IN THE HIGH COURT OF SOUTH AFRICA

(GAUTENG DIVISION, PRETORIA)

The matter between:	**Case no: 25978/17**
AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC	1st Applicant
SOLE STEPHEN PATRIC	2nd Applicant
And	
MINISTER OF JUSTICE AND CORRECTIONAL SERVICES	1st Respondent
MINISTER OF STATE SECURITY	2nd Respondent
MINISTER OF COMMUNICATIONS	3rd Respondent
MINISTER OF DEFENCE AND MILITARY VETERANS	4th Respondent
MINISTER OF POLICE	5th Respondent
THE OFFICE OF INSPECTOR-GENERAL OF INTELLIGENCE	6th Respondent
THE OFFICE FOR INTERCEPTION CENTRES	7th Respondent
THE NATIONAL COMMUNICATIONS CENTRE	8th Respondent
THE JOINT STANDING COMMITTEE ON INTELLIGENCE	9th Respondent
THE STATE SECURITY AGENCY	10th Respondent

AMICI CURIAE'S HEADS OF ARGUMENT

TABLE OF CONTENTS

I INTRODUCTION 3
II INTERNATIONAL AND COMPARATIVE LAW 7
III NOTIFICATION OF INTERCEPTION 8
SECTION 38 VIOLATION 10
INTERNATIONAL LAW 12
COMPARATIVE LAW 16
Comparative Legislation 16
European Courts 19
CONCLUSION 20
III THE DESIGNATED JUDGE 22
COMPARATIVE PRACTICE 23
RIGHT TO PRIVACY 26
THE DANGER OF A RETIRED JUDGE 28
SECRECY 30
III MANDATORY BLANKET RETENTION OF METADATA 35
MANDATORY BLANKET RETENTION OF METADATA UNDER RICA 36
Retention 37
Access 39
Conclusion 43
LIMITATION OF PRIVACY AND EXPRESSION 45
International Law 46
European 48
The United States 54
South Africa 58
JUSTIFICATION 59
CONCLUSION 62
V BULK SURVEILLANCE 63
OPERATION OF BULK SURVEILLANCE 64
LIMITATION OF THE RIGHT 66
COMPARATIVE AND INTERNATIONAL PRACTICE 70
International Law 70
European Law 72
DECIDING THE CASE 75

I INTRODUCTION

1. "*Everyone has the right to privacy, which includes the right not to have … the privacy of their communications infringed*".[1] The right to privacy – and particularly to the privacy of our communications – is central to the constitutional order founded on human dignity. As O'Regan J has held, we protect privacy because of "*our constitutional understanding of what it means to be a human being*":

> "*We value privacy for this reason at least – that the constitutional conception of being a human being asserts and seeks to foster the possibility of human beings choosing how to live their lives within the overall framework of a broader community. The protection of this autonomy, which flows from our recognition of individual human worth, presupposes personal space within which to live this life.*"[2]

2. While that personal space includes deep and intimate relations, it is also the way we "l*ive our daily lives. This sphere in which to pursue our own ends and interests in our own ways, although often mundane, is intensely important to what makes human life meaningful.*"[3]

3. This personal privacy extends to where we go, and what we do with our mobile phones. As Langa DCJ (as he then was) explained in *Hyundai*:

> "*when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such*

---

[1] Constitution s 14(d).

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

[3] Ibid at 130.

a decision will be respected is reasonable, the right to privacy will come into play."[4]

4. This application concerns serious threats to the privacy of our constitutionally protected personal space.

5. It is a challenge to the constitutionality of the Regulation of Interception of Communications and Provisions of Communication – Related Information Act 70 of 2002 (**RICA**) and the National Security Intelligence Act 39 of 1994 (**NSIA**).

6. RICA and the NSIA, combined with the development of modern technology and the way we use that technology allow intense and unjustifiable intrusions by the South African state authorities into our personal daily lives.

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

8. RICA also compels cell phone and internet companies to store extremely intrusive data about all users' movements and communications for up to five years just in case it may one day be relevant to an investigation. This metadata – even absent the content of the communications – can reveal a deep and intimate portrait of our personal lives. It records who we communicate with, where we are at almost every minute of the day, and what websites we visit.

9. The Respondents assert that the NSIA allows them to engage in bulk surveillance of foreign internet signals. In simple terms, that means that the

---

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

government believes it is entitled to intercept, copy, analyse and disseminate virtually all internet traffic of all people in South Africa. This is an astounding violation of the right to privacy. It is without doubt unconstitutional and unlawful.

10. R2K and PI therefore support the application on the four issues identified above. With regard to notification and the independence of the designated judge, they merely provide additional arguments to support the relief sought by the Applicants.

11. On the mandatory blanket retention of metadata and foreign bulk surveillance, R2K and PI take a stronger position, based on existing analysis of international human rights mechanisms and on jurisprudence of European courts. The Applicant contends that the primary flaws are the absence of appropriate safeguards to regulate the exercise of those powers. R2K and PI contend that

    11.1. The mandatory blanket retention of metadata will always be unconstitutional, even with safeguards and for a shorter period. Only targeted retention of metadata could be justifiable.

    11.2. Foreign bulk surveillance will always be unconstitutional, even if it was authorised by law and regulated. It is never possible to regulate bulk surveillance of all internet traffic constitutionally. Only targeted surveillance of internet traffic could be justifiable.

12. However, this Court is not called to determine ultimately the constitutionality of mandatory blanket retention of metadata, or of bulk surveillance of foreign signals. It is only required to determine the Applicants' narrower challenges. R2K and PI ask this Court to: (a) recognise the fundamental constitutional problem with these types of surveillance, even with safeguards; and (b) leave the door open for a direct constitutional challenge in the future.

13. These heads of argument are structured as follows:

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

13.2. **Part III** address **post-interception notification**;

13.3. **Part IV** concerns the independence of the **designated judge**;

13.4. **Part V** examines **mandatory blanket retention of metadata**.

13.5. **Part VI** deals with **mass surveillance** of “foreign” signals.

II INTERNATIONAL AND COMPARATIVE LAW

14. As the *Amici* rely in detail on international and comparative law, this Part briefly sets out why it is relevant to this Court's determination of the issues.

15. International law is relevant for four reasons:

15.1. When interpreting the Bill of Rights, s 39(1)(b) of the Constitution mandates courts to consider international law. In *Glenister II*,[5] the Constitutional Court stressed the importance of international law in determining the content of the Bill of Rights, and particularly s 7(2). It held that an international obligation does not only exist on the international plane: "*Our Constitution appropriates the obligation for itself, and draws it deeply into its heart, by requiring the state to fulfil it in the domestic sphere.*"[6]

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

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

---

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

[6] Ibid at para 189.

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

15.4. In terms of s 233 of the Constitution: "*When interpreting any legislation, every court must prefer any reasonable interpretation of the legislation that is consistent with international law over any alternative interpretation that is inconsistent with international law.*" This is particularly relevant for the challenge to bulk surveillance where the Respondents contend their conduct is authorised by legislation.

16. While the courts are not compelled to consider comparative law, they are permitted to do so when interpreting the Bill of Rights.[8] Naturally, courts must be cautious when relying on foreign law, and should not simply import foreign doctrines to South Africa uncritically.[9] Nonetheless, comparative practice – in the form of both legislation and judicial decisions – can be extremely helpful in illuminating how to interpret our own Constitution. It too is particularly relevant in the s 36(1) analysis. If there is a clear trend in comparative practice, it may suggest that a law is or is not justifiable in an "*open and democratic society*".

III NOTIFICATION OF INTERCEPTION

17. The first problem with RICA is that it allows people to be placed under surveillance, and never to be notified that this occurred, even after the surveillance is complete, and when secrecy is no longer necessary to protect the investigation.

