communications are kept aggravates this limitation;

120.4. That a higher threshold should apply for subjects with a source protection duty, such as journalists and lawyers;

120.5. There is lack of sufficient safeguards.

121. We respectfully submit that the relief sought by the applicants is therefore brought in the abstract. In this regard, the Constitutional Court has held that:

> "[13] …Courts generally treat abstract challenges with disfavour. And rightly so. Will hearsay, similar facts or evidence of previous convictions be led at the applicants' trial? At this stage we simply do not know. Abstract challenges ask courts to peer into the future, and in doing so they stretch the limits of judicial competence. For that reason the applicants in this case bear a heavy burden — that of showing that the provisions they seek to impugn are constitutionally unsound merely on their face. The analysis that follows demonstrates just how heavy that burden is." [41]

J. LIMITATION OF RIGHTS

122. The applicants invoke four constitutional rights:

122.1. The right to privacy in section 14 of the Constitution;

---

[41] **Savoi and others v National Director of Public Prosecutions and another** 2014 (5) SA 317 (CC)

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

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

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

123. The extent to which the full enjoyment of a constitutionally protected right might be limited is circumscribed by the Constitution itself. Section 36 of the Constitution provides that:

"36 Limitation of rights

(1) 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.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights."

124. In **S v Makwanyane and Another** 1995 (3) SA 391 (CC) the Constitutional Court held that:

> "[104] The limitation of constitutional rights for a purpose that is reasonable and necessary in a democratic society involves the weighing up of competing values, and ultimately an assessment based on proportionality. This is implicit in the provisions of s 33(1). The fact that different rights have different implications for democracy and, in the case of our Constitution, for 'an open and democratic society based on freedom and equality', means that there is no absolute standard which can be laid down for determining reasonableness and necessity. Principles can be established, but the application of those principles to particular circumstances can only be done on a case-by-case basis. This is inherent in the requirement of proportionality, which calls for the balancing of different interests. In the balancing process the relevant considerations will include the nature of the right that is limited and its importance to an open and democratic society based on freedom and equality; the purpose for which the right is limited and the importance of that purpose to such a society; the extent of the limitation, its efficacy and, particularly where the limitation has to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question. In the process regard must be had to the provisions of s 33(1) and the underlying values of the Constitution, bearing in mind that, as a Canadian Judge has said, 'the role of the Court is not to second-guess the wisdom of policy choices made by legislators'."

125. Security services have a constitutional duty to protect every person from harm whilst simultaneously securing the national interests and well-being of the people of the Republic as set out in section 198 of the Constitution.

126. We have already shown that the Intelligence Services form part of a cluster of security services to protect citizens. It is common cause that the discharge by members of the Intelligence Services of their constitutional and statutory mandates sometimes encroaches upon the basket of protections provided for in

the Bill of Rights. But where those tasked by the statute to exercise powers conferred upon them by legislation do so in a manner that encroaches upon the constitutional rights of others, it is their conduct that is unconstitutional, not the legislation that confers the power on them. Put differently, the unconstitutionality of an official's conduct in the exercise of powers conferred by a perfectly constitutional piece of legislation cannot render the constitutionality of the legislation itself. If, for example, the designated judge simply rubber stamps an application without even considering the application, he or she acts unlawfully. But his or her conduct cannot have the effect of tainting the legislation under which he or she purports to exercise those powers. This is the distinction that the applicants fail to appreciate.

127. The regulation of such encroachment is what RICA is intended to, and does, secure.

128. We now turn to the specific challenges which the applicants raise. We address whether there are any rights that are limited by the impugned provisions in respect of each challenge and if so, why these limitations are reasonable and justifiable in terms of section 36 of the Constitution.

K. RESPONSE TO EACH OF THE APPLICANTS' CHALLENGES

(i) First Challenge: Notification to the subject of an interception direction

129. The applicants' complaint is that it is mandatory under RICA that the subject is not notified prior to the granting of the application.

130. But the Constitution confers no right to notification. So, the applicants allege that section 16(7) of RICA, and the other sections relying on it, are inconsistent with the Constitution and invalid because they breach the rights to privacy (section 14) and access to courts (section 34).

131. As regards the right to privacy, section 14 of the Constitution provides that:

> "14 Privacy
>
> Everyone has the right to privacy, which includes the right not to have –
>
> (a) their person or home searched;
> (b) their property searched;
> (c) their possessions seized; or
> (d) the privacy of their communications infringed."

132. The applicants accept that prohibiting pre-surveillance notification is a justifiable limitation of the rights involved[42] but contend that there is no justification for the subject of an interception not to be notified after the surveillance has taken place.

133. The applicants, however, fail to appreciate that the nature of intelligence gathering is a process, not an event that starts and ends within a determinable time frame or that necessarily produces fool-proof results.

134. Interception is necessitated by the demands of national security, is a measure of last resort and is done with the leave of a designated judge after satisfying jurisdictional facts that set a high threshold.

135. An interception direction may only be issued if the designated judge concerned is "satisfied" that **"there are reasonable grounds to believe"** that, among other things,

135.1. a serious offence has been or is being or will probably be committed;

135.2. the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

---

[42] See FA para 69.1; RA para 26; Applicants' heads paras 86 & 87

135.3. the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary.

136. Notification in these circumstances defeats the very object of an interception, which is to neutralise or prevent the security threat before it happens.

137. Section 34 of the Constitution provides that everyone 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.

138. The designated judge is such **"independent and impartial forum"**. He or she has the institutional judgment and competence, as well as the statutory authority, to interrogate any perceived or unwarranted deviations that are inconsistent with the powers accorded to these Intelligence Services.

139. The applicants contend that secrecy should be the exception not the rule.

140. However, in **Independent Newspapers (Pty) Ltd v Minister for Intelligence Services: In re Masetlha v President of the Republic of South Africa and another** 2008 (5) SA 31 (CC), the Constitutional Court held that:

"[43] …I accept that the default position is one of openness. My difficulty arises in defining the circumstances in which that default position does not apply. As will become apparent later, I cannot accept the argument that the default position may only be disturbed in exceptional circumstances.

[44] The 'exceptional circumstances' standard advanced is inconsistent with the design of our Constitution and the jurisprudence of this court on several counts. The better approach, I think, is to recognise that the cluster of rights that enjoins open justice derives from the Bill of Rights and that, important as these rights are individually and collectively, like all entrenched rights, they are not absolute. They may be limited by a law of general application provided the limitation is reasonable and justifiable. It is not uncommon that legislation and the common law in this country, and elsewhere in open and democratic societies, limit open court hearings when fair trial rights or dignity or rights of a child or rights of other vulnerable groups are implicated."

141. The principle of open justice is therefore not without exception.[43]

142. We respectfully submit that sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) do not constitute a violation of the Constitution.

(ii) <u>Second Challenge: Independence of the designated judge</u>

143. The applicants raise two issues under this rubric. First, they allege that RICA fails to secure the independence of the designated judge (**"the independence argument"**). Second, they allege that there is no adversarial process before the designated judge and that the other side of the case is never presented (**"the audi argument"**).

---

[43] **Shinga v The State (Soc of Advocates, Pietermaritzburg Bar as Amicus Curiae); O'Connell v The State** 2007 (4) SA 611 (CC) at [27]

144. In respect of the independence argument, the applicants hinge their proposition on two pegs:

144.1. They say there is no term specified under RICA. The present term for a designated judge is one year, with the option for renewal. But they are unhappy that there is no restriction as regards the number of renewals of the designated judge's term there can be; and

144.2. They say the designated judge is appointed at the instance of a member of the executive, the Minister.[44]

145. We submit that RICA is consistent with the core values of judicial independence.

146. RICA defines a 'designated judge' as

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

147. Section 174 of the Constitution provides for the appointment of judicial officers. Section 174(1) provides that:

---

[44] Applicants' HoA, p 54-55, para 134

"Any appropriately qualified woman or man who is a fit and proper person may be appointed as a judicial officer. Any person to be appointed to the Constitutional Court must also be a South African citizen"

148. Section 174(8) provides that:

"Before judicial officers begin to perform their functions, they must take an oath or affirm, in accordance with Schedule 2, that they will uphold and protect the Constitution."

149. The process of applying for an interception direction is therefore validated by the institutional independence of the designated judge. The designated judge performs a quasi-judicial function, is independent and impartial in his or her application of the law and is appropriately qualified for such appointment. The applicants have failed to set out why a Judge cannot be trusted to perform this function without the assistance of a public advocate. There is absolutely no explanation why a designated judge alone is a threat to accountability or will not be able to ensure compliance with constitutional prescripts.

150. In respect of the second issue, the fault line that runs through the applicants' support for an adversarial process is inappropriate to the environment within which intelligence services operate.

151. RICA provides sufficient safeguards:

151.1. The designated judge must have before him or her an application that complies with the requirements detailed in section 16, 17, 18 or 19.

151.2. The designated judge has the right to call for any information which s/he considers necessary (section 16(7) & (8));

151.3. Regardless of whether the application complies with the requisites, the designated judge has a discretion whether to issue the direction or not (section 16(4));

151.4. The designated judge has an obligation not to issue a direction unless s/he is satisfied that **there are objective grounds to believe** that the prevailing circumstances warrant an interception direction (section 16(5)). This is high threshold;

151.5. The designated judge is called upon to make an independent evaluation and determine whether there are reasonable grounds for believing that the necessary conditions for and interception direction are present (section 16(5))

152. In reply the applicants demonstrate amply that the suggestion of a public advocate would indeed add another layer, thus constituting delay that could compromise the very purpose of the interception sought. The applicants propose that there should be a "return date" after a rule nisi has been granted[45].

---

[45] Bundle, p 1015, Replying Affidavit, para 85

153. In the replying affidavit, the applicants only state that "…tasking a singular designated judge with all the applications will necessarily constrain the amount of independent inquiry that singular designated judge can undertake."[46] This bold assertion is made without any reference to evidence that a designated judge is inundated with applications that are beyond his or her time and capacity.

154. There is absolutely no evidence to suggest that a designated judge's independence will be diminished by the volume of applications. In any event, there is no evidence that such applications are so voluminous as to impair the independence of the designated judge.

155. What the applicants fail to appreciate, with respect, is that the process of applying for an interception direction is not presided over by an overzealous clerk in a government office armed with a rubber stamp and a political party membership card. It is a rigorous process that is validated by the institutional independence of the designated judge who performs a quasi-judicial function, is independent and impartial in his or her application of the law, and is appropriately qualified for such appointment.

156. The fact that the designated judge is appointed by the Minister without a Judicial Service Commission process does not detract from his or her independence and

---

[46] Bundle, p 1016, Replying Affidavit, para 86

impartiality. Judges are often appointed to head Commissions of Inquiry (e.g, the "State Capture" Commission of Inquiry or the Marikana Commission of Inquiry) , or to preside over Inquiries (e.g, the Justice Mokgoro Inquiry), without undergoing the JSC process. That does not detract from their impartiality or independence.

157. We respectfully submit that the definition of "designated judge" in section 1 of RICA is therefore consistent with the Constitution. The challenge in this regard has no merit.

(iii) <u>Third Challenge: Safeguards regarding data obtained</u>

158. The applicants allege that 37 of RICA is inconsistent with the Constitution and is 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 the interceptions.

159. They further allege that the storage of personal communications limits the right to privacy and that the length of time that the communications are kept aggravates this limitation. In this regard, they also challenge section 30(2)(a)(iii) of RICA.

160. They contend that RICA fails to prescribe

160.1. the procedure to be followed for examining, using and storing data obtained from the surveillance;

160.2. the precautions to be taken when communicating the data to other parties; and

160.3. the circumstances in which recordings may or must be erased.

161. But, section 35 of RICA provides that in order to achieve the objects of RICA, the Director must, among other things,

161.1. regulate the procedure and determine the manner in which the provisions of RICA must be carried out by interception centres;

161.2. coordinate the activities of interception centres;

161.3. 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; and

161.4. prescribe the manner in, and the period for, which such information must be kept.

162. In respect of section 30, the directive of the Minister of Communications prescribes what must be stored and the period for which such information must be stored.

163. The applicants seem to have overlooked these provisions.

(iv) <u>Fourth Challenge: The question of legal privilege and the confidentiality of journalists' sources</u>

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

164.1. A stricter or higher threshold for granting an application; and

164.2. An independent intermediary should screen the information and pass any relevant information on to the Agency that sought the direction.

165. However, the merits of these claims fail to acknowledge that the limitations that apply to other rights in the Bill of Rights also apply to the rights exercised by lawyers and journalists. There is no reason why a threat posed by a journalist or a lawyer should be treated with less rigour. Security threats can be posed by any individual, regardless of their profession. There is absolutely no threat posed by bulk surveillance or interception in general to investigative journalism. It is submitted therefore that this challenge is ill-conceived as it requires a law of general application to apply a different standard to journalists and lawyers in circumstances where national security is at stake.

166. This is an untenable proposition which may have consequences that the applicants may not have intended. For example, if journalists and lawyers are to be treated differently in relation to interceptions for purposes of national security, why should priests and other faith leaders not be treated differently in relation to, say, the Sexual Offences Act, on the ground that priests are in the business of saving souls and not abusing bodies? Why should the police not be treated differently in relation to the Prevention of Organised Crime Act on the ground that they are in the business of solving crime and not committing it?

167. In their Replying Affidavit, the applicants dispute the fact that when it comes to security threats, journalists are no different from everybody else. In this regard, the applicants contend that "…the protection of journalists' sources is fundamental to the freedom of the press, as enshrined in section 16 of the Constitution. The surveillance of journalists undermines their ability to protect the anonymity of their sources. The disclosure of journalistic sources would have a chilling effect on the media, and their critical role in our constitutional democracy."[47]

168. With respect, this emotive plea is self-serving. Indeed, the role of journalists in a democracy is not questioned. However, the applicants make no case as to why this role should trump the genuine security imperatives of the State. There are no facts set out by the applicants to suggest that a journalist is incapable of posing a security threat. Accordingly, and for purposes of preventing security threats, not disclosure of sources, there is no reason why persons who are journalists or lawyers should be distinguished from the rest of society. It is therefore the duty of the designated judge to ensure that when applications for interception are made, there is scrupulous compliance with the requirements of RICA in this regard.

169. In respect of legal professional privilege, a material requirement for the privilege to be claimed is that the communication between legal advisor and client should

---

47 Bundle, p 1018, Replying Affidavit, para 95

not facilitate the commission of a crime. Indirect communication and archived communication related information do not qualify for specific protection on the ground of legal privilege as it does not qualify as a communication and merely indicates that a communication took place at a certain time between persons.

170. RICA is a law of general application. There is therefore no cause for journalists to be exempted. It is the subject matter not the subject that determines the rationale of the interception. There is no suggestion that RICA should ever be used to discover lawful discussions between lawyers and their clients or to establish journalists' sources in the performance of their important function as journalists. Accordingly, there is no basis for this challenge by the applicants.

171. In any event, the fact that a journalist or a lawyer is the subject of the interception may form part of the detail that the applicant may bring to the attention of the designated judge, whose duty is in turn to ensure that the limitation of the subjects right to privacy merits interception. There is no compelling reason why that fact should be specifically provided for in legislation.

(v) Fifth Challenge: Bulk & foreign signals surveillance

172. The applicants allege that RICA makes no provision for general bulk/mass surveillance of the public. They contend that:

172.1. The bulk surveillance and/or foreign signals surveillance that has taken place is *ultra vires* and that no bulk surveillance and/or foreign signals surveillance may lawfully take place until new legislation is enacted which incorporates sufficient safeguards.

172.2. In the alternative, in the event that the Court finds that RICA and/or the NSIA do empower bulk surveillance and/or foreign signals surveillance, then RICA and/or the NSIA are unconstitutional for their failure to provide any statutory safeguards for these forms of surveillance.

173. The applicants, however, misconstrue the nature and purpose of bulk interception.

174. These operations are conducted in fulfilment of the counter intelligence mandate of the Agency.

175. In their Replying Affidavit, the applicants incorrectly allege that "…the first respondent does not address the allegations relating to bulk intelligence."[48] This may be so, but this is addressed in the answering affidavit deposed to by Mr Fraser of the SSA. It is stated clearly in the answering affidavit that bulk surveillance is an internationally accepted method of monitoring transnational

[48] Bundle, p 1031, Replying affidavit, para 125.1

signals. It is not designed to intrude on the privacy of individuals, but is used to screen transnational signals for certain cue words and phrases in order to pre-empt transnational threats. By its very nature, it is focused on key words associated with transnational threats like terrorism and such global threats to sovereign states and their citizens. The applicants have entirely missed the nature and purpose of bulk surveillance.

176. The development of unconventional threats to peace and stability, technological advances and the pervasiveness of cybercrimes have compelled various jurisdictions to adopt modalities such as bulk surveillance in an effort to secure the well-being of their inhabitants[49]. South Africa is no different, and as with other jurisdictions, has institutionalised oversight mechanisms that are intended to provide checks and balances to ensure that the intelligence services execute their mandate within constitutional bounds.

L. APPROPRIATE REMEDY

177. In the event that the Court is persuaded to set the impugned provisions aside, regard must be had to the fact that RICA has been earmarked for revision and appropriate amendments in respect of, among other things,

---

[49] Bundle, p 794, Answering Affidavit, paras 128-146

177.1. The need to enhance governance, **transparency and accountability mechanisms** in order to oversee the interception of communications; and

177.2. The broadening of RICA to cater for the combating of cyber-crime, making provision for other forms of electronic surveillance and regulating the use of remote access tools to investigate crimes.[50]

178. In the light of the above, it is respectfully submitted that the appropriate policy development process should be allowed to take its course and reach its conclusion prior to any order of constitutional invalidity being made.

179. For the reasons set out above, it is submitted that the applicants have failed to make out a case for the relief sought. As a result, this application ought to be dismissed with costs, including the costs of three counsel.

V Ngalwana SC
M Sikhakhane SC
F Karachi
Z Ngwenya

Sandton Chambers
15 March 2019

[50] Bundle, p 800-801

LIST OF AUTHORITIES

- Minister of Defence and Military Veterans v Motau NO and Others 2014 (5) SA 69 (CC)

- Minister of Environmental Affairs and Tourism and Others v Phambili Fisheries (Pty) Ltd; Minister of Environmental Affairs and Tourism and Others v Bato Star Fishing (Pty) Ltd 2003 (6) SA 407 (SCA)

- Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs and Tourism and Others 2004 (4) SA 290 (CC)

- South African Defence and Aid Fund and Another v Minister of Justice 1967 (1) SA 31 (C)

- President of the Republic of South Africa and Others v South African Rugby Football Union and Others 2000 (1) SA 1 (CC) ("SARFU")

- Kimberley Junior School and Another v Head, Northern Cape Education Department and Others 2010 (1) SA 217 (SCA)

- Democratic Alliance v President of the RSA and Others 2012 (1) SA 417 (SCA)

- Valuline CC and Others v Minister of Labour and Others 2013 (4) SA 326 (KZP)

- Freedom Under Law v NDPP 2014 (1) SA 254 (GNP)

- Walele v City of Cape Town and Others 2008 (6) SA 129 (CC)

- Savoi and others v National Director of Public Prosecutions and another 2014 (5) SA 317 (CC)

- S v Makwanyane and Another 1995 (3) SA 391 (CC)

- Independent Newspapers (Pty) Ltd v Minister for Intelligence Services: In re Masetlha v President of the Republic of South Africa and another 2008 (5) SA 31 (CC)

- Shinga v The State (Soc of Advocates, Pietermaritzburg Bar as Amicus Curiae); O'Connell v The State 2007 (4) SA 611 (CC)