**REPUBLIC OF SOUTH AFRICA**

**IN THE HIGH COURT OF SOUTH AFRICA**

**GAUTENG DIVISION, PRETORIA**

**CASE NO: 25978/2017**

(1) REPORTABLE: YES
(2) OF INTEREST TO OTHER JUDGES: YES

**16 September 2019** **ROLAND SUTHERLAND**

In the matter between

| | |
|---|---|
| **AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC** | **First Applicant** |
| **SOLE, STEPHEN PATRICK** | **Second Applicant** |
| **and** | |
| **MINISTER OF JUSTICE AND CORRECTIONAL SERVICES** | **First Respondent** |
| **MINISTER OF STATE SECURITY** | **Second Respondent** |
| **MINISTER OF COMMUNICATIONS** | **Third Respondent** |

| | |
|---|---|
| **MINISTER OF DEFENCE AND MILITARY VETERANS** | **Fourth Respondent** |
| **MINISTER OF POLICE** | **Fifth Respondent** |
| **THE OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE** | **Sixth Respondent** |
| **THE OFFICE FOR INTERCEPTIONS 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** |
| **THE RIGHT2KNOW CAMPAIGN** | ***1st Amicus Curiae*** |
| **PRIVACY INTERNATIONAL** | ***2nd Amicus Curiae*** |

---

**JUDGMENT**

---

**SUTHERLAND J:**

**INTRODUCTION**

[1] There are two discrete questions raised in this matter.

[2] The first is a challenge to the constitutionality of several provisions of the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA) which statute permits the interception of communications of any person by authorised state officials subject to prescribed conditions.

[3] The second question is a challenge to the admitted practice of the State in conducting 'bulk interceptions' of telecommunications traffic on the basis that no lawful authority exists to do so. The National Strategic Intelligence Act 30 of 1994 (NSI) and the Intelligence Services Control Act 40 of 1994 (ISO) are implicated in the analysis of this issue.

[4] The two questions are addressed in turn, although much of the normative controversy that attaches to one or other question permeates the other question too.

[5] The parties to this case, where necessary to identify them individually, are referred to by their names as set out in the heading to this judgment. In support of the applicant's case, two *amici curiae* participated; Right2Know Campaign and Privacy International, represented by a single counsel. The Minister of Justice, the Minister of Defence and the Minister of Police were together represented by one set of counsel. A group of respondents forming the security cluster, ie, the Minister of State Security, the office for Interception centres, the national communications Centre, and the Parliamentary Joint Standing Committee on

Intelligence were represented by one set of counsel. The other respondents played no part in the hearing.

## PRELIMINARY CONTROVERSIES ABOUT THE APPLICATION

[6] There are three preliminary controversies which are addressed thus:

6.1 The argument that the application is premature.

6.2 The argument that the relief sought violates the separation of powers between the judicial arm and other legislative and executive arms of the state.

6.3 The argument that the application raises issues in the abstract and for that treason ought not to be entertained.

### Is the application premature?

[7] The respondents' argument is straightforward. The state is at work adapting RICA; leave it to get on with the task.

[8] First, it must be asked what is the State actually doing? In the answer given to Parliament by the Deputy Minister of Justice in 2017, vague remarks were made about consideration being given to amendments to RICA, which work would take about two years. That task was apparently not thought to be urgent as the distraction of the 2019 general election was alluded to as a reason why progress could not be quicker. The hearing took place a month after that event. When prompted by me for an up to date account of progress, an affidavit by Robbertze, a senior state law adviser, was produced during the hearing. He is the

lead person in the revision of RICA. He states that research of a comparative nature was carried out. Apparently, his team's recommendation is going to be that a new statute should replace RICA rather than a series of amendments; by implication this must mean a significantly novel approach to the subject matter in RICA. A first draft, it is said, "could" be finalised by 31 August 2019 to be followed by extensive public consultation. Save as mentioned, the affidavit is scrupulously bereft of any hint of the substance of such proposed legislation.

[9] It was said that the Deputy Minister's parliamentary answers in 2017 addressed the issues and the terrain of at least some of the criticisms ventilated in the application and, so it is argued, foreshadow consideration being given to the themes covered in the applicant's affidavits. Hence the exhortation to the court not to duplicate the work.

[10] The counter to this line of argument is that the State's efforts, in this regard, do not matter to the application. No sound reason exists, it is argued, not to prosecute the application, even if the August 2019 deadline could be taken seriously. Indeed, it is argued that the ventilation of the issues raised in the application can do no less than to inform the legislative process and contribute to the open and transparent debate over the value choices inherent in this type of law-making.

[11] In this regard, the authority in *Mazibuko v Sisulu* 2013 (6) SA 249 (CC) at [70] is invoked to argue that the purported imminence of reforming legislation could be no bar to the litigation. In that case the Rules of Parliament were at issue. The Constitutional Court held that the courts have no discretion to withhold a declaration of unconstitutionality if presented

with such a proven fact. The riposte to the invocation of this decision was that it is distinguishable on the facts. So it is. However, the point of importance is not similarity of the factual circumstances; rather, the point is that the Constitutional Court held that there can be no merit in delaying a challenge to the inconsistency of a statute with constitutional norms on the ground that a repair job on the statute is work-in-progress.

[12] Moreover, given the spirited resistance to almost every contention advanced by the applicant in criticising RICA, there can be no expectation that the reforming legislation, which we are told is being contemplated at this time, is in the least benign towards the criticisms advanced and solutions offered to address the criticisms.

[13] In my view, the argument of prematurity fails. If the provisions of RICA fall foul of the Constitutional norms, this court must pronounce on such issues, not prevaricate.

**Would granting the relief sought be judicial overreach?**

[14] Of the four issues raised about RICA, and the issue concerning bulk interceptions, the applicant seeks various forms of relief, some of it interim; eg in respect of the designated judge whose function in RICA is to authorise secret interceptions it is proposed that in order to demonstrate, convincingly, the independence of the designated judge, that the incumbent be appointed by the Judicial Service Commission, not the Minister of Justice, and that notice to a person who has been subjected to surveillance be given in order to facilitate an effective remedy for alleged abuse of the surveillance process. There are other examples in similar vein.

[15] The gravamen of the criticisms is that the several provisions of RICA oblige, or permit, conduct at odds with the constitution. Were a court to reach such a conclusion, no trespass into the domain of the executive or the legislature occurs. This outcome is plain because the state cannot perform any exercise of public power that is not authorised by a law, and in turn, that law must be constitutionally compliant.[1]

[16] The fact that the State is allegedly engaged in revision of the legislation has been addressed above. The subject matter of the challenge is not a ground for what is called deference to the policy making preserve of Parliament. True enough, as stated in *Case & Another v Minister of Safety and Security* 1996 (3) SA 617 (CC) at [73]: " ... our role is to review, rather than redraft legislation" Another caution was articulated in *Prince v Minister of Justice* 2017 (4) SA 299 (WCC) at [111] – [112] that our country is not a "juristocracy".

[17] But, in this case, no such danger exists. The critique is about the statute and its inadequacies. Either the provisions are compatible with the Constitution or they are not. Interim relief to ameliorate the unconstitutionality of a statute is no trespass onto the legislature's terrain.

**Are the challenges "in the abstract" ripe to be heard?**

[18] What restraints should a Court impose on itself when it is alleged a law is unconstitutional? The respondents join in protesting the propriety of the application *per se.* Their premise is that there is no factual basis laid for the attack on RICA, thus the challenge

[1] See: Pharmaceutical Manufacturers Association of South Africa & Others In Re Ex Parte President, RSA & Others 2000 (2) SA 674 (CC) at [20]

is in the abstract, which is said to be undesirable, ought to result in the application being dismissed on that ground alone. Two questions arise; first is it true that there are no facts and second, even if there were not any such facts to ground the critique, is not the very existence of a law that intrudes on rights sufficient, even if the challenge is in the abstract?

[19] Several examples of abuse of RICA are recounted in the founding affidavit. Among them is the undisputed first-hand experience of the deponent, Sam Sole, who, together with Adv Downer, a State Prosecutor, was spied upon. No rebuttal or explanation or effort to justify the interception is attempted. No good reason exists not to hear the matter on the facts alleged by Sole alone. Because Sole has no right to demand disclosure, he, being forbidden by RICA from being informed, the fact of the spying became public knowledge fortuitously. Sole's efforts to obtain details, plainly fruitless in the light of the prohibition on disclosure, were furthermore met with contemptuous responses and unsubstantiated allegations that no irregularities occurred. In my view, these facts, alone, take the matter out of the abstract.

[20] Secondly, it is common cause that at least one applicant, lied blatantly to a designated judge to obtain an interception order in respect of the journalists Hofstatter and Wa Afrika, claiming false that their details were that of criminals. The designated judge, doubtless in good faith, was taken in by the lies and authorised a surveillance for a corrupt purpose. [2]

[21] As to the other examples, all widely canvassed in the public domain, no rebuttals are offered that the interceptions were legitimate. Instead the faint response is that the reports are hearsay. Given the Constitutional values at stake in this litigation, that deflection leaves one

---

[22] An account is given of this sullied affair by Jane Duncan in "Communications surveillance is South Africa: The case of the Sunday Tines Newspaper." The Global Information Society Watch 224 -227.

unimpressed. The examples illustrate real vulnerabilities in the system, even if hearsay, and as illustrations of such vulnerabilities ought not to be ignored.

[22] However, even were the matter to be construed as being in the abstract, without these examples, it is, in my view, a proper case for full consideration. The upshot is that the distaste for deciding abstract issues is contingent on the circumstances of each case. Whether or not to engage on a given issue in the abstract has been the subject of several decisions. (eg: *Centre for Child Law v Minister of Justice* 2009 (6) SA 632 (CC) at [12] – [13]; *Savoi v NDPP* 2014 (5) SA 317 (CC) at [9] – [13]). These authorities make it plain that an abstract challenge is appropriate when legislation is challenged for unconstitutionality. In this case the principal challenges address aspects of the legislation which are alleged to display inadequate respect for Constitutional rights *per se*.

[23] Accordingly, in my view, the arguments about an abstract challenge must be answered in favour of the applicants.