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

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

18. As the Applicants rightly contend, this is an unjustifiable limitation of the rights to privacy and access to court. The subjects of surveillance will never know their privacy was violated, and will never have an opportunity to argue that the surveillance was unlawful.

19. R2K supports the Applicants' arguments, and advances three additional arguments:

    19.1. The absence of notification violates s 38 of the Constitution;

    19.2. International law supports the need for appropriate notification; and

    19.3. Comparative law and practice support the need for appropriate notification.

20. To be clear upfront, neither the Applicants nor the Amici contend that subjects of surveillance should be notified before the surveillance is complete. And they accept that there may be circumstances even after the surveillance is complete where notifying the subject would prejudice an ongoing investigation. What we contend is unconstitutional is the absolute prohibition on notification even when it serves no legitimate end. Parliament must craft a remedy that ensures notification is provided as soon as notification can be done without jeopardising the purpose of the surveillance. Precisely what mechanism achieves that end is a matter for Parliament.

SECTION 38 VIOLATION

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

22. Section 38 of the Constitution is often regarded as only dealing with standing. But it does more than that. It creates a right to approach a court when a constitutional right has been infringed or threatened, and it creates a right to "*appropriate relief*". It reads: "*Anyone listed in this section …the right to approach a competent court, alleging that a right in the Bill of Rights has been infringed or threatened, and the court may grant appropriate relief, including a declaration of rights*." It can fairly be described a "*right to a remedy*" where a constitutional right has been infringed.[11]

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

24. In *Fose v Minister of Safety and Security*, Ackermann J held:

> "*In our context an appropriate remedy must mean an effective remedy, for without effective remedies for breach, the values underlying and the*

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

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

> *rights entrenched in the Constitution cannot properly be upheld or enhanced. Particularly in a country where so few have the means to enforce their rights through the courts, it is essential that on those occasions when the legal process does establish that an infringement of an entrenched right has occurred, it be effectively vindicated.*"[12]

25. While s 34 protects the general right to approach a court to resolve any legal dispute, s 38 provides special protection to ensure that rights violations are adjudicated and remedied. As surveillance, even with an authorisation, will always limit the right to privacy, s 38 entitles the subject to test whether that limitation was lawful or not.

26. The point of notification is to determine the *existence* of an allegation that a right has been violated. It may be that the surveillance happened lawfully and that any limitation of the right to privacy was justified. Section 38 is about ensuring that those questions are determined by courts. That can only happen if there is notification. Without such notification, the party whose privacy has been limited will be unaware of such limitation and thus unable to bring a challenge as envisaged in s 38. This renders s 38 impotent for such parties.

27. Naturally, after the surveillance has been concluded, the remedies that can effectively vindicate the right are limited. Setting aside the surveillance is hollow as it has already occurred. But there are a number of potential remedies that remain available – a declaration of rights, constitutional damages, and an order that the surveillance material be destroyed or provided to the subject.

28. Section 38 expressly recognises a declaration of rights as an appropriate remedy. This is still a powerful remedy because it compels the State to justify

---

[12] 1997 (3) SA 786 (CC), 1997 (7) BCLR 851 (CC). The Court has since made it clear that this holding applies to s 38. See *National Coalition for Gay and Lesbian Equality v Minister of Home Affairs & Others* 2000 (2) SA 1 (CC), 2000 (1) BCLR 39 (CC) at para 65.

the limitation of the right to privacy, which is itself an appropriate check on this immense power, and will encourage the lawful use of the power in the future. In *Rail Commuters Action Group v Transnet Ltd t/a Metrorail* the Constitutional Court noted: "*A declaratory order is a flexible remedy which can assist in clarifying legal and constitutional obligations in a manner which promotes the protection and enforcement of our Constitution and its values.*"[13]

29. For these reasons, R2K and PI argue that RICA also violates s 38 of the Constitution. As we show below, in the context of surveillance, international and comparative law tightly ties the right to privacy to the international right to an effective remedy.

INTERNATIONAL LAW

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

31. The right to an effective remedy is also a strong part of international law:

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

    31.2. Article 2(3) of the International Covenant on Civil and Political Rights requires states to "*ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy,*

[13] [2004] ZACC 20; 2005 (2) SA 359 (CC); 2005 (4) BCLR 301 (CC) at para 107.

notwithstanding that the violation has been committed by persons acting in an official capacity".[14]

32. In its *General Comment 31* on the nature of State Parties' obligations, the Human Rights Committee considered the right to an effective remedy. It emphasised that "*[a]dministrative mechanisms are particularly required to give effect to the general obligation to investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies.*"[15] It also stressed that reparation, which could include "*public apologies, public memorials, guarantees of non-repetition and changes in relevant laws and practices*" are necessary to provide an effective remedy.[16]

33. Without reparation to individuals whose Covenant rights have been violated, the obligation to provide an effective remedy, which is central to the International law has increasingly recognised that notification is a fundamental safeguard to protect the right to privacy, the right to an effective remedy and the right to free expression. This position is evidenced by the findings of the UN Human Rights Committee, the UN High Commissioner for Human Rights,

---

[14] Art 2(3) reads in full:

3. Each State Party to the present Covenant undertakes:

(a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;

(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;

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

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

[16] Ibid at para 16.

and the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.

34. First, the UN High Commissioner for Human Rights notes that:

> "*Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy."*[17]

35. In his 2018 Report, the UN High Commissioner wrote: "*Recognizing that advance or concurrent notification might jeopardize the effectiveness of legitimate surveillance measures, individuals should nevertheless be notified once surveillance has been completed*".[18]

36. Second, in his 2013 Report the Special Rapporteur on the Promotion of the Right to Free Expression put the position in even stronger terms:

> *"Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek*

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

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

> *redress in respect of the use of communications surveillance measures in their aftermath."*[19]

37. Third, in its 2016 evaluation of Poland, the Human Rights Committee expressed a number of misgivings about Poland's surveillance system. As a number of them relate to this application, it is worth repeating in full:

> *The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities, as reflected in the law on counterterrorism of June 2016 and the act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: (a) the unlimited and indiscriminate surveillance of communications and collection of metadata; (b) the targeting of foreign nationals and application of different legal criteria to them; (c) the insufficient procedural safeguards; (d) the lack of adequate judicial oversight; (e) the possibility of banning or terminating assemblies and mass events; and (f) the lack of notification, complaints procedure or mechanism for remedies*"[20]

38. The various bodies tasked to enforce the ICCPR and the UDHR have all concluded that the failure to provide notification is problematic. The Special Rapporteur expressly states that it is required. International law considers notification to be a necessary element of an effective remedy, without which the affected person would be unable to approach a court to allege an infringement of their rights. That is a powerful factor in favour of a finding that the limitation is not justifiable.

---

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

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

COMPARATIVE LAW

39. R2K and PI have conducted an analysis of various countries' laws on subject notification. The analysis demonstrates that the majority of comparable countries require subject notification. The countries vary in terms of the details of when notification is required, the standard for notification, and how the decision is made. But they share the common themes identified by the Applicants: (a) the subject must be notified either before or after the surveillance unless it will threaten the purpose of interception; and (b) the decision whether to notify or not is overseen by an independent authority.

40. A broader survey of the legislative provisions of countries in Europe, South America and Asia evidence these themes. We first consider relevant legislation, and then jurisprudence of European supra-national courts.

Comparative Legislation

41. A consideration of other countries' legislation shows that notification is common and possible. The following countries all have some notification provision:

    41.1. The Netherlands;[21]

    41.2. Germany'[22]

    41.3. Belgium;[23]

    41.4. Austria;[24]

---

[21] Intelligence and Security Services Act 2002.

[22] German Code of Criminal Procedure 1987, Article 101.

[23] Belgium, Constitutional Court Case No. 145/2011 at paras 88 and 92.

[24] Code of Criminal Procedure of the Republic of Austria 1975, Annexe 2 (138).

41.5. Ireland;[25]

41.6. The Czech Republic;[26]

41.7. Switzerland;[27]

41.8. Slovenia;[28]

41.9. Montenegro;[29]

41.10. Hungary;[30]

41.11. the United States of America;[31]

41.12. Canada;[32]

41.13. Japan;[33]

41.14. South Korea;[34]

41.15. Taiwan;[35]

41.16. New Zealand;[36] and

41.17. Chile.[37]

42. These countries use a variety of methods to identify when a person must be notified. Many use language such as "*as soon as it is possible to do so without compromising intelligence work*" or without compromising the investigation, or

---

[25] Criminal Justice (Surveillance) Act 2009, s 10(3).

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

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

[28] Criminal Procedure Code, Article 154.

[29] Criminal Procedure Code 2009, Article 162.

[30] Act on Criminal Proceedings XIX 1998, Title V, s 205(5).

[31] 18 U.S. Code § 2518.

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

[33] Act on the Interception of Communications.

[34] Protection of Communications Secrets Act 2002, art 9-2 .

[35] Communications Protection and Surveillance Act 1999, art 15.

[36] Search and Surveillance Act 2012, Part 3.

[37] Code of Criminal Procedure.

"*unlikely to hinder the investigation in the future of such offences*". Others include a risk to life or physical integrity of a third party (such as Chile).

43. Some provide for a default duty to inform unless that condition is present (such as Austria). Others provide for a duty to inform unless some other condition is met – for example if the communications are not used in criminal proceedings. Hungary requires notification unless the material is used in criminal proceedings and notification would jeopardise those proceedings.

44. Some countries require the intervention of a court to justify not notifying the person (such as Switzerland, the United States, Taiwan and Montenegro). That can be at the judge's own instance, or on application by a prosecutor. Normally, the judge merely postpones notification until it will no longer pose a threat to the investigation.

45. Some include timeframes – the Netherlands, for example, requires the authorities to re-assess whether notification is possible after five years. Slovenia assumes notification should be done if the prosecutor does not act within two years. Japan and South Korea require notification within 30 days. Some, like Ireland, allow the Minister to enact regulations addressing the details.

46. What is clear is that it is <u>possible</u> to design a mechanism that appropriately balances the respective interests – protecting the investigation, and providing an effective remedy.

47. Of course, not all countries provide for notification.[38] But European courts that have considered the issue have – like the international bodies discussed above – held that notification is vital.

European Courts

48. The Court of Justice of the European Union (**CJEU**) and the European Court of Human Rights (**ECHR**) have both recognized that notification is a critical safeguard when governments conduct surveillance:

49. First, in *Szabó and Vissy v Hungary*,[39] the ECHR identified the requirement for "*subsequent notification of surveillance measures*" to the person affected as

> *"inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned*".[40]

50. Second, and most recently, in *Big Brother Watch & Others v United Kingdom*, the ECHR summarised its earlier jurisprudence as follows:

> "*the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and*

[38] See, for example, Croatia (Criminal Procedure Code 2009, art 335(5)); Bulgaria (Special Surveillance Means Act); Sweden (Act (2007: 980) on the Supervision of Certain Law Enforcement Activities); and Mexico (Ley Federal de Telecomunicaciones (2014) Arts. 189, 190, 191).

[39] [2016] ECHR 579, available at http://www.bailii.org/eu/cases/ECHR/2016/579.html.

[40] Ibid at at para 86 (emphasis added).

hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken."[41]

51. Third, in *Tele2 Sverige AB and C-698/15 Watson and Others*,[42] the CJEU held that:

> "*Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.*"[43]

CONCLUSION

52. Without notification, the possibility of a remedy for violations of rights is extremely low. A person illegally placed under surveillance will not be able to test whether the surveillance was lawful unless they know they have been under surveillance.[44] This not only leaves that individual without a remedy, it

[41] [2018] ECHR 722 at para 310 (citations omitted). The ECHR declined to extend the requirement of subsequent notification to bulk surveillance because it would not be possible to notify all the subjects of surveillance. Ibid at para 317.

[42] [2016] EUCJEU C-203/15, available at www.bailii.org/eu/cases/EUCJEU/2016/C20315.html.

[43] Ibid at para 121.

[44] The possibility of a hypothetical challenge to surveillance by somebody who might theoretically be under surveillance cannot provide an individual remedy to the person in fact under surveillance unless, at some point, there is notification.

creates impunity within the system because the risk of abuses being identified and punished are slim. It is only in the unusual case where a person who has not been notified (and who is not subsequently prosecuted) will learn that his communications were intercepted.

53. As the Applicants' explain, the Respondents' defences miss the point. The question is whether it is possible to develop a system that allows for post-surveillance notification, with exceptions for when doing so would still compromise an investigation. It is. Therefore, the limitation of the rights to privacy, access to courts and to an effective remedy cannot be justified.

III THE DESIGNATED JUDGE

54. The designated judge is central to RICA's mechanism. She has the ultimate power to authorise the interception of communications. It is vital that she is adequately independent to perform that function. If she is not independent, the limitation of privacy inherent in allowing the state to intercept communications will not be justifiable.

55. The Applicants argue that the designated judge, and the process she employs to issue directions, is insufficiently independent on two grounds:

    55.1. The process is not adversarial; and

    55.2. The designated judge is appointed by the executive for an indeterminate time (normally one year) that is subject to renewal.

56. R2K and PI support these arguments and advance four further lines of argument:

    56.1. Comparative practice supports the arguments that the designated judge is insufficiently independent;

    56.2. The lack of independence makes the limitation of the right to privacy unjustifiable;

    56.3. Requiring the designated judge to be retired further undermines her independence; and

    56.4. The secrecy under which the designated judge operates enhances the need for independence.

COMPARATIVE PRACTICE

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

58. Firstly, many states require surveillance to be approved by a sitting member of the judiciary. In Africa, the following countries require a sitting judge to authorise the issue of a surveillance warrant: Egypt;[45] Ghana;[46] Kenya;[47] and Lesotho.[48] Outside of Africa, countries that require judicial authorisation include Germany,[49] Belgium,[50] Austria,[51] Ireland,[52] the Czech Republic,[53] Bulgaria,[54]

---

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

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

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

[48] Communications Act 2012 read with the Criminal Procedure and Evidence Act 1981.

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

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

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

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

[53] Amendment Code of Criminal Procedure No. 177/2008.

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

Switzerland,[55] Slovenia,[56] Croatia,[57] Portugal,[58] Montenegro,[59] Hungary,[60] Mexico,[61] South Korea,[62] Taiwan,[63] Hong Kong,[64] New Zealand,[65] Canada,[66] the USA.[67] and Chile.[68]

59. In some of these countries (including Bulgaria, Germany, Austria, New Zealand, Taiwan and Mexico) the executive – either the police or the prosecutor –must approach a court to authorise the surveillance. In many European civil-law countries, such as Slovenia, Montenegro and Croatia, it is the investigating judge who performs the role. The investigating judge is a unique civil law

---

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

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

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

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

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

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

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

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

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

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

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

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

[67] US Code, Title 18, ss 2510-2522.

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

institution that oversees the investigative process and also performs other tasks such as issuing ordinary search warrants. In other countries, the sitting judge is part of a panel of judges who performs this role.[69] Many countries provide an exception for when interception is urgent and a warrant cannot be obtained in time. None of the countries the amici considered provide for a single, retired judge to determine surveillance applications.

60. Of course, there are other countries that do not require judicial authorisation,[70] or that require judicial authorisation in some circumstances, and executive authorisation in others.[71]

61. The need for independent authorization of surveillance is supported in international human rights law which treats independent authorization as a fundamental safeguard of the right to privacy. As recommended by the Special Rapporteur: '*Legislation must stipulate that State surveillance of communications must only occur … exclusively under the supervision of an independent judicial authority*.'[72] And the UN High Commissioner for Human Rights has made the same point in the following terms:

> "*Surveillance measures, including communications data requests to business enterprises and intelligence-sharing, should be authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after*

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

[70] Some examples are: India; Australia; Singapore;

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

[72] Report of Special Rapporteur (n 19) at 81.

> *they have been terminated. The independent body authorizing particular surveillance measures, preferably a judicial authority, needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary and proportionate and authorize (or reject) ex ante the surveillance measures.*"[73]

62. There is an obvious advantage to requiring the government to approach the ordinary courts rather than a specifically designated judge. It limits the ability for the executive to choose a specific person who will act favourably. It also ensures that the workload is spread, avoiding the risk that a single judge will be overburdened by the number of applications, and therefore unable to devote sufficient time to each application to ensure that only those which meet the requirements of the Act are granted.

RIGHT TO PRIVACY

63. Whilst R2K and PI agree that lack of independence is a violation of the rule of law and the right of access to courts as the Applicants allege, it also demonstrates that the limitation of the right to privacy permitted by RICA is not justifiable.

64. Any authorisation of a search, or the surveillance of a person's property limits their right to privacy. Ordinarily, these limitations are justified by the grant of a search warrant. The warrant justifies the limitation if it is based on a reasonable suspicion that a crime has been committed, and is issued by an independent judicial officer. This importance of independence appears clearly from our case law regarding search warrants:

---

[73] UNHRC *Privacy in the Digital Age* (n 18) at para 39 (emphasis added, citation omitted).

64.1. In *Heath*, Chaskalson P (as he then was) held that the granting of a search warrant

> *"calls for the qualities and skills required for the performance of judicial functions – independence, the weighing up of information, the forming of an opinion based on information, and the giving of a decision on the basis of a consideration of relevant information.*"[74]

64.2. In *Thint*, Langa CJ wrote:

> *"The fact that the decision as to whether a warrant is to be issued is taken by an impartial and independent judicial officer has been recognised as an important consideration in determining the constitutionality of search powers. … This Court too has recognised that requiring a search warrant to be issued by a judicial officer is an important part of the protection of fundamental rights and, in particular, the right to privacy.*"[75]

64.3. And in *Van der Merwe*[76] Mogoeng J (as he then was) again considered why search warrants justify an intrusion of privacy. He pointed out that, while warrants served to combat crime, they "*inevitably interfere with the equally important constitutional rights of individuals who are targeted by these warrants.*"[77] The limitation is justified by various "*safeguards*" to "*ensure that the power to issue and execute warrants is exercised within*

---

[74] *South African Association of Personal Injury Lawyers v Heath and Others* [2000] ZACC 22; 2001 (1) SA 883; 2001 (1) BCLR 77 (CC) at para 34 (emphasis added).

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

[76] *Minister of Safety and Security v Van der Merwe and Others* 2011 (5) SA 61 (CC) at para 36-8.

[77] Ibid at para 35.

the confines of the authorising legislation and the Constitution."[78] The first safeguard is "*the significance of vesting the authority to issue warrants in judicial officers*".[79] Citing *Thint* and *Heath*, he again noted that the judicial granting of warrants justifies the limitation of privacy because they "*possess qualities and skills essential for the proper exercise of this power, like independence and the ability to evaluate relevant information so as to make an informed decision.*"[80]

65. The independence of a warrant-issuing authority[81] is therefore a key element that justifies the limitation of the right to privacy. If the issuing authority is not independent of the executive, the limitation of privacy will be far harder to justify.

66. For the reasons given by the Applicant, and those set out below, the designated judge is not independent. The limitation of privacy at the heart of RICA – permitting the state to intercept our communications, including the most personal and intimate – cannot be justified.

THE DANGER OF A RETIRED JUDGE

67. While RICA plainly envisages that there may be multiple judges designated to determine applications, the practice has been that only one retired judge is designated. While this practice is not required by RICA, it is consistent with RICA.

---

[78] Ibid at para 36.

[79] Ibid at para 37.

[80] Ibid at para 38 (emphasis added).

[81] The Constitutional Court has not held that the warrant issuing authority must be a judicial officer. But it has held that, if it is not a judge, the issuing authority must have similar characteristics of independence. See, for example, *Thint* (n 75) at para 84.

68. The dangers of allowing surveillance applications to be determined by a single retired judge, hand-picked by the Executive branch for a renewable term is obvious. As the Applicants rightly point out, it is inconsistent with our basic constitutional principles of independence.

69. The fact that RICA requires the designated judge to be a retired judge is, combined with term renewal, extremely problematic. The legislation governing retired judges creates a clear financial incentive for the designated judge to make decisions that will make it more likely that her term will be renewed. Those financial incentives would not be present if the designated judge was a sitting judge.

70. Under the Judges' Remuneration and Conditions of Employment Act,[82] a judge who has been discharged from active service[83] continues to receive a salary[84] and a gratuity[85] calculated according to their active service salary and the length of their service.

71. Judges who have been discharged from active service are also required to continue to perform "service" for up to three months per year until they reach the age of 75.[86] If they do not do so, their salary is reduced. They may voluntarily perform more than three months' service. "Service" is defined to include "*service as a chairperson or a member of a body or institution*

---

[82] Act 47 of 2001.

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

[84] Judges' Remuneration Act s 5.

[85] Judges' Remuneration Act s 6.

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

established by or under any law; or (d) any other service which the Minister may request him or her to perform". That would plainly capture service as the designated RICA judge.

72. Retired judges are, quite rightly, paid monthly for their service.[87] In the case of service as the designated RICA judge, the rate would be determined by the President.[88]

73. As a result, a retired judge who is asked by the Minister of Justice to serve as the RICA Judge has a clear financial incentive to act in a way that makes it more likely that her term will be renewed. The longer she serves as the RICA Judge, the more money she will make. That plainly undermines independence.

74. That would not be the case if RICA required the designated judges to be sitting judges. Sitting judges who were merely assigned to consider RICA applications would not be paid an additional amount. It would also not be the case if the retired RICA Judge's term was not subject to renewal. There would be no possibility of future enrichment as a result of renewal. In either case, there would be no financial incentive that could possibly affect the decisions the designated judge is required to make.

SECRECY

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

---

[87] Judges' Remuneration Act s 7(2).

[88] Judges' Remuneration Act s 7(2)(b). While we were unable to find the specific rate determined for the designated judge

76. First, and obviously, all the applications are determined in secret.[89] Unlike an ordinary court, the applications are not public, and the proceedings are not adversarial.

77. Second, while the designated judge is required to submit reports in terms of the Intelligence Services Oversight Act (**Oversight Act**),[90] the reporting requirements are insufficient to provide the necessary accountability and oversight which may counterbalance the inherent secrecy.

78. The Oversight Act does not specify what information should be provided by the designated judge. This has resulted in inconsistent, undetailed and incomplete reporting on the activities of the designated judge, greatly undermining public and Parliamentary oversight of the judicial function in RICA. No information is available in these reports on:

    78.1. What were the warrants for – direct interception of metadata, direct interception of communication, provision of archived metadata?

    78.2. To how many people did the warrant pertain?

    78.3. To which alleged offence did the investigation pertain?

    78.4. What technology/method was used for the interception?

    78.5. What number of interceptions actually resulted in arrests and convictions?[91]

---

[89] RICA s 16(7).

[90] Act 40 of 1994. Section 3(a)(iii) provides, in relevant part: '*The functions of the Committee are… to obtain from … any designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002), a report regarding the functions performed by him or her in terms of that Act, including statistics regarding such functions, together with any comments or recommendations which such designated judge may deem appropriate: Provided that such report shall not disclose any information contained in an application or direction referred to in that Act*"

[91] Amicus FA at paras 81-86.

79. This information should be available. In the United States, for example, public annual reports include information on the offenses under investigation, types and locations of interception devices, costs and duration of authorized intercepts, and number of arrests and convictions resulting from intercepts.[92]

80. This information is vital to allow the public and oversight bodies to assess whether the directions the judge grants are actually fulfilling their supposed purpose. If only a very small percentage of directions led to arrests or prosecutions, the public could legitimately ask whether too many directions are being granted.

81. There is no challenge to s 3 of the Oversight Act in this application. This Court must accept that the limited reporting requirements are constitutionally compliant. But those limited reporting requirements – coupled with the inherent secrecy of the authorisation process – heighten the need for independence of the designated judge. The question is this: considering that the designated judge performs her work in secret, and that she is not required to report in detail on the work she does, are the structural guarantees of independence adequate? Independence guarantees that are adequate for a court that operates openly may be inadequate to secure the independence of a secret court.

[92] Amicus FA at para 84.

82. The principle of open justice demonstrates they are not. The Constitutional Court[93] and the Supreme Court of Appeal[94] have repeatedly endorsed the principle of open justice. The principle derives from multiple constitutional rights, including the rights to freedom of expression, access to courts and access to information. It is also entrenched by the constitutional guarantees of judicial independence.[95]

83. Open court rooms are a powerful guarantee of independence. As Ponnan JA put it: "*The publicity of a trial usually serves as a guarantee that the matter will be determined independently and impartially. The glare of public scrutiny makes it far less likely that the courts will act unfairly.*"[96] Or as Chief Justice Langa explained in *SABC*: "*The public is entitled to know exactly how the judiciary works and to be reassured that it always functions within the terms of the law and according to time-honoured standards of independence, integrity, impartiality and fairness.*"[97]

84. The Applicants rightly rely on this principle to support the challenge on the absence of notification.[98] But it also buttresses the challenge on the independence of the designated judge.

---

[93] *South African Broadcasting Corporation Limited v National Director of Public Prosecutions and Others* [2006] ZACC 15; 2007 (1) SA 523 (CC); *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services (Freedom of Expression Institute as Amicus Curiae) In re: Masetlha v President of the Republic of South Africa and Another* [2008] ZACC 6; 2008 (5) SA 31 (CC); *Shinga v The State and Another (Society of Advocates, Pietermaritzburg Bar as* Amicus Curiae*); O'Connell and Others v The State* [2007] ZACC 3; 2007 (4) SA 611 (CC)

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

[95] Constitution ss 165 and 173.

[96] *City of Cape Town* (n 94) at para 17.

[97] *South African Broadcasting Corporation* (n 93) at para 32.

[98] Applicants' Heads of Argument at paras 77-79.

85. Openness ensures independence. Where judicial functions are performed in secret, the risk that they will not be performed independently is higher. That enhances the need to ensure that the structural measures to guarantee independence are in place.

III MANDATORY BLANKET RETENTION OF METADATA

86. It is important to be clear about what is at stake here. The Government asserts that it has the power to mandate all telecommunications companies to store all metadata about most South Africans' phone calls, SMSs, emails, and other messaging services, for up to five years. This includes the location from which those communications were made, and may, in some instances, also implicate the content of messages, such as the subject lines of emails. It also asserts the power to mandate internet service providers to capture and store metadata about South Africans' internet activity at all times, for no reason whatsoever. This is a massive and systemic violation of the rights of all people who use cell phones or the internet in South Africa who use phones and computers.

87. The amici curiae take a stronger stance on the mandatory retention of metadata than the Applicants. The Applicants' attack is limited to two aspects of RICA:

87.1. First, it is directed at s 30(2)(a)(iii) of RICA, which obliges the Minister to issue a directive determining the period for which a telecommunication service provider must store metadata. The period must be between three and five years. The Applicants argue that three years is too long.

87.2. Second, the Applicants rightly complain about the absence of oversight mechanisms for the stored metadata. In particular, the Applicants contend that RICA must have mechanisms regulating "*the proper procedure to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions*".[99]

[99] Applicants' Heads of Argument at para 190.

88. R2K and PI support these arguments. If the mandatory, blanket retention of metadata could be constitutional, it could only be constitutional if the data is kept for short periods and subject to clear safeguards.

89. But the *amici* argue that the mandatory blanket retention of metadata can never be constitutional. Even with the safeguards set out by the applicants, it unjustifiably limits the right to privacy to mandate all phone and internet providers to store metadata about all South Africans all the time.

90. However, R2K and PI accept that, given the way in which the Applicants' challenge is framed, it is not possible for this Court, at this time, to grant the broader relief they contend the Constitution requires. For the purposes of this application, the *amici*'s submission are limited to:

    90.1. Explaining in more detail how metadata is retained under RICA, and how it is accessed;

    90.2. Demonstrating that there is a strong case that mandatory blanket retention of metadata – even for a shorter period and with safeguards – unjustifiably limits the right to privacy;

    90.3. Asking this Court to leave the door open for a future frontal attack to mandatory blanket retention of metadata.

MANDATORY BLANKET RETENTION OF METADATA UNDER RICA

91. To understand the scope and impact of the surveillance of all South Africans that RICA permits, it is necessary to consider various provisions of RICA. We first consider how metadata is retained, and then how it is accessed.

Retention

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

92.1. "Communication-related information" is metadata – it is all information available to an electronic communication service provider about a communication other than its content. It is defined as:

> "*any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system*".

92.2. To appreciate the full breadth of the definition, it is necessary to look at the definition of "*indirect communication*":

> "*the transfer of information, including a message or any part of a message, whether-*
>
> *(a) in the form of-*
>
> *(i) speech, music or other sounds;*
>
> *(ii) data;*
>
> *(iii) text;*
>
> *(iv) visual images, whether animated or not;*
>
> *(v) signals; or*
>
> *(vi) radio frequency spectrum; or*
>
> *(b) in any other form or in any combination of forms,*
>
> *that is transmitted in whole or in part by means of a postal service or a telecommunication system*"

93. With regard to whom the obligation rests on, RICA is somewhat confusing. In 2006, an amendment removed the definition of "*telecommunication service provider*" and replaced it with a definition of "*electronic communication service provider*", without amending the references to the former in the body of the Act, including in s 30. The term "*electronic communication service provider*" is defined with reference to the Electronic Communications Act 36 of 2005, as:

> "*(a) person who provides an electronic communication service under and in accordance with an electronic communication service licence issued to such person under Chapter 3 of the Electronic Communications Act, and includes any person who provides-*
>
> *(i) a local access communication service, public pay-telephone service, value-added network service or private electronic communication network as defined in the Electronic Communications Act; or*
>
> *(ii) any other electronic communication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act; and*
>
> *(b) Internet service provider*"

94. In essence, it includes all phone operators and all internet service providers. The latter term is broadly defined in RICA as "*any person who provides access to, or any other service related to, the Internet to another person*". This obviously includes companies like Telkom, MWeb or WebAfrica that provide internet connections to customers. But it also potentially includes all hotels, cafes, and workplaces that offer internet connections.

95. Section 30(1)(b) is stated in broad terms. The details of the obligation to store metadata are meant to be set out in directives issued by the Minister under

s 30(2)(a)(iii). The Minister has exercised that power with regard to phone operators.[100] She has not issued a directive to deal with internet service providers.[101] In the absence of a directive, it is not clear whether and in what manner internet service providers are complying with their obligation to store metadata.

96. Once the information is stored, it is regarded as "*archived communication-related information*". Section 12 of RICA prohibits the electronic communication service provider from disclosing this information to anyone but the customer.

Access

97. Metadata can be accessed by the government using a direction issued in terms of s 19 of RICA. This has the following limitations and safeguards:

97.1. It can only be obtained if there are "*reasonable grounds*" to believe that certain types of serious offences, or threats to national security exist, and the communication related information is "*necessary for purposes of investigating such offence or gathering such information*";[102]

---

[100] GN 1325 of 28 November 2005: *Directives in respect of different categories of telecommunications service providers made in terms of the Act.*

[101] The above directive addresses internet service providers in Schedule C. However, it only deals with interception, and not with the storage of communication related information.

[102] RICA s 19(4), which reads in full:

> *on the facts alleged in the application concerned, … there are reasonable grounds to believe that-*
>
> *(a) a serious offence has been or is being or will probably be committed;*
>
> *(b) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;*
>
> *(c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;*
>
> *(d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in*

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

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

97.4. The application is not made to the designated judge, but to "*a judge of a High Court, a regional court magistrate or a magistrate*".[103] However, if a judicial officer issues the direction, she must provide a copy to a designated judge,[104] who must ensure it is kept for at least five years.[105]

98. However, archived communication-related information can also be accessed outside of s 19 of RICA. In fact, all this metadata can be accessed at <u>any time</u>, by virtually <u>any prosecutor</u> for an investigation into <u>any crime</u> without having to make out <u>any case</u> at all.

99. This flows from s 15 of RICA read with s 205 of the Criminal Procedure Act 51 of 1977 (**CPA**). Section 15 of RICA provides:

> "*(1) Subject to subsection (2), the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in sections 17 and 19 does not*

> *connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in-*
>
> *(i) accordance with an international mutual assistance agreement; or*
>
> *(ii) the interests of the Republic's international relations or obligations; or*
>
> *(e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary,*
>
> *and that the provision of archived communication-related information is necessary for purposes of investigating such offence or gathering such information.*

[103] RICA s 19(1).

[104] RICA s 19(7).

[105] RICA s 19(8).

preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act.

(2) Any real-time or archived communication-related information which is obtained in terms of such other Act may not be obtained on an ongoing basis."

100. Section 205(1) of the CPA is one such procedure. It provides for a person to be subpoenaed to provide documents or answer questions before a magistrate with regard to any offence. It is a routine tool of all criminal investigations.

101. The provision reads:

> "*A judge of a High Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection (4) and section 15 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, upon the request of a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the Director of Public Prosecutions, require the attendance before him or her or any other judge, regional court magistrate or magistrate, for examination by the Director of Public Prosecutions or the public prosecutor authorized thereto in writing by the Director of Public Prosecutions, of **any person** who is likely to give material or relevant information as to **any alleged offence**, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the Director of Public Prosecutions or public prosecutor concerned prior to the date on which he or she is required to appear before a judge, regional court magistrate or magistrate, he or she shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.*" (emphasis added)

102. The reference to RICA was added in 2002, with effect from 2005.[106]

103. Section 205 – as amended – is clearly intended to be used to obtain archived communications related information. Yet s 205 contains none of the safeguards in s 19 of RICA:

103.1. A request under s 205 can be made to investigate any offence;

103.2. It is not necessary to know the identity of the alleged offender;

103.3. There is no requirement of "*reasonable grounds*", or that the information is "*necessary*" in order to investigate an offence;

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

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

104. In practice, s 205 warrants are extremely easy to obtain. Indeed, the vast majority of metadata requests are not made in terms of s 19, but in terms of s 205. The applications for subpoenas are generally determined on paper, in chambers by any magistrate or judge.[107] The resulting subpoena is then handed to the cell phone company official, who provides the records directly to the police or the prosecutor and therefore never appears in front of a magistrate.

105. The way in which s 205 is used is apparent from the matter of *S v Miller and Others*.[108] The police seized the accused's cell phones. It then subpoenaed the cell phone operators in terms of s 205 for the records of the accused, and various other witnesses. The companies provided the information. It was then "*fed into a laptop computer equipped with a software program called 'Analyst*

[106] Section 59 of Act 70 of 2002.

[107] Amicus FA at para 57.

[108] 2016 (1) SACR 251 (WCC).

Notebook' " which was "*used to collate data and to provide a visual link where similarities are found*".[109] That analysis "*will show when particular cellphone numbers have been in contact with each other*".[110] The police can then determine "*who called whom, for how long they spoke, what handsets were used during the conversations and where each handset was geographically located during the call.*"[111]

106. It is important to stress that, under both s 19 of RICA and s 205 of the CPA, the state can obtain information not only about an alleged offender, but about any person whose metadata might be relevant to the offence. This would include his friends, family and colleagues if their communications or movements are necessary (in the case of s 19 of RICA) or relevant (in the case of s 205) to an investigation.

Conclusion

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

107.1. All phone companies must maintain a record of the who, when, how and where of every single phone call and SMS of their users.

107.2. All ISPs will be obliged (once the Minister publishes a directive) maintain a record of every website any person visits, and the who, when, how and where of every electronic message sent, including emails, Whatsapp, Facebook messages or any other form of electronic communication. That includes telecommunication service providers

[109] Ibid at para 17.

[110] Ibid.

[111] Ibid.

who operate as ISPs when consumers use their phones to access the internet. In the case of emails, the communication-related information includes the subject of the email.

107.3. That information must be stored in accordance with a directive issued by the Minister, for up to five years.[112]

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

108. The amici do not attack the validity of s 205 – the Constitutional Court has held that it is constitutional.[113] The problem is that s 205 was created long before the internet and cellphones existed, and before RICA mandate cellphone companies to store our metadata. As the Western Cape High Court explained: "*Section 205 was extensively used in the pre-constitutional era for the examination of persons (often members of the media) to obtain information regarding the sources of their reports, or generally to glean information about the commission of an offence.*"[114] It was not used to effectively track and monitor the populace.

109. RICA has radically enhanced the capacity of s 205. Whereas it used to be employed primarily to require a person to answer a question or produce a document, it is now employed as a substitute for s 19 of RICA in order to track people's movements and communications. And it can only serve that purpose

---

[112] RICA, section 30(2)(a)(iii).

[113] *Nel v Le Roux NO and Others* [1996] ZACC 6; 1996 (3) SA 562 (CC).

[114] *S v Miller* 2016 (1) SACR 251 (WCC) at para 21.

because s 30 of RICA obliges telecommunication service providers to store metadata for between three and five years.

LIMITATION OF PRIVACY AND EXPRESSION

110. For those people who have cellphones the information that phone operators and ISPs are mandated to store is incredibly personal. It is information about when, where, how and with whom we communicate. It is information about what internet sites we visit. For those with cellphones – and particularly those who own smartphones – the metadata will literally track their movements minute by minute. Every time the phone makes a connection with the network – whether to make a call, check for emails, update an app, or any other purpose – the service provider will be obliged to record the user's location.

111. While cellphones allow the greatest intrusion into our private lives, it still applies to users of landlines, computers, or any other device that connects to the internet or a telecommunication network – smartwatches, tablets, smart TVs and so on. Information about our use of all of these devices is captured and stored.

112. This information is incredibly sensitive, and its collection is extremely invasive of the right to privacy. The only available information that is left untouched is the actual content of the messages. But the metadata on its own – especially when looked at systematically over a period of time – can tell the government a huge amount about a person's private life. Governments use this information not only to obtain evidence for prosecution of particular offences, but to build

detailed profiles of people – who they interact with, where they move, what their interests are.

113. In this section, we first show with reference to international and comparative law, that mandatory blanket retention of metadata under RICA violates the right to privacy, and the right to free expression. We consider international, European and American law. We then explain why the concerns expressed in those jurisdictions limit the right in the South African context.

International Law

114. In 2014, the UN High Commissioner for Human Rights issued a report titled *The Right to Privacy in the Digital Age*. The report deals with a range of issues, and particularly with surveillance. It says two things of central importance to mandatory blanket retention of metadata.

114.1. It dismisses the argument that metadata is necessarily less intrusive of the right to privacy than the content of a communication: "*The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.*"[115]

114.2. It holds that mandatory blanket retention of metadata " *'just in case' it is needed for government purposes … appears neither necessary nor proportionate.*"

[115] *Right to Privacy in the Digital Age 2014* (n 17) at para 19.

115. The subsequent 2018 Report of the UN High Commissioner for Human Rights on *The Right to Privacy in the Digital Age* has confirmed the point:

> "*States continue to impose mandatory obligations on telecommunications companies and Internet service providers to retain communications data for extended periods of time. Many such laws require the companies to collect and store indiscriminately all traffic data of all subscribers and users relating to all means of electronic communication. They limit people's ability to communicate anonymously, create the risk of abuses and may facilitate disclosure to third parties, including criminals, political opponents, or business competitors through hacking or other data breaches. Such laws exceed the limits of what can be considered necessary and proportionate.*"[116]

116. That conclusion is supported by a finding of the Human Rights Committee in its 2016 periodic report on South Africa.[117] The Committee stated that it was "*concerned about the wide scope of the data retention regime under the Act.*"[118] It recommended that South Africa should "*consider revoking or limiting the requirement for mandatory retention of data by third parties.*"[119] That concern was repeated in several other conclusions assessing states compliance with the International Covenant on Civil and Political Rights.[120] In the United States,

---

[116] *Right to Privacy 2018* (n 18) at para 18 (emphasis added).

[117] *Concluding Observations on the Initial Report of South Africa* Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1, paras. 42-43 (27 April 2016).

[118] Ibid at para 42.

[119] Ibid at para 43.

[120] *Concluding Observations on the Sixth Periodic Report of Italy, UN Human Rights Committee* U.N. Doc. CCPR/C/ITA/CO/6, para. 37 (28 March 2017). See also *Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland*, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015).

for example, it called on the US to "*[r]efrain from imposing mandatory retention of data by third parties*".[121]

117. The UN Special Rapporteur on the Right to Freedom of Opinion and Expression has also recognised how mandatory data retention threatens free expression by limiting their ability to remain anonymous:

> "*Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.*"[122]

European Law

118. The Applicants rely heavily on *Weber and Saravia v Germany*[123] for their argument concerning the safeguards that should apply to access to intercepted data, and to mandatorily stored of metadata. The *amici* agree that those safeguards are important for data is intercepted – but they cannot cure the privacy violation caused by the mandatory blanket retention of metadata.

119. *Weber* did not concern metadata. It was concerned with the surveillance of communications on both an individual and a systemic basis. The European

---

[121] *Human Rights Committee Concluding observations on the fourth periodic report of the United States of America* CCPR/C/USA/CO/4 (2014) at para 22(d).

[122] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (22 May 2015) U.N. Doc. A/HRC/29/32 at para 55.

[123] [2006] ECHR 1173.

Court of Human Rights did not in *Weber* – and nor has it subsequently – endorsed mandatory retention of metadata subject to safeguards.

120. Most recently, in *Big Brother Watch*, the ECHR declined to decide whether the *Weber* safeguards applied to the bulk surveillance of metadata.[124] However, it recognised the severe privacy intrusion of allowing the state to collect large quantities of metadata:

> "*[T]he Court is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content. For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with The European Court of Justice, however, has.*"[125]

121. It held that the failure to apply the same safeguards to metadata that were applied to the content of communications was one of the reasons that the UK's bulk surveillance regime was inconsistent with the Charter.[126]

122. In *Digital Rights Ireland Ltd v Ireland*,[127] the CJEU considered a direct attack on a directive of the European Parliament concerning the retention of metadata.

---

[124] *Big Brother Watch and Others v The United Kingdom* [2018] ECHR 722 at para 352. This decision will be reviewed by the Grand Chamber of the ECHR later this year. I discuss it in more detail below.

[125] *Big Brother Watch* at para 356.

[126] *Big Brother Watch* at para 357.

[127] *Digital Rights Ireland (Judgment of the Court)* [2014] EUECJ C-293/12.

Article 5 of the Directive defined in detail the type of data to which it applied, including all the types of metadata discussed above – basically everything except the content of the communication. Article 4 obliged member states to "*adopt measures to ensure that the data specified in Article 5 of this Directive are retained*". The metadata had to be stored for between six months and two years. The directive justified its provisions on the basis that

> *"retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive.*

123. Challenges were raised in domestic courts in both Ireland and Germany attacking the validity of the Directive. They were referred to the CJEU for a decision on whether they were compatible with European law, including the European Charter on Human and Peoples' Rights.

124. The CJEU held that the Directive was not compatible with arts 7 and 8 of the Charter of Fundamental Rights of the European Union. First, it pointed out that even though the Directive did not permit the storage of the actual communication, it permitted a real invasion of a person's privacy:

> *"Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out,*

the social relationships of those persons and the social environments frequented by them."[128]

125. The retention of metadata was covered by both arts 7[129] and 8[130] of the European Charter.

126. Second, the retention of the data also impacted on the right to free expression because the fact of mandatory retention "*might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive*".[131]

127. The CJEU stressed that both the retention of the data[132] and subsequent state access of the data[133] limited the privacy rights in the Charter. It held that the limitation was "*wide-ranging*" and "*particularly serious*". As the Court explained, the mandatory and untargeted retention of metadata "*is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.*"[134]

128. Turning to a justification analysis, the Court recognised the important purpose of targeting serious crime, and accepted that mandatory blanket retention of

---

[128] Ibid at para 27. See also *Tele2 Sverige/Watson* [2016] EUECJ C-203/15 at para 99.

[129] Art 7 reads: "*Everyone has the right to respect for his or her private and family life, home and communications.*"

[130] Art 8 reads:

"***Protection of personal data***

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

[131] *Digital Rights Ireland* (n 127) at para 28.

[132] Ibid at para 34.

[133] Ibid at para 35.

[134] Ibid at para 37.

metadata served that goal.[135] But it held that the importance of the purpose "*does not, in itself, justify a retention measure such as that established by [the] Directive*".[136]

129. The limitation was not justified, the court held, for two primary reasons. First, there were inadequate safeguards. But second, the retention of data was "*generalised*". As the Court explained, the Directive applied "*to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives.*"[137] Because it applied to all subscribers, it constituted "*an interference with the fundamental rights of practically the entire European population.*"[138]

130. The Directive (like RICA) applied to all forms of electronic communication, and all metadata, of all subscribers "*without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.*"[139] It demanded the retention of metadata even of "*persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.*"[140] As the Court pointed out, the retention obligation was not limited to any particular time, geographic zone, circle of persons likely to be involved in serious crime; it applied to everybody indiscriminately.

131. The CJEU concluded that – notwithstanding the value of metadata in fighting crime – the Directive was "*a wide-ranging and particularly serious interference*

---

[135] Ibid at paras 41-44.

[136] Ibid at para 51.

[137] Ibid at para 56.

[138] Ibid.

[139] Ibid at para 57.

[140] Ibid at para 58.

with [the] fundamental rights [of privacy] in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[141] It held that the Directive was invalid.

132. The CJEU upheld this conclusion in *Tele2 Sverige/Watson* in December 2016.[142] The case concerned both Swedish and UK laws that provided for mandatory blanket retention of metadata. The Court repeated its concerns in *Digital Rights Ireland* about the impact of metadata to violate the right to privacy, emphasising that it allowed the government to develop a profile of an individual "*that is no less sensitive, having regard to the right to privacy, than the actual content of communications.*"[143]

133. Again, the Court held that the "*indiscriminate*" nature of the retention obligation exceeded "*the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society.*"[144] The European Charter, however, allows legislation permitting "*the <u>targeted</u> retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*"[145] None of those limits concerning the scope of the retention are present in RICA.

---

[141] Ibid at para 65.

[142] *Tele2/Watson* (n 128).

[143] Ibid at para 99.

[144] Ibid at paras 106-107.

[145] Ibid at para 108 (emphasis added).

The United States

134. Two cases of the United States demonstrate the dangers of mandatory retention of metadata: *Riley v California*[146] and *Carpenter v United States*.[147]

135. *Riley*, decided in 2014, concerned whether police needed a search warrant to examine the data on a person's cell phone which was in their possession when they were arrested. The Court held that a warrant was required. While the case related to all the data on the phone – not only the metadata – Chief Justice Roberts set out why the data cell phones store, including the metadata, demands privacy protection.

136. He explained that "cell phone" is a "misleading shorthand" as modern cell phones "*are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.*"[148] In particular, Roberts CJ noted that the location data collected by modern phones was particularly intrusive of privacy:

> "*Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. … "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'* "[149]

---

[146] 573 U.S. __ (2014); 134 SCt 2473.

[147] 585 US ____ (2018); 138 SCt 2206.

[148] *Riley* (n 146) at 17.

[149] *Riley* (n 146) at 19-20, quoting *United States* v *Jones* 565 US (2012) (Sotomayor J, concurring) (slip opinion at 3).

137. The Court returned directly to the issue of tracking a person's locations through their phone in *Carpenter*, decided in 2018. In *Carpenter* the Supreme Court considered the process for obtaining metadata from cell phone companies, and particularly cell-site location information (CSLI). This information tracks where a cell phone user is at any time their cell phone is operational. In the US, the retention of this information was not mandatory, but was stored as part of the agreement between the user and the provider for the provider's own business purposes.[150]

138. The FBI obtained Carpenter's CSLI under a statute[151] that established a procedure comparable to s 205 of the CPA. It entitled the FBI to demand the information from a cell phone carrier, without any independent authorisation, if it could show "*reasonable grounds*" for believing that the records were "*relevant and material to an ongoing investigation*". As the Supreme Court noted, that "*falls well short of the probable cause required for a warrant*".[152]

139. The question in *Carpenter* was whether accessing CSLI without a warrant was consistent with the US Constitution's Fourth Amendment which protects "*[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*". The Court – by a 5-4 majority – held that it was not.

---

[150] The Court described those purposes as follows: "*finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.*"

[151] The Stored Communications Act

[152] *Carpenter* (n 147) at 19.

140. The majority judgment – again by Roberts CJ – sets out in detail just how intrusive it is to permit access to this type of data, by comparing it to the pre-digital age:

> "*Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." For that reason, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." Allowing government access to cell-site records contravenes that expectation."*[153]

141. This data "*tracks nearly exactly the movements of its owner. … when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.*"[154]

142. And providing the government the power and the right to access information about where we have been "*provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." These location records "hold for many Americans the 'privacies of life.'* "[155]

143. Most importantly for the concern about the mandatory blanket retention of metadata, granting access to several years of location information allows the government to "*travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain*

---

[153] Ibid at 12 (citations omitted).

[154] Ibid at 13 (emphasis added).

[155] Ibid at 12-13 (citations omitted).

records for up to five years."[156] In South Africa, that immense power is not even limited by the vagaries of carriers' business needs; the time travel machine is mandated by legislation.

144. Lastly, the Supreme Court decried the blanket nature of the surveillance, which applied to almost all Americans who used cell phones:

> "*[B]ecause location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. … Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.*"[157]

145. *Carpenter* could be interpreted as supporting RICA. It allows access to metadata if the government obtains a warrant – exactly what s 19 of RICA requires. But there are two major difficulties:

145.1. There was no statutory obligation for cell phone carriers to store metadata. As we expand on below when we consider the international and European law – that is the fundamental violation in RICA.

145.2. RICA does – through s 205 of the CPA – permit access to mandatorily stored metadata without a warrant, but through exactly the type of subpoena process that *Carpenter* rejected.

---

[156] Ibid at 13.

[157] Ibid at 13-14.

South Africa

146. The type of information s 30 of RICA requires companies to store is fundamentally personal information, and is particularly revealing of individuals' private lives when it is aggregated over a period of time. For those who possess cell phones, is the equivalent of being constantly tracked and monitored by the state.

147. Evidently this information as a whole concerns an "*individual's intimate personal sphere of life*".[158] Obliging companies to retain such information – for any length of time and with even the most stringent safeguards –violates the right to privacy.

148. The interference arises both from the fact that it is stored by a private company at the behest of the government, and from the fact that the government can access that data, with little or no safeguards, for the investigation of any crime.

149. Further, as the CJEU and international law demonstrates, RICA also violates the right to free expression.[159] Even though the content of the communication is not recorded, the mandatory, blanket retention of metadata may prevent people from freely communicating with others because of the knowledge that the private information revealed by their metadata is available to the state. This has been recognised, for example, by the United Nations and Inter-American Special Rapporteurs on free expression:

---

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

[159] 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 or ideas;
(c) freedom of artistic creativity; and
(d) academic freedom and freedom of scientific research.

'It is especially concerning that indiscriminate access to information on communication between persons can have a chilling effect on the free expression of thought and the search for and distribution of information in the region.'[160]

150. Chilling how people communicate because of the ever-present threat of government surveillance is a clear violation of the right to free expression. It chills expression in at least two ways:

150.1. It forces people to choose between expression and privacy. If they want access to all the multitude of benefits that cell phones and internet access provide, they must be willing to forsake their privacy.

150.2. It will affect how people communicate. People may be unwilling to use the most effective means of communication because there will be a record that they have done so, which can be easily accessed by the state.

JUSTIFICATION

151. The Government seeks to justify this power because one day it might need the information in serious criminal investigations, and to combat threats to national security. This temptation is understandable. When crimes are committed we naturally want to be able to use all means available to identify and prosecute the wrongdoers. Seeking to investigate, punish and prevent those crimes is plainly a legitimate government objective.

[160] Joint Declaration on surveillance programs and their impact on freedom of expression (June 21, 2013). Accessible from: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1

152. But there are four reasons why this can never justify the scheme created by RICA.

153. First, individualized reasonable suspicion is an established and fundamental safeguard to protecting the right to privacy. There must be some reason to suspect a particular person of wrongdoing in order to justify limiting their privacy. This was expressly held by the Constitutional Court in *Hyundai*, in a matter concerning the issue of a search and seizure warrant:

> "*The warrant may only be issued where the judicial officer has concluded that there is a reasonable suspicion that such an offence has been committed, that there are reasonable grounds to believe that objects connected with an investigation into that suspected offence may be found on the relevant premises and, in the exercise of his or her discretion, the judicial officer considers it appropriate to issue a search warrant. These are considerable safeguards protecting the right to privacy of individuals.*"[161]

154. That is why, in *Tele2/Watson*, the CJEU held that combatting