## THE RICA CONTROVERSY

### *Introduction*

[24] The controversy about RICA is centred on the effect of the authorisation of interceptions on the Constitution's section 14 privacy rights, section 16(1) rights to freedom of expression and of the media, section 34 rights of access to a court, and section 35(5) rights to a fair trial.[3]

[3] These Constitutional provisions are:

[25] It is common cause that RICA and the bulk interceptions practice intrude on privacy section 14 rights. An important part of the controversy is whether an exercise involving section 36 and 39 of the Constitution can excuse the admitted privacy intrusions.[4] It is in dispute whether other rights alleged to be violated have indeed been compromised, but if so,

---

**Section 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.

**Section 16(1) Freedom of expression**

Everyone has the right to freedom of expression, which includes-

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

**Section 34 Access to courts**

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.

**Section 35(5)**

Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice.

[4]**Section 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.

**Section 39 Interpretation of Bill of Rights**

(1) When interpreting the Bill of Rights, a court, tribunal or forum-

*(a)* must promote the values that underlie an open and democratic society based on human dignity, equality and freedom;
*(b)* must consider international law; and
*(c)* may consider foreign law.

(2) When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.

(3) The Bill of Rights does not deny the existence of any other rights or freedoms that are recognised or conferred by common law, customary law or legislation, to the extent that they are consistent with the Bill.

the question is, again, whether an examination as contemplated by section 36 and 39 can excuse the violations so caused.

[26] There are four discreet challenges alleging unconstitutionality of RICA:

26.1 The absence in RICA of a right of notice to a person, who has been surveilled, of such surveillance.

26.2 The alleged shortcomings in RICA of the model of safeguards in respect of the selection of a designated judge to authorise surveillance operations and the procedures employed to facilitate the role of the designated judge.

26.3 The alleged shortcomings in the RICA model of safeguards concerning custody and management of information gathered by surveillance.

26.4 The alleged shortcomings in RICA of the model of safeguards to effectively:

26.4.1 preserve legal privilege in respect of lawyers and their clients, and,

26.4.2 preserve the confidentiality of the sources of investigative journalists

***A succinct overview of RICA***

[27] The aim and scheme of RICA is to protect privacy of communications subject to certain exceptions. The exceptions are a limited species of serious crimes or threats to national security. The tension between privacy and security of both individuals and society at large is acknowledged. The model has several attributes. Central to the model is the principle of accountability. This takes two main forms. First is the advent of the independent authority to give permission to intercept – the designated judge or, in certain cases, any other judicial

officer. Second, a bureaucratic edifice is constructed in which officials are required to record and report on their activities.

[28] RICA was enacted 2002, self-evidently, composed to address what was understood to be the character of the telecommunications environment of that time. Seventeen years later, that environment has evolved. Technological possibilities and awareness of the scope of such possibilities in 2019 are different and so are the habits of those who seek the utilisation of telecommunications technology to their own advantage. The risk of abuse by criminal and other nefarious elements was expressly recognised by a default prohibition on the interception of signals or storing the content of communications.

[29] Thus, a prohibition of interception is the point of departure, reflecting the privacy norm embodied in section 14 of the Constitution. Naturally, it was recognised that there were also honourable motives to intercept communications. Therefore, exceptions to the prohibition are created for law enforcement officers and security officials in the execution of their duties. Serious crimes and espionage, rather than petty crimes, could justify an interception.

[30] The intrusive nature of such a power was fully recognised and a model of safeguards was built into the statute. Officials of the state alone could intercept communications. These officials had to, as a general rule, make application for permission to intercept a given person's communications. In these applications the need to take such a step had to be motivated. In a limited number of instances, where circumstances of urgency could justify

intercepting a communication before getting permission, such presumptuous conduct had to ratified *ex post facto*.

[31] The information so derived may not be broadcast to anyone, save authorised persons. The persons being surveilled are not notified and indeed notification to them is expressly forbidden. In practice, the fact of a surveillance exercise would remain secret forever unless it was brought up in court proceedings to be used a proof of misconduct by the persons surveilled or persons linked to them.

[32] The "designated judge" who evaluates these applications and issues the permission to surveil a person is a "retired judge", and thus by implication an experienced judge.[5] The designated judge is selected by the Minister of Justice, at his discretion, and serves for fixed but renewal terms. The designated judge is remunerated for this work. Annually a report must be tabled in Parliament by the designated judge about this work.

[33] This regime operates, as described, in respect of real-time surveillance. However, law enforcement had also the option of examining a person's communications history. Service providers of telecommunications products such as Vodacom, MTN, Cell-C and others are subject to statutory obligations about the storage of the content of data transmissions which are to be kept available to law enforcement and the security forces of the state for prescribed periods. The Minister of Justice is authorised to prescribe the duration for which it must be kept accessible This practice facilitates *ex post facto* examination of past communications.

---

[5] The allusion to a 'retired' judge is slightly misleading. The category of judges from which the designated judges are drawn include persons who have been relieved of active service but who are still liable for judicial service for a period, typically, of five years, thereafter until they reach 75 years of age and other judges who have indeed retired.

[34] An agency, the Office for Interception Centres (OIC) is created. It is headed by a director who is vested with various powers over the operations of the centres.

[35] What does a qualitative assessment of RICA yield? The value of privacy is privileged and expression is given to the idea that where exceptions to respect for privacy are to be allowed, a high threshold of justification is stipulated. Self-evidently, to trespass into the private realm is permissible only to the extent that a superior claim to do so can be made out on grounds of necessity. This implies that other means to achieve the aims of the interception would have been ineffective, and the gravity of the circumstances outweighs the primary value of privacy. The safeguards model recognises the need for an independent authority to approve interceptions. This model, in which the person desiring the interception is distinct from the person authorising it, is designed to prevent, as far as possible, abuse of the system. Self-evidently, the approving authority's efficacy in achieving this aim is dependent on the information made available to that authority, ie the designated judge.

## OVERVIEW OF THE FOUR SPECIFIC CHALLENGES TO RICA AND THE APPROACH TO DETERMINE A CONFLICT WITH THE CONSTITUTION

[36] The approach to the test for constitutionality of a law is in two stages. The first is to determine the violation *per se* of the right. In this case, it is common cause that section 14 rights to privacy are violated. The second stage is an examination of the character of the violation and its rationale. Although privacy is the primary right violated, it is also alleged that freedom of expression and of the media, legal privilege, and access to courts rights are also violated.

[37] Section 36 requires that a subtraction from the constitutionally guaranteed right must be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors. Of especial importance in the debate has been subsection 36(e)[6] on a minimum intrusion compatible with the needs of the exception. In this regard the injunctions in section 39 are pertinent, and much material has been put before the court in this regard, to which reference shall be made where necessary. In *Independent Newspapers (Pty) Ltd v Minister for Intelligence In Re Masetla v President, RSA* 2008 (5) SA 31 (CC) at [45] such measures were described as needing to be :

" .... properly tailored and proportional to the end it seeks to attain..."

[38] Moreover, in *Gaertner v Minister of Finance 7 Others* 2014 (1_) SA 442 (CC) at [47] – 73] the issue was extensively addressed in the context of search and seizure powers of customs officials. At [67] – [68] it was held:

> "The relation between the limitation and its purpose
>
> [67] There must be a rational connection between the purpose of the law and the limitation imposed by it. In broad terms, that rational connection does exist between the limitation at issue here and the provision's purpose. The tight regulation of the customs-and-excise industry is enforced through inspections. Intrinsically, inspections of this kind are still intrusive, although they must be somewhat tolerable in respect of business premises. But this is something that participants in the industry must be content with if compliance with the Customs and Excise Act is to be achieved. It is in this context that the limitation of the right to privacy must be understood.
>
> Less restrictive means to achieve the purpose
>
> [68] It is difficult to see how the achievement of the basic purposes of the Customs and Excise Act requires that inspectors be allowed to enter private homes and inspect documents and possessions at will. The fact that the Customs and Excise Act is manifestly in the public interest in no way diminishes the need to protect and uphold the privacy and, indeed, dignity of individuals where — as in the case of private dwellings — these rights are by no means attenuated."

[6] Cited supra, footnote 2.

[39] The safeguards model is heavily dependent on the role of the designated judge. But the judge's role and scope to effectively prevent abuse is tied up with the rationale to intercept and the ramification of that rationale in some respects limit what the judge can do; ie, the judge has to work in secrecy, not the typical public judicial terrain.

[40] What does the applicant want as a renovated model? It wants a system where the visible independence of the designated judge is enhanced by an independent selection of the incumbent by the Judicial Service Commission, and the work process of the designated judge is assisted by a public advocate to introduce an adversarial element into the process of evaluation. Moreover, because, implicitly, even these measures cannot eliminate the risk of abuse, a right of notice after the cessation of the interception to facilitate at least a damages claim for improper violation of privacy. Moreover, the storage of data must be reduced from a minimum period of three years to maximum of 6 months. The statute itself should stipulate the management of the data collated rather than be left to subordinate regulation and administrative discretion. The peculiar needs for confidentiality of lawyers and journalists must be addressed with especial restraint in respect of the interception of their communications and, if a real need to intercept their communications exists, in a given instance, an intermediary should filter the communications to exclude what properly is covered by legal privilege or an investigative journalist's confidential source. It is a model bearing these attributes which is constructed to contrast the inadequacies of the present model.[7]

[7] In most respects, the stance adopted by the applicant is derived from the paper prepared by A mare and J Duncan for the Media Policy and democracy Project under the title; "An Analysis of the communication surveillance legislation framework in South Africa". The paper exhorts reform to align the South African legislation with the "Necessary and Proportionate Principles" sponsored by the United Nations Human Rights Council.

**CHALLENGE NO 1:**

**THE ABSENCE OF A RIGHT TO BE NOTIFIED THAT ONE HAS BEEN SUBJECTED TO SURVEILLANCE:**

**(SECTIONS 14 AND 34 OF THE CONSTITUTION; SECTION 16 OF RICA)**

[41] The criticism proceeds from the premise that interceptions *per se* can be justified. Section 16(7)(a) of RICA forbids any disclosure to the subject of the surveillance. The notion of pre-interception notice is self-evidently problematic; the idea is vulnerable to a cogent argument that to do so defeats the very purpose of the exercise. Thus, the focus of the application is on a *post-surveillance notice*.

[42] This is no novel concern. In *Klass v Germany ECHR [1978] 5029/71*, the ECHR recognised the unhappy need for surveillance but nevertheless observed that one cannot undermine democracy on the grounds of defending it. It was held at [50] that:

> "The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse."

[43] In broad terms, once it is assumed that secret surveillance is capable of justification, the controversial terrain is the risk of abuse, whether by zealous or corrupt officials. Such a risk is not academic in South Africa.[8] The whole safeguards model built into the statute must be examined and the presence of or absence of a right to notice is only one aspect of that model. Subject to that contextual caution, the absence of a right to notice means, logically, that the subjects of the surveillance who have wrongly had their privacy violated have no opportunity to initiate steps in a court to seek relief in respect of the abuse. Thus, the right of access to the courts as contemplated in section 34 of the constitution is indeed compromised.

---

[8] See, eg: the examples of abuse or unexplained interception (supra).

In this sense the right of notice is critically instrumental in securing a section 34 right. After all, there can be no right without a remedy. Much of the debate centred on this notion. In *Klass* (supra) at [36] it was held:

> "The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the [European] convention [ie article on 8 privacy rights] could be thus removed by the simple fact that the person concerned is kept unaware of its violation."

[44] The challenge supposes that the purpose of RICA can be achieved without a total ban on post-surveillance disclosure. The respondents stand fast on a total ban. At its extreme, it was contended that the Constitution confers no right of notice. The contention is misconceived; it would not be expected for such a right to be expressed in the Constitution itself. As alluded to, notification is critically instrumental to securing a section 34 right and thus at the functional level is implicated in the securing of that right.

[45] The consequent enquiry must be whether there is a cogent case for perpetual secrecy of the surveillance that outweighs a section 34 right read with section 14. It may be assumed that sometimes there may be a proper case for perpetual secrecy, and if that case can, on sound grounds be shown, the authority supervising the surveillance, ie the designated judge, must be persuaded to order a deferral of notice for a specified period, in much the same way an authorised interception is valid for three months and is renewable. Such deferrals, refreshed for as long as the case to defer holds good, would mean, in a given extreme example, forever. This scenario is capable of contemplation in the case of treasonable espionage where exposure might truly threaten the national interest, but less so in the case of criminal activities. Nonetheless, it could mean very long periods, stretching to many years and notionally extend even after the death of the subject.

[46] It was argued that a suit at law cannot be established to provide an adequate remedy against past surveillance. This perspective is incorrect; obviously there is no remedy to *prevent* the intrusion, but, at very least constitutional damages, *ex post facto*, for an improper intrusion ought to be available.[9] Whether the impropriety contaminating the decision to surveil or the manner in which it was carried out or how the information derived was used or abused flows from false information provided to the designated judge, or inadequate scrutiny by the designated judge, and whether the irregularities were the result of conscious abuse or merely negligence or a failure to properly apply one's mind to the relevant circumstances is immaterial to this consideration. In cases where propriety prevailed no harm to any legitimate interest can occur; where impropriety attaches, the opposite is true. Notionally, even an irregularity might be legitimately concealed if a proper case exists, but these extreme examples must not be allowed to prevent due redress where fair and feasible.

[47] There are examples in Canada and USA where a post surveillance notice is given within 90 days after surveillance if is decided it is appropriate to do so.[10] In Japan, the period

---

[9] See, eg: Ngomane & Others v City of Johannesburg [2018] ZASCA 57 (SCA)

[10] Section 196 (1) of the Criminal Code of Canada provides:

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

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

> "8(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518 (7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

to notify is 30 days after surveillance. The norm is that unless reasons exist not to give notice, notice will be given. An independent authority makes that judgment call.

[48] Two obvious considerations flow from these examples; first, it is a practice in other democratic societies, and second it is indeed a mechanism that serves to ameliorate the intrusions into the privacy of persons because it affords redress by a court, if an abuse occurs.

[49] In the jurisprudence of the ECHR a post surveillance notice is an essential ingredient of a surveillance model that complies with article 8 of the European Convention of Human Rights which article guarantees privacy. In Germany, as in USA and Japan, a right to a notification, after it is safe to do so, is mandatory. See: *Klass v Germany (Supra) at [19]; Weber & Saravia v Germany* [2008] 46 EHRR SE5; [2006] ECHR 1173 at [51] and at [133-135]. Russia, which lacked such a right to notice was held to have violated article 8; see *Zakharov v Russia* [2016] 63 EHRR 17 at [289] – [291] and [298] – [302].

[50] The tenor of that jurisprudence is captured in this passage from *Klass v Germany*:

> "58. In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted

---

(1) the fact of the entry of the order or the application;
(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.
The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed."
(Emphasis added.)

> the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the "interference" resulting from contested legislation is in principle justified under Article 8 para 2 (art. 8 – 2) (see paragraph 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the "interference". Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction (see paragraphs 11 and 19 above).
>
> 59. Both in general and in relation to the question of subsequent notification, the applicants have constantly invoked the danger of abuse as a ground for their contention that the legislation they challenge does not fulfil the requirements of Article 8 para 2 (art. 8 – 2) of the Convention. While the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system, the considerations that matter for the purposes of the Court's present review are the likelihood of such action and the safeguards provided to protect against it."

[51] What is to be made of these considerations? Plainly, the illustration of the right to notice in other jurisdictions demonstrates that world opinion has embraced this right as a facet of a democratic social order, subject to safeguards against undoing the very objectives of legitimate surveillance. What is there to the SA condition that would justify a rejection of a post interception notice, subject to the judge authorising delays for good cause shown? None have been shown. Indeed, the two examples, one of clear abuse and the other of unexplained spying alluded to, point in the other direction. The resistance has been directed at circumstances which would justify a ban on notification; an absolutist stance.

[52] Thus, as contemplated by the exercise dictated by section 36 of the Constitution to determine whether or not less restrictive means exist to achieve the purpose of RICA, in my view, the need for protection from abuse through accountability before a court can be effected practicably, by a post surveillance notification as is the case in other democratic societies.

[53] The applicant seeks the following declaration:

> "It is declared that:
>
> (a) RICA, including sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe procedure for notifying the subject of the interception;
>
> (b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and
>
> (c) Pending the enactment of legislation to cure the defect, RICA shall be deemed to read to include the following additional sections 16(11) and (12):
>
> > '(11) The applicant that obtained the interception direction shall, within 90 days of its expiry, notify in writing the person who was the subject of the interception and shall certify to the designated judge that the person has been so notified.
> >
> > (12) The designated judge may in exceptional circumstances and on written application made before the expiry of the 90 day period referred to in sub-section (11), direct that the obligation referred to in sub-section (11) is postponed for a further appropriate period, which period shall not exceed 180 days.'"

[54] Immediate interim relief is self-evidently appropriate. Save with one qualification, in my view, the proposed interim text is appropriate. The cruel fact must be recognised that a deferral of notice in *de facto* perpetuity is sometimes legitimate. That is, of course, an extreme position. For that reason I would add a proposed (13). That text would go hand in hand with a tail to proposed subsection (12) to read: " ....exceed 180 days at a time." The text of (13) would read:

> "In the event that orders of deferral of notification, in total, amount to three years after surveillance has ended, the application for any further deferral shall be placed before a panel of three designated judges for consideration henceforth, and such panel, as constituted from time to time, by a majority if necessary, shall decide on whether annual deferrals from that moment forward should be ordered."

**CHALLENGE NO 2:**

**THE DESIGNATED JUDGE AND THE PROCESS OF EVALUATION OF AN APPLICATION**

[55] The model of safeguards, alluded to in broad terms earlier, has as its centre piece a 'designated' judge who authorises interceptions both in real time and of archived communications. Section 16 is the pivotal provision in this system and is the key target of the criticism which is examined hereafter. Delving into stored communications is also regulated by section 19 and applications to access them may, in addition to the designated judge, be granted by any judge or magistrate, who must thereafter report the fact of an authorisation to the designated judge, though ostensibly need not report rejected applications.

[56] A designated judge is defined thus:

> " .... 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"

[57] The pool of eligible persons is therefore composed of experienced jurists and the persons carry with them the cache of such public record. Plainly, restricting the pool of eligibility to such persons is a crucial dimension of the credibility of what is represented to the citizenry as the epitome of independence, impartiality, legal knowledge and decision making skill.

[58] The provisions of section 16(4) – (7) stipulate what a designated Judge must do. These provisions are substantially replicated in sections 17, 18 and 19, these sections all dealing with one or another kind of interception.

[59] Section 16 is long and labyrinthine and provides thus:

"Application for, and issuing of, interception direction

(1) An applicant may apply to a designated judge for the issuing of an interception direction.
(2) Subject to section 23 (1), an application referred to in subsection (1) must be in writing and must-

*(a)* indicate the identity of the-

(i) applicant and, if known and appropriate, the identity of the law enforcement officer who will execute the interception direction;

(ii) person or customer, if known, whose communication is required to be intercepted; and

(iii) postal service provider or telecommunication service provider to whom the direction must be addressed, if applicable;

*(b)* specify the ground referred to in subsection (5) *(a)* on which the application is made;

*(c)* contain full particulars of all the facts and circumstances alleged by the applicant in support of his or her application;

*(d)* include-

(i) subject to subsection (8), a description of the-

*(aa)* nature and location of the facilities from which, or the place at which, the communication is to be intercepted, if known; and

*(bb)* type of communication which is required to be intercepted; and

(ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception;

*(e)* if applicable, indicate whether 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: Provided that this paragraph does not apply to an application for the issuing of a direction in respect of the ground referred to in subsection (5) *(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;

*(f)* indicate the period for which the interception direction is required to be issued;

*(g)* indicate whether any previous application has been made for the issuing of an interception direction in respect of the same person or customer, facility or place specified in the application and, if such previous application exists, must indicate the current status of that application; and

*(h)* comply with any supplementary directives relating to applications for interception directions issued under section 58.

(3) An application on a ground referred to in-

*(a)* subsection (5) *(a)* (i), must be made by an applicant referred to in paragraph *(a)*, *(d)* or *(f)* of the definition of 'applicant';

*(b)* subsection (5) *(a)* (ii) or (iii), must be made by an applicant referred to in paragraph *(b)* or *(c)* of the definition of 'applicant';

*(c)* subsection (5) *(a)* (iv), must, in the case of-

(i) the investigation of a serious offence, be made by an applicant referred to in paragraph *(a)* or *(d)* of the definition of 'applicant'; and

(ii) the gathering of information, be made by an applicant referred to in paragraph *(c)* of the definition of 'applicant'; and

*(d)* subsection (5) *(a)* (v), must be made by an applicant referred to in paragraph *(e)* of the definition of 'applicant':

Provided that an applicant referred to in paragraph *(f)* of the definition of 'applicant' may only make an application on the ground referred to in subsection (5) *(a)* (i)-

(i) if the offence allegedly has been or is being or will be committed by a member of the Police Service; or

(ii) in respect of a death in police custody or as a result of police action.

(4) Notwithstanding section 2 or anything to the contrary in any other law contained, a designated judge may, upon an application made to him or her in terms of subsection (1), issue an interception direction.

(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.

(6) An interception direction-

*(a)* must be in writing;

*(b)* must contain the information referred to in subsection (2) *(a)* (ii) and (iii) and *(d)* (i);

*(c)* may specify conditions or restrictions relating to the interception of communications authorised therein; and

*(d)* 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.

(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.

(8) The requirements of subsections (2) *(d)* (i) *(aa)* and (5) *(b)* (ii) relating to the description of the facilities from which, or the place at which, the communication is to be intercepted do not apply if, in the case of an application for the issuing of an interception direction which authorises the interception of-

*(a)* a direct communication-

(i) the application contains full particulars of all the facts and circumstances as to why such description is not practical;

(ii) the application indicates the identity of the person whose communication is required to be intercepted; and

(iii) the designated judge is satisfied, on the facts alleged in the application, that such description is not practical; and

*(b)* an indirect communication, the-

(i) application indicates the identity of the customer whose communication is required to be intercepted;

(ii) applicant submits proof that there are reasonable grounds to believe that the actions of the customer concerned could have the effect of preventing interception from a specified facility;

(iii) designated judge is satisfied that sufficient proof has been submitted; and

(iv) interception direction authorises the interception only for such time as it is reasonable to presume that the customer identified in the application is or was reasonably close to the instrument through which such communication will be or was transmitted.

(9) The interception of a communication under an interception direction to which the requirements of subsections (2) *(d)* (i) *(aa)* and (5) *(b)* (ii) do not apply by reason of subsection (8) *(a)* may not take place until the place at which the communication is to be intercepted is determined by the authorised person who executes the interception direction concerned or assists with the execution thereof.

(10)

*(a)* A telecommunication service provider to whom an interception direction referred to in subsection (8) *(b)* is addressed, may in writing apply to a designated judge for an amendment or the cancellation of the interception direction concerned on the ground that his or her assistance with respect to the interception of the indirect communication cannot be performed in a timely or reasonable fashion.

*(b)* A designated judge to whom an application is made in terms of paragraph *(a)* must, as soon as possible after receipt thereof-

(i) inform the applicant concerned of that application; and

(ii) consider and give a decision in respect of the application."

[60] A reading of this provision cannot leave the reader under the impression that the drafter did not go to some lengths to construct a model that had, as its aim, several safeguards. Without regurgitating the section itself, the eligible applicants are in a select

class, the applicant is required to give 'full particulars' upon which reliance is made, the target is to be unambiguously identified, why other measures are inadequate to procure the desired information must be stated, the crime alleged must be serious, the prospects of a successful yield from the interception must be motivated, and the designated judge must interrogate the application to become satisfied it is justified, and may authorise interceptions subject to conditions. Notwithstanding these stipulations and the reporting obligations in respect of authorisations there are allegations of inadequacy raised against the model.

[61] The particular criticism of the model, being considered now, falls into two parts; first, that the independence of the designated judge is compromised by the selection process and *de facto* unlimited duration of appointment, and second, the absence of an adversarial process compromises the efficacy of the judicial role. These issues are addressed in turn.

***Independence of the designated judge***

[62] The role of the minister of justice in selecting a judge to designate, at the minister's discretion alone, to perform such an inherently contentious function, carried out in secrecy, for a *de facto* indefinite term of service, through renewals thereof, for additional remuneration is argued to be an anathema to independence of the designated judge. The stark contrast with the regular judicial role of open performance and the publishing of orders to the world is emphasised. The secrecy of the process is aberrant to the usual judicial role and thus a greater need, it is argued, exists to bolster the perceived and actual independence of the incumbent. The present system, it is argued, fails dismally.

[63] These criticisms are not met with any serious rebuttal. The argument advanced to counter the criticism is that it is the job of a judge to be independent. This true, but is no answer to the point. Moreover, it is pointed out that in UK, Australia and Canada the role is performed by an official not a judge, a submission which seems to me to be a *non sequitur*. Other unpersuasive arguments about the persons who have been incumbents and their supposed honourable attributes are in my view, wholly beside the point. Further, the proposition that the ministerial role in the appointment (nominally, by the President) of judges to serve on commissions of enquiry serves as a useful comparison is inherently misconceived.

[64] Perhaps the critical dimension of the impropriety of a judge serving in any capacity at the pleasure of a minister of state is aptly illustrated by the development of the institutional independence of the judiciary since 2002 when RICA was legislated. The present appointment process of the designated judge is plainly on the wrong side of history. The remedy suggested is that the JSC should appoint the designated judge and indeed appoint not one, but a panel to serve non-renewable terms. By such means, it is argued, the judicial flavour of the appointment can be assured.

[65] The arguments draw on remarks made in the Constitutional Court. In *Glenister II at [207]* it was held in respect of the saga about the institutional independence of the Scorpions:

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

[66] The duration of the appointment is also said to be an aspect which compromises independence because it is renewable. The device of a non-renewable term of office is already well known as a measure to bolster independence, for example in the case of the Public Protector. It is argued that it is appropriate that a similar approach be applied in the case of a designated judge. The appointment must not be capable of being perceived as a sinecure that might induce, if only subliminally, an appetite to appease. Remarks by the court in *Helen Suzman Foundation v President, RSA: in re Glenister v President, RSA 2014*(4) BCLR 841 (WCC) at [68] are cited in support:

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

[67] A further criticism is that a panel of designated judges should be appointed not a single person. The functional implications of such a model are significant. An application would be heard by more than one person with the benefit of different perspectives or insights being brought to bear. These thoughts are addressed in the next part of this judgment.

[68] In my view, it must be an embarrassment to the Minister of Justice to have to select and appoint the designated judge in terms of the present provisions of RICA.

[69] The remedy proposed is this:

> "It is declared that:
>
> (a) RICA, including the definition of 'designated judge' in section 1, is

inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe an appointment mechanism and terms for the designated judge which ensure the designated judge's independence;

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

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

> 'any judge of a High Court discharged from active service under section 3 (2) of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act 47 of 2001), or any retired judge, who is appointed by the Judicial Service Commission for a non-renewable term of two years to perform the functions of a designated judge for purposes of this Act'."

[70] I am not convinced that the full extent of such interim relief is appropriate. The policy choice to have the Judicial Services Commission appoint the designated judges is ostensibly a viable and sensible option, but ought to enjoy greater degree of reflection in order that a process to govern it be put in place. That is highly problematic as an interim measure. In the meantime, a more pragmatic option presents itself.

[71] In my view, the Minister of Justice should, in the interim, continue to appoint the designated judges, however, the appointees should be nominated by the Chief Justice and the Minister should be obliged to accept the nominations. Thus the relief which, in my view, is appropriate is thus:

> "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 nominated by the Chief Justice and upon which nomination is appointed by the minister of Justice for a non-renewable term of two years to perform the functions of a designated judge for purposes of this Act'."
> (Underlining indicates my amendment to the relief sought)

***The Case for a Public Advocate or Other means to overcome lack of audi alterem partem***

[72] The second leg of the criticism is the absence of a prescribed procedure for proper evaluation of the information placed before the designated judge and of the interests of the persons adversely affected by such potential authorisation. This, it is argued, implicates section 34 rights to a fair hearing. In keeping with our adversarial tradition, it is argued that a public advocate be invented to fulfil this role of devil's advocate. By such means the designated judge can, in a more familiar and traditional judicial process, have a range of considerations ventilated by two parties and thus the duty to apply one's mind can be more fruitfully achieved. Allusion is made to the practice in USA where a public advocate may be called for, but is not in that country, a default procedure.

[73] The thrust of the argument is therefore that less restrictive measures can be out in place to achieve the objectives of RICA. More significantly, the thesis advanced assumes that a means can be constructed to prevent an unjust or unmeritorious authorisation of interception, a consideration supplementary to the notion of *ex post facto* notification to facilitate a review of an inappropriate interception.

[74] Perhaps the most basic underlying problem with this idea is that the very process, in its conception, excludes *audi alterem partem*. If the case is to be argued on the premise that it is legitimate to spy secretly on persons in given limited circumstances, then can one intelligibly factor back into that process a legitimate claim for *audi alterm partem*? I think not. However, that "right" ought to be distinguished from an equally basic issue which is the condition upon which the secret spying process can be justified; ie fundamental values are reluctantly trampled on with as a light a tread as possible.

[75] In countering these criticisms, two lines of argument are advanced.

[76] First, it is argued that, at a practical level a public advocate, can do no more than a diligent judge would in any event do. The diligence of the judge ought to be assumed for the purpose of the analysis and the presence of such an attribute would, it is to expected, be among the considerations of the appointing authority in selecting the person so designated. The judicial appreciation of the facts alleged is enhanced, so it is argued, by the duty on an applicant to behave as counsel are expected to do in *ex parte* applications and make truly full disclosure including factors adverse to the success of the application. In my view, it is not apparent that the applicants for these authorisations understand their ethical responsibilities in this way.

[77] Second, there is no room for testing 'evidence' in these applications; ie some degree of faith has to be put in the applicants' integrity. It is a fair point that the public advocate, bereft of instructions from the subject and perforce relying on no more than what is laid out in the application might be able achieve very little of real value. Indeed, the primary area of assistance that a public advocate could offer is in the form of posing interrogatives that the designated judge could embrace and put to the applicants. Such a process would doubtless be useful, but it is not obvious that it is necessary in order to achieve a fair evaluation of the application, given the limitations imposed on the public advocate. Indeed knowing no more than an experienced judge, is it likely the judge would not consider aspects that the public advocate would raise?

[78] The Respondents objections to a public advocate include the security risks of involving other persons. This is a real problem and thus a proper consideration. Who should they be? How should they be selected, vetted, and briefed to study the applications? What implications are there in respect of timing and accessibility?

[79] The example from the USA of the utilisation of a public advocate (called in the US an *amicus curiae*) is not a default position. Under the provisions of the US Freedom Act, an *amicus* may be called for. This is ostensibly sparingly done and only when a novel law point arises.[11] The impression made on me by this information is that the limited role of the *amicus* is to aid the development of jurisprudence rather than address the merits of a given application.[12]

[80] An alternative to a public advocate might be that a panel of designated judges, as alluded to above, have regard to an application. That might overcome the risk of tunnel vision and ensure a diversity of perspectives in the evaluative process. If three designated judges, say, were appointed and two had to approve an authorisation, might that not be a better solution to balancing security of the information with the need to intensively interrogate the application?

[81] Save to conclude that measures are needed to overcome the absence of adversarial process, in my view the criticism cannot be taken further. There may be many options, including some not ventilated here.

---

[11] See: Reports of the Administrative Office of the United States Courts, 25 April 2018 on the year 2017 and 25 April 2019 on the year 2018.

[12] See; C Squitieri "The Limits of the Freedom Act's amicus Curiae" *Journal of Law, Technology and Arts vol 11 Fall 2015, issue no 3, 198 -210.* The author is critical of the efficacy of the amicus owing to its limited role and distinguishes it from a 'special advocate' as desired by some proponents of freedom from surveillance, which is akin to what is sought in the form of a "public Advocate" by the applicant.

[82] The relief sought is thus:

> "It is declared that:
>
> (a) RICA, including sections 16(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to provide for a system for a public advocate or other appropriate safeguards to deal with the fact that the orders in question are granted ex parte; and
>
> (b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect."

[83] In my view the prayer sought minus the underlined text is appropriate.

**CHALLENGE NO 3:**

**THE ARCHIVING OF DATA AND ACCESSIBILITY OF ARCHIVED COMMUNICATIONS**

**(Sections 30, 35 and 37 of RICA)**

***General considerations***

[84] RICA envisages two forms of intrusion into the communications of a person. One is a real time interception of communications. These communications are of course recorded and then stored at statutory Interception Centres. The other form of intrusion is into past communications.

[85] Service providers of telecommunications are obliged to retain all data for a period prescribed by the Minister, exercising a discretion, in terms of section 30(2) of RICA, between a minimum of three years and a maximum of five years. The current prescription is three years. In short, all of a person's personal telecommunications, up to three years past, lie in wait for the state to pry into, if its officials convince a judicial officer to authorise access.

In addition, the Director of the Office for Interception Centres is vested with responsibilities concerning the aspect of storage and management.

[86] The scope of RICA itself in regard to this aspect of the surveillance model is captured in Sections 30, 35 and 37:

**Section 30:**

Interception capability of telecommunication services and storing of communication-related information

(1) Notwithstanding any other law, a telecommunication service provider must-

*(a)* provide a telecommunication service which has the capability to be intercepted; and

*(b)* store communication-related information.

(2) The Cabinet member responsible for communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and the telecommunication service provider or category of telecommunication service providers concerned, must, on the date of the issuing of a telecommunication service licence under the Electronic Communications Act, to such a telecommunication service provider or category of telecommunication service providers-

*(a)* issue a directive in respect of that telecommunication service provider or category of telecommunication service providers, determining the-

(i) manner in which effect is to be given to subsection (1) by the telecommunication service provider or category of telecommunication service providers concerned;

(ii) 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 the-

*(aa)* interception of indirect communications in terms of this Act; and

*(bb)* storing of communication-related information in terms of subsection (1) *(b)*; and

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

*(b)* determine a period, which may not be less than three months and not more than six months from the date on which a directive referred to in paragraph *(a)* is issued, for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.

(3) A directive referred to in subsection (2) *(a)*-

*(a)* must, where applicable, prescribe the-

(i) capacity needed for interception purposes;

(ii) technical requirements of the systems to be used;

(iii) connectivity with interception centres;

(iv) manner of routing duplicate signals of indirect communications to designated interception centres in terms of section 28 (1) *(b)* (i); and

(v) manner of routing real-time or archived communication-related information to designated interception centres in terms of section 28 (2) *(a)*; and

*(b)* may prescribe any other matter which the Cabinet member responsible for communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority, deems necessary or expedient.

(4) Notwithstanding any other law, agreement or licence, a telecommunication service provider must, subject to section 46 (1) *(a)*, at own cost acquire, whether by purchasing or leasing, the facilities and devices determined in a directive referred to in subsection (2) *(a)*.

(5) ....(6) ....

(7) The Cabinet member responsible for communications must, within two months after the fixed date and in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and a telecommunication service provider or category of telecommunication service providers to whom, prior to the fixed date, a telecommunication service licence has been issued under the Electronic Communications Act-

*(a)* issue a directive referred to in subsection (2) *(a)* in respect of such a telecommunication service provider or category of telecommunication service providers; and

*(b)* determine a period, which may not be less than three months and not more than six months from the date on which a directive referred to in paragraph *(a)* is issued, for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.

(8) ....

**Section 35(1):**

Powers, functions and duties of Director

(1) In order to achieve the objects of this Act, the Director-

*(a)* must carry out the administrative duties relating to the functioning of the Office;

*(b)* must exercise control over heads of interception centres and staff of the Office;

*(c)* must manage, and exercise administrative control over, interception centres;

*(d)* must regulate the procedure and determine the manner in which the provisions of this Act must be carried out by interception centres;

*(e)* must co-ordinate the activities of interception centres;

*(f)* must prescribe the information to be kept by the head of an interception centre in terms of section 37, which must include particulars relating to-

(i) applications for the issuing of directions and the directions issued upon such applications which is relevant to the interception centre of which he or she is the head; and

(ii) the results obtained from every direction executed at that interception centre;

*(g)* must prescribe the manner in, and the period for, which such information must be kept; and

*(h)* is, for purposes of the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, accountable to the Minister.

**Section 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).

[87] The Minister's directives, published in *GN 1325 of 2005,* run to 84 pages prescribing separately what mobile operators and internet providers must do. The directive addresses security concerns. There are injunctions to forbid unauthorised dissemination, require the minimum number of staff to be engaged in interceptions, and to require a record of all access-events. In addition, the SAPS has crafted "internal procedures" which were described in an affidavit but a copy was not produced in the litigation.

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

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

89.2 Second, having accessed and stored this material in servers at Interception Centres, RICA *per se* is bereft of appropriate injunctions on how it is to be managed and used and by whom it may be accessed; the directives issued about such management are said to be inadequate to meet the need to be an effective safeguard against abuse or impropriety. In this regard, the contention draws on the report of the office of the UN high commissioner for Human Rights report of 30 June 2014:

> [29] Consequently, secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the pubic concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.

[90] The *amicus* contends the very act of storage is *per se* unconstitutional but points out that that is not the case pleaded by the applicant. Thus, as the amicus correctly contends, this court ought not to consider that point, and ought to confine itself to the case the respondents were required to meet, ie that, in general, less intrusive means would suffice to satisfy

RICA's legitimate aims and, once having intruded, safeguarding the communications and appropriate management thereof is vital.

[91] The Report of the UNHRC[13] on the South African model was invoked to support the criticisms.

> "42. The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Relation of Interception of Communications and Provisions and Provision of Communications Related Information Act (RICA). It is also concerned about the wide scope of the data retention regime under the Act. The Committee is further concerned at reports of unlawful surveillances practices....."
>
> "43. The State party should take all necessary measures to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality. The State party should .... consider revoking or limiting the requirement for mandatory retention of data by third parties. It should also ensure that interception of communications by law enforcement and security services is carried out only on the basis of the law and under judicial supervision. The State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies."
>
> (Underlining supplied)

[92] The two prongs of attack are now addressed.

***Duration of archiving***

[93] The choice of duration for the archiving of data is problematic in several respects. In general, it seems that SA has a longer period of lawful retention; ie 3-5 years than countries to whose regimes I was referred. Australia caps the period at two years; other jurisdictions cap it at between 1 year and 6 months duration. The contention is that the shortest possible period necessary to achieve RICA's aims is the appropriate limit if privacy rights are given

[13] Portions excised do not address the specific issue being addressed in this part of the judgment.

due regard. This proposition is *per se* not contested. The real locus of the debate is *what is a necessary period* in South Africa?

[94] In my view, it does no injustice to the limitations enquiry to recognise that in determining a duration, the choice of a period is one about which reasonable people may disagree. It is argued by the Minster of Justice that criminal investigations in SA tend to take longer than elsewhere. Although not expressed, it must be inferred that this is an indirect acknowledgment of the lack of capacity of the Police, indeed, a notorious fact. A proper exercise of the Minister's discretion must have involved assessing the capacity of the Police. The minister chose the minimum period by law that he could choose.

[95] In my view, once it is to be accepted that storage for some prescribed period is not inappropriate, then the choice of an appropriate period is difficult to second guess. The authorisation to prescribe up to five years may seem excessive, if emphasis is given to comparative jurisdictions, but is not, in my view, inconsistent with the prescripts of section 36 of the Constitution.

[96] The revelation by Minster of Justice that, as a rule, requests for archived material are not in practice (up until now) made later than 19 months after the time that the communication occurred was argued to mean that a concession was implied that three years is too long. I disagree. Not enough factual matter is before this court to draw that conclusion. There was a hint of an argument that different types of investigations for different sorts of crimes or threats to the country could warrant different periods of archiving. This seems eminently correct. But, obviously, one cannot know in advance. The choice of duration has to be a "one size fits all" selection for all anticipated possibilities.

[97] I am unpersuaded that the statute is inconsistent with Constitutional imperatives in this regard.

***Management, usage and accessibility controls and integrity-oversight model***

[98] The specific respects of alleged inadequacy in regulation are listed thus :

(1) where intercepted information is stored; (S 37(1); S 26; S 10(4) act 65 of 2002)

(2) who may have access to it and under what conditions;

(3) whether any access has to be recorded/registered;

(4) whether copies may be made;

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

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

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

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

[99] Particular emphasis was placed on the methodology of examination, the possible uses to which the information could be put, the methodology of storage, the protocols about dissemination and the protocols for erasure of data irrelevant to the enquiry. Apart from the criticism of the UNHRC, cited already, it is common cause that the SA Inspector General of Intelligence, as long ago as 2011 expressed an adverse opinion about the efficacy of RICA's provisions in regard to the handling of data collected.

[100] The criticisms rely heavily on comparative jurisdictions' approaches to the issue.

[101] The decisions of the ECHR were alluded to. These cases are cited in support for the view that *RICA itself, not mere directives*, must set out the procedures. In my view, that is a sound policy choice; if privacy rights are to be compromised then the extent of the limitation to those rights ought not be dealt with in regulations or directives but rather broadcast to the world in the provisions of the statute. It was submitted that SAPS have internal guidelines that meet the case. That cannot be good enough. The Statute that subtracts from privacy rights is the appropriate location to effect that subtraction, including the safeguards to limit the extent of the subtraction.

[102] In *Weber and Saravia v Germany at [95]* and *[106]* the ECHR held:

> 95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offenses which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limited on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia, Huvig,* cited above, [34]; *Amann*, cited above, [76]; *Valenzuela Contreras,* cited above, [46]; and *Prado Bugallo v Spain,* no. 58469/00, [30], 18 February 2003).
>
> 106. The Court reiterates that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security (see, *inter alia, Klass and Others,* cited above [49]; *Leander*, cited above, [59]; and *Malone,* cited above, [81]). Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see *Klass and Others,* cited above, [49-50]; *Leander,* cited above, [60]; *Camenzind v Switzerland,* 16 December 1997, [45], *Reports* 1997 – VIII; and *Lambert,* cited above, [31]). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to organise, carry out and supervise them, and the kind of remedy provided by the national law (see *Klass and Others,* cited above, [50]).

[103] Moreover, in the United Kingdom, the QB in *Davis v The Secretary of State for the Home Department* [2015] EWHC 2092 ( 17/07/2005) at [114], condemned the Data Retention and Investigatory Powers Act 2014 for its inconsistency with the European Union Law because:

> " ...it does not lay down clear and precise rules providing for access to and use of communications data retained pursuant to a retention notice to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences..."

[104] It was posed in argument whether RICA could be held to be deficient simply because the statute does not address *all* of these issues. In my view the question is misdirected. If it is correct that RICA fails to address any aspect, the omission of which emasculates the safeguards model, the model is deficient. There can be no pass-mark approach.

[105] For example, erasure of surplus data and erasure of relevant data, once it has been legitimately used, in order to inhibit subsequent abuse, is not addressed at all in RICA. Hand in hand with that issue is the vexed issue of discreet copying and the protocols for not abusing copying and showing data to persons who have no necessary reason to learn of its existence, also not addressed in RICA.

[106] The oversight regime is extremely light. Section 37, as cited above, deals with reports by the director to Joint Standing Committee on Intelligence (JSCI) (A creature of the Intelligence Services Control Act 40 of 1994), an annual event, and heads of Interception Centres must keep records and report to the director. The section is notable for its generality. There is no judicial oversight role over this component of the model. Moreover, in as much as a 'specialist' designated judge authorises interceptions in real time as a front-end safeguard,

the resort to any judicial officer anywhere in the country, however inexperienced and unfamiliar with the legislation and the constitutional norms at stake to effect access to stored communications, is not only not an ineffective safeguard, it is no safeguard at all.

[107] The counter arguments are premised on deference to the authority of the Executive to address the details of a management regime. It is plain that the regulation through subordinate legislation and departmental guidelines is out of kilter with the norms espoused by other democratic jurisdictions.

***The remedy sought***

[108] A simple declaration is sought. In my view, a declaration as follows is appropriate:

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

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

**CHALLENGE NO 4:**

**PROTECTION OF LEGAL PRIVILEGE AND JOURNALISTS' CONFIDENTIAL SOURCES**

[109] The relief sought is formulated thus:

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

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

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

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

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

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

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

[110] The foundational proposition is that both lawyers and journalists have obligations to preserve the confidential communications from, respectively, clients or from secret sources. The contentions advanced in the debate in no way contradict this notion.

[111] The prickly point, however, is whether they should be protected from legal means to access those exchanges at all. In short, ought access to their confidential exchanges, in either absolute or in relative terms, be *prevented*?

[112] This analysis is past the point where it is accepted, if only grudgingly, that privacy can be punctured for a competing and supposedly greater good. The nub is the effect of interceptions on their professional roles and the efficacy with which those roles can be

performed if their confidential exchanges are accessed. Both lawyers and journalists perform not merely professional roles, but social roles which are part and parcel of the fabric of a society ordered upon the premise that the Rule of Law must prevail.

[113] There is, in my view, a substantive distinction between the role of a lawyer and the role of a journalist and that distinction warrants discreet treatment of the claims made in respect of each.

***Lawyers***

[114] The duty in law upon lawyers not to reveal what passes between them and their clients is trite. This is a privilege belonging to the client, not the lawyer. The rationale for this privilege is primarily that confidentiality of exchanges is an instrument necessary to facilitate a fair trial. Axiomatically, the admissibility of evidence of privileged communications is a question to be decided by a trial court. How evidence was procured is an issue in that process. In this paradigm privacy is instrumental to a fair trial.

[115] It is uncontroversial that privilege cannot attach to exchanges that comprise criminal plotting.

[116] The locus of the present controversy is the ability of third parties to gain access to such communications and when they can do so, what are the consequences. Whether the argument of inadmissibility in a court is a sufficient protection of the privilege against disclosure by a third party who unlawfully got access to the exchanges is not the point.

Rather, the point is the harm that knowledge of such exchanges can have for the client or the lawyer even if no court proceedings follow.

[117] The practical dynamics of eavesdropping on lawyers falls into two categories. On one hand intercepting the client's communications and on the other hand, intercepting the lawyer's communications. The former, in which the client is the target, creates a narrower intrusion than when the lawyer is targeted because the wholesale revelation of all of a lawyer's dealings are not at risk of being accessed. True enough, a lawyer might be targeted merely to get information about a certain client; if so the risk indeed does exist.

[118] When a lawyer may be the suspect in criminal conduct, the lawyer stands in the same relation to the risk of access to private dealings as any other person. Therefore the justifiability thereof is not assessed differently from ordinary persons. A wit has quipped that it is impossible in the modern world to commit large scale crime without the aid of accountants and lawyers and the existence of a rational premise to intercept a lawyer's communications must be acknowledged.

[119] Moreover, if the lawyer is personally suspected of defrauding his clients, a not unknown phenomenon, the wholesale interception of his communications with all clients would be thought to be necessary, even if some communications with non-victims were caught in the net. Alternatively, the lawyer may be involved in criminal activity that is independent of the clients he otherwise serves, in which example the status of lawyer would be an irrelevance.

[120] However, in any of the examples mentioned, if a lawyer is targeted for surveillance, there may be privileged communications with persons in whom the state has no interest but whose confidential exchanges would nevertheless be revealed. These inadvertent revelations are the locus of the mischief even if it is assumed the authorisation to subject the lawyer to surveillance was appropriate. A recognition of this class of inadvertent disclosures when appropriately targeting a lawyer is appropriate and warrants specific attention. The applicant's case is that the statute should recognise this issue. Plainly, RICA does not do so.

[121] The argument advanced on behalf of the applicants is that the satisfactory approach to inhibit these undesirable consequences is that an intermediary is needed whenever a lawyer is under surveillance so that the intermediary can filter out these inadvertent disclosures. A comparison is drawn with the practice of the Competition Commission which utilises independent persons to sift large volumes of data to yield only the relevant information for use before the tribunal. A comparison is also made with the practice in Anton Pillar applications where the order is executed in similar fashion.

[122] These observations give rise to the question whether, in the statute itself, the micro-management of the interception process is feasible. The applicants' case is that RICA requires more; ie the statute, per se, should make it compulsory for an applicant to disclose the status of the intended subject and the designated judge must be obliged to be responsive to such status by further enquiry as to the appropriate reach of an interception order and how the fruits of surveillance are to managed by, among other considerations, ad hoc conditions including the appointment of an intermediary to sift the data.

[123] Prima facie, section 16(2)(c) of RICA, might serve to address this sort of issue. It requires the applicant for an interception order to supply " ....full particulars of all the facts and circumstances". The relevance of the status of the subject ought, upon a proper interpretation of that subsection to be included. In similar vein, Section 16(6)(c) empowers the designated judge to " ....specify conditions or restrictions..."

[124] It is argued by the applicant that because RICA itself does not expressly provide for a disclosure of the subject's status, it is deficient in providing proper safeguards in such examples. Whereas spelling that requirement out in the statute would be useful, perhaps a simple interpretation of section 16(2)(c) that such facts about status must be disclosed to qualify the application as having supplied "full particulars and circumstances" is enough to meet the case.

[125] If that were done, the problem of how to deal with the communications intercepted would still remain. Must the appointment of an intermediary be compulsory or, at least, a default position to impose in terms of section 16(6)(c) ?

[126] There is, apparently, no support to found in the systems of other jurisdictions for an intermediary role as envisaged here. Yet is seems plain that in some circumstances the employment of an intermediary would be not only useful, but the only practical way to avoid undesirable disclosures. The absence of details in RICA itself about how to manage collated information has already been criticised in the previous part of this judgment and needs no repetition here, save to point out that the risk of impropriety in this context is greater.

[127] In my view, despite the present provisions in section 16 seeming to be adequate to cater for the respect for privilege through the imposition of conditions, a stronger injunction located in the statute is more appropriate, given the delicacy of the implications of an interception order. A statutory obligation should exist to make a positive disclosure as to the status of the subject to the designated judge who may impose such conditions as meet the needs evidenced by the particular facts, including an intermediary if in a given case that is appropriate.

[128] It can be assumed that the status of a subject will always be a topic to be interrogated by the designated judge. The manifest relevance of that fact in relation to honouring the norm of minimal intrusion to meet the *ad hoc* need makes it axiomatic. The contention is advanced that a higher threshold should apply to the granting of such interception orders. I am not convinced that meddling with the formulation of the threshold is the correct locus to address the problem. Rather, the conditions and restrictions imposed are the appropriate mechanisms to manage intrusions on lawyers.

***Journalists***

[129] The dynamic of investigative journalism is the ferreting out of facts by enquiry, largely, from whistle-blowers and others who rat on their fellows and their bosses.[14] The need to keep secret these sources is axiomatic to the exercise. [15]

[130] Despite much lauding of the role of the media and the express guarantee of freedom of expression and of the media, in particular, in section 16(1)(a) of the Constitution, there has

[14] See; seg, Nova Property Group Holdings Ltd 7 Others v Cobbett & another 2016 (4) SA 317 (SCA) at [38]
[15] See, eg: Government, RSA v The Sunday Times 1995 (2) BCLR 182 (T)

been a reluctance to take the next step needed to recognise journalists as a special class of persons whose intrinsic working methods warrant especial protection, such as lawyers enjoy.[16] There is an ambivalent general, but not universal, acceptance that journalists are not themselves to be compelled to disclose their sources, but what is at stake here is a preventive measures to inhibit third parties from finding out who the rats are by intercepting a journalist's communications.

[131] Section 16(1)(a) and (b) of the Constitution[17] do not, true enough, expressly address the confidentiality of sources. The burden of the section is the uninhibited right to broadcast information. Yet, if the output is so highly valued, why ought we to be precious about recognising the critical instrumentality of confidential sources in producing that valuable output? It is somewhat mealy-mouthed to proclaim the press as a bastion of democracy and then choose to ignore the realities of how information is gathered to enable the press to fulfil that role. Why allude to the media expressly in section 16(1)(a) of the Constitution, thereby recognising a constitutional value in its existence and role, and then white-ant the very function that is so recognised by a reluctance to privilege its methodology? In a country that is as wracked by corruption in both our public institutions and in our private institutions as ours is, and where the unearthing of wrongdoing is significantly the work of investigative journalists, in an otherwise, seemingly, empty field, it is hypocritical to both laud the press and ignore their special needs to be an effective prop of the democratic process.

---

[16] The Minster of Justice cites *Holomisa v Argus newspapers 1996 (2) SA 588 (W)* per Cameron J, for the proposition that our law recognises no blanket privilege. That norm is not implicated in this controversy and is beside the point.

[17] The Constitution, Section 16 (1): everyone has the right to freedom of expression, which includes –
(a) Freedom of the press and other media
(b) Freedom to receive or impart information and ideas

[132] Several ECHR decisions explicate the societal role of the press. These were considered by Tsoka J in *Bossasa Operations (Pty) Ltd v Basson & Another* 2013 (2) SA 570 (GSJ). At [38] it was held that:

> "Having regard to the authorities cited above, it is apparent that journalists, subject to certain limitations, are not expected to reveal the identity of their sources. If indeed the freedom of the press is fundamental and a sine qua non for democracy, it is essential that in carrying out this public duty for the public good, the identity of sources should not be revealed, particularly when the information so revealed would not have been publicly known. The essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded." [18]

[133] Can it be argued that it is a necessary dimension of section 16(1) rights that journalistic sources are protected from prying? If a purposive interpretation is applied to the section, ought not this dimension be recognised? In my view, the answer is yes; and, by because of such a perspective, the role of the media would be "fostered not denuded", as Tsoka J rightly observed. The right to withhold the identity of a source must extend to protection from being spied on too, subject only to the sort of extreme circumstances that warrant a breach of that norm. Such circumstances must be rare indeed; perhaps related only to clearly shown cases of espionage with the intent to cause serious human rights injuries. The journalists' need to secure confidentiality requires statutory protection and regulation of the exceptional circumstances where an intrusion is truly warranted.

---

[18] See too: *Government of RSA v The Sunday Times* 1995 (2) BCLR 182 (T) at [188]; *Goodwin v United Kingdom* [1996] 22 ECHR 123.

[134] The *Declaration on principles of Freedom of Expression in Africa of 2002*[19], contains pertinent injunctions about securing press freedom. It recognises that freedom of expression is a human right and a "cornerstone of Democracy". The media is said to play a "key role" in securing respect for the freedom of expression. In Article XV the "protection of sources and other journalistic material" is addressed thus:

> "Media practitioners shall not be required to reveal confidential sources of information or to disclose other material held for journalistic purposes except in accordance with the following principles:
>
> - the identity of the source is necessary for the investigation or prosecution of a serious crime, or the defence of a person accused of a criminal offence;
> - the information or similar information leading to the same result cannot be obtained elsewhere;
> - the public interest in disclosure outweighs the harm to freedom of expression; and
> - disclosure has been ordered by a court, after a full hearing."

[135] These provisions, like those in section 16(1) of the Constitution make no express reference to a protection against involuntary acquisition of the confidential information through interceptions. However, if protections of this nature are appropriate to inhibit revealing a source or the information disclosed, then RICA must, for similar policy reasons, give appropriate recognition to the threshold that would justify spying on a journalist *per se*, as distinct from other persons.

[136] Accordingly, the notion that there is a deficiency in Section 16 of RICA because the peculiar position of journalists is not expressly catered for is sound. As with lawyers, except

---

[19] Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session, 17 - 23 October, 2002: Banjul, The Gambia.

for the rare occasion when the journalist *per se* is the suspect in criminal activity, on good grounds alleged, spying on a journalist would be to investigate the people with whom that journalist is in contact. That conduct cannot be appropriate.

[137] The counter argument is built on several unconvincing premises.

137.1 It is argued that there is no Constitutional right that a journalist can claim for special status. In my view, this contention is untenable given the reference to the "media" in section 16(1)(a) of the Constitution.

137.2 It is argued that there is no obligation on journalists to use telecommunications; this is an anti-modern notion and is on a par with saying that people who live in towns are not compelled to use electricity to run their lives.

137.3 The notion is posited that the designated judge must make a judgment call and no more is required to be said because section 16(6)(c) of RICA empowers the designated judge to impose conditions. This proposition has already been refuted in respect of lawyers.

137.4 Lastly, it is argued that the sources may reveal themselves; this is true but is besides the point. The point is the journalist's right to have the fact of a communication kept secret on the premise that the valuable social role played by a journalist is compromised if that secrecy cannot be preserved.

[138] The unhappy fact that it is journalists, investigating organs of state and officialdom and the political class and their involvement in corrupt practices to loot the State's resources, who, by so doing, attract the attention of powerful and influential persons who are capable of

suborning the apparatus of the State to smell out their adversaries, cannot be ignored. The examples of abuse of the system have been addressed elsewhere in this judgment.

[139] Moreover, the respondents' perspectives assume that the designated judge is not lied to and is diligent. How these assumptions fare, for example, in respect Sole and Downer, where the State was spying on a journalist and one of its own prosecutors is not evident on these papers. In my view, in the absence of a rebuttal, this example illustrates a grave vulnerability in RICA that such an apparent abuse could occur. The common cause examples of blatant lies being told to the designated judge further exacerbates the vulnerability of the system.

[140] In my view the absence of express provisions enjoining the designated judge to examine the justification of spying on a journalist is evidence of a failure to align RICA with section 16(1) rights. The absence renders RICA in that respect, unconstitutional.

[141] The suggestion is made by the applicant that the threshold be formulated not as "reasonable grounds to believe" but rather as "a high degree of probability". I am not persuaded that tinkering with the semantics achieves anything of substance. Several formulations abound, some more strident than others.[20] The true issue is that all relevant facts need to be disclosed to the designated judge and in respect of which that judge is expressly directed to have especial regard as to propriety of the interception *per se,* and if truly justified how to deal with the information collated.

---

[20] See *Goodwin v United Kingdom* ECHR 16/1994/463/544 at[39] which states the threshold for compelling disclosure by a journalist of a source as being: " ....justified by an overriding requirement in the public interest."

[142] In my view, the relief sought by the applicant is appropriate.

**CHALLENGE NO 5: BULK INTERCEPTIONS**

[143] The phrase " Bulk Interceptions' is a commonly used shorthand for what is described by the respondents as follows:

> "Bulk surveillance is an internationally accepted method of strategically monitoring transnational signals, in order to screen them for certain cue words or key phrases. The national security objective is to ensure that the State is secured against transnational threats.
> It is basically done through the tapping and recording of transnational signals, including, in some cases, undersea fibre optic cables."
>
> "intelligence obtained from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals. It also includes any communication that emanates from outside the borders of [South Africa] and passes through or ends in [South Africa]"

[144] Another useful description is that to be found in the ECHR judgment in *Centrum For Rattvisa v Sweden* [2019] 68 EHRR *2* at paragraph 7:

> "Signals intelligence can be defined as intercepting, processing, analysing and reporting intelligence from electronic signals. These signals may be processed to text, images and sound. The intelligence collected through these procedures may concern both the content of a communication and its associated communications data (the data describing, eg, how, when and between which addresses the electronic communication is conducted). The intelligence may be intercepted over the airways – usually from radio links and satellites – and from cables. Whether a signal is transmitted over the airways or through cable is controlled by the communications service providers. ..."

[145] It is common cause that this form of monitoring would also capture communications between two South Africans, both of whom are in South Africa, if the signal passes through a server located outside South Africa.

[146] Two questions arise in this controversy: first is there a law that authorises public power to be used to conduct this conduct in mining of metadata or bulk interceptions, and second, if so, is such a law constitutionally compliant. Whether such conduct is lawful must first be examined.

[147] It is undisputed that bulk surveillance cannot take place by officials of the state in the absence of a law authorising it.[21] It is argued that the National Strategic Intelligence act 39 of 1994. (NSIA) authorises such conduct. This contention is challenged by the applicant. It is common cause that RICA does not authorise such conduct by the State.

[148] The NSIA was enacted, so its preamble states, to define the functions of members of the national intelligence structures, and provides for related enabling measures 'relating to the security of the Republic'. The structures contemplated in the preamble are defined to include the National Intelligence Coordinating Committee, the State Security Agency (SSA), and the intelligence units within the Defence Force and the Police.

[149] Section 2, a pivotal provision in NSIA, addresses "Functions relating to Intelligence". It is extensive. It deals in turn with the functions of the SSA, the Defence Force and the Police. The section reads;

"(1) The functions of the Agency shall, subject to section 3, be-

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

(i) identify any threat or potential threat to national security;

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

---

[21] See: *Pharmaceutical Manufacturers Association of South Africa & Others* In *Re Ex Parte President of RSA & Others* 2000(2) SA 674 (CC) at [20].

*(b)* to fulfil the national counter-intelligence responsibilities and for this purpose to conduct and co-ordinate counter-intelligence and to gather, correlate, evaluate, analyse and interpret information regarding counter-intelligence in order to-

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

(ii) inform the President of any such threat;

the purposes of investigating any offence or alleged offence; and

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

(iv) 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;

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

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

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

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

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

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

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

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

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

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

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

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

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

(2A) ....

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

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

*(b)* to institute counter-intelligence measures within the South African Police Service; and

*(c)* to supply crime intelligence relating to national strategic intelligence to Nicoc.

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

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

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

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

(Underlining supplied)

[150] The emphasized passages in the text of section 2 seem to be the operative provisions; ie instructing the relevant entity, in broad terms, what to do. What is evident is that nowhere in this text is there any instruction to mine internet communications covertly.

[151] Indeed, the NSIA does not expressly authorise interceptions of any kind except in section 2A(5). This section deals with the role of the SSA to vet people for security clearances. Self-evidently the vetting exercise is wholly distinct from bulk surveillance. Section 2A(5) reads thus:

"The relevant members of the National Intelligence Structures may, in the prescribed manner, gather information relating to-

*(a)* criminal records;

*b)* financial records;

*(c)* personal information; or

*(d)* any other information which is relevant to determine the security clearance of a person:

> Provided that where the gathering of information contemplated in paragraphs *(c)* and *(d)* requires the interception and monitoring of the communication of such a person, the relevant members shall perform this function in accordance with [RICA]"

[152] It is plain that (a) and (b) do not lend themselves to interceptions at all. Subsection (c) relates to personal information (which is not defined) and subsection (d), the catch-all, are relevant to targeted interceptions, not to bulk interceptions. Importantly, if such interceptions do take place, RICA applies.

[153] The implication is plain that vetting is the only rationale mentioned in NSIA to intercept an individual's communications. The only sensible explanation why the section alludes to RICA is that RICA *per se* is not available for vetting. Thus, individual interceptions by the SSA must always be done by justifying the need in terms of RICA, which section thereby extends the scope of RICA for this limited purpose.

[154] Nowhere else in the NSIA is there reference to using interception as a tool of information gathering, still less any reference to bulk surveillance as a tool of information gathering.

[155] In the absence of any express authorisation to use bulk interception as a tool of information gathering on what basis can the NSIA be understood to sanction the conduct? The sole contention advanced to support that idea is that section 2 authorises the conduct because it is awash with the refrain: "Gather, correlate, evaluate and analyse". However, this phrase does not *per se* prescribe methodology nor do its semantic variants in that section do so. Moreover, on ordinary interpretative approaches, it is not evident why such a

methodology could be implied.[22] Further explorations into the NSIA yield no comfort for this contention.

[156] "Intelligence", itself, is defined thus:

> "**intelligence**' means any information obtained and processed by a National Intelligence Structure for the purposes of informing any government decision or policy-making process carried out in order to protect or advance the national security, and includes-
>
> *(a)* counter-intelligence;
> *(b)* crime intelligence;
> *c)* departmental intelligence;
> *(d)* domestic intelligence;
> *(e)* domestic military intelligence;
> *f)* foreign intelligence; and
> *(g)* foreign military intelligence;
> (Underlining supplied)

[157] In section 2(2)(b)(i), (ii), and (iii) there are allusions to protecting critical "electronic communications" against unauthorised access. This must be read as keeping hackers out, not as mining other data.

[158] Section 2(1)(b) deals with counter intelligence and again repeats the mantra of "gather correlate evaluate and analyse". Counter intelligence is defined as:

> ".... measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct vetting investigations and to counter any threat or potential threat to national security;

[159] The phrase: " ...measures and means..." read with the rest of that text is deliberately wide. What is its scope?

---

[22] *Natal Joint Municipal Pension Fund v Endumeni Municipality* 2012 (4) SA 593 (SCA) at [18]

[160] "covert collection" is defined as:

> "…. the acquisition of information which cannot be obtained by overt means and for which complete and continuous secrecy is a requirement;

Curiously, this term appears nowhere again in the statute.

[161] Could these provisions be the fount of an authorisation to use "measures and means' in covert circumstances, which, if read with Section 2(1)(b) or 2(2) (b), include, by implication, bulk interceptions?

[162] In my view, to read all of that into the text would mean placing a gloss on these provisions to embrace conduct wholly unhinted at. That extravagance is impermissible in terms of conventional techniques of statutory interpretation.

[163] The Answering Affidavit of Fraser, then the Director – General of Intelligence, says that bulk interceptions is common practice in many countries. This is, indeed, a notorious fact. However, even were it be to assumed, for the purpose of this analysis, that bulk interceptions *per se,* or subject to certain conditions, is a good idea, or even a practice that any sovereign State cannot do without, despite its distaste for the practice, the least that can be required is a law that says intelligibly that the State can do so. The NSIA does not do so. Our Law demands such clarity, especially when the claimed power is so demonstrably at odds with the Constitutional norm that guarantees privacy. If there was a law it could be tested in terms of section 36 and 39 of the Constitution.

[164] The requirement of a clear law to authorise the State to undertake bulk interceptions has been the subject of judicial attention. For example, in *Centrum For Rattvisa v Sweden*

*(Supra)* the ECHR addressed the issue of the extent to which Swedish domestic law, the Foreign Intelligence Act, measure up to European Covenant on Human Rights. The point of departure was the express authorisation of such monitoring in that statute. Upon that foundation a normative assessment of the law could take place.

[165] Accordingly, in my view, no lawful authority has been demonstrated to trespass onto the privacy rights or the freedom of expression rights of anyone, including South Africans, whose communications criss-cross the world by means of bulk interception. A declaratory order to that effect is appropriate. The applicant seeks an order in these terms, which I endorse:

> "The bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid."

[166] Whether or not bulk interception *per se* could be constitutionally compliant in our law, were there to be a law that allows it, it is unnecessary to decide.

**SUMMARY OF CONCLUSIONS**

[167] From the analysis set out above, the conclusion that in several respects RICA is deficient in meeting the threshold required by section 36 of the Constitution to justify the subtraction of the rights in section 14, 16(1) and 34 and 35(5) of the Constitution. Less restrictive means than those in force are feasible and ought to be enacted. The practice of bulk interception of international communications is unlawful for want of a law authorising it to take place.

**THE COSTS**

[168] In keeping with the character of the controversy and the conventions in this genre of litigation, there shall be no order as to costs.

**THE ORDER**

I make orders as follows:

**Order No 1:**

It is declared that:

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

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

   (c) Pending the enactment of legislation to cure the defect, RICA shall be deemed to read to include the following additional sections 16(11), (12) and (13):

   '(11) The applicant that obtained the interception direction shall, within 90 days of its expiry, notify in writing the person who was

the subject of the interception and shall certify to the designated judge that the person has been so notified.

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

(13) In the event that orders of deferral of notification, in total, amount to three years after surveillance has ended, the application for any further deferral shall be placed before a panel of three designated judges for consideration henceforth, and such panel, as constituted from time to time, by a majority if necessary, shall decide on whether annual deferrals from that moment forward should be ordered."

**Order No 2:**

It is declared that:

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

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

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

> "any judge of a High Court discharged from active service under section 3 (2) of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act 47 of 2001), or any retired judge, who is nominated by the Chief Justice, and upon which nomination is appointed by the minister of Justice, for a non-renewable term of two years to perform the functions of a designated judge for purposes of this Act'."

**Order no 3:**

It is declared that:

(a) RICA, including sections 16(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to adequately provide for a system with appropriate safeguards to deal with the fact that the orders in question are granted *ex parte*; and

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

**Order No 4:**

It is declared that:

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

sharing, sorting through, using, destroying and/or storing the data obtained from interceptions;

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

**Order no 5:**

It is declared that:

(1) Sections 16(5), 17(4), 19(4), 21 (4) (a), and 22(4) (b) of RICA are inconsistent with the Constitution and accordingly invalid to the extent that they fail to address expressly the circumstances where a subject of surveillance is either a practising lawyer or a journalist.

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

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

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

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

b) The designated judge shall only grant the order sought if satisfied that the order is necessary and

appropriate, notwithstanding the fact that the subject is a journalist or practising legal practitioner; and

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

**Order no 6:**

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

Roland Sutherland

**ROLAND SUTHERLAND**
**Judge of the High Court**
**Gauteng Division, Pretoria**

Date of hearing: 4 – 5 June 2019

Date of judgment: 16 September 2019

For the Applicants: Advs S Budlender SC, SJ Scott and I Phalane.

Instructed by: Webber Wentzel Attorneys

For the 1st, 4th and 5th Respondents: Advs SK Hassim SC and MPD Chabedi.

Instructed by: State Attorney Pretoria

For the 2nd, 7th, 8th and 10th Respondents: Advs V Ngalwana SC, M Sikhakhane SC, F Karachi and Z Ngwenya.

Instructed by: Kgoroeadira Mudau Inc

For the *Amici Curiae*: Adv M Bishop and P Wainwright (pupil)

Instructed by: The Legal Resources Centre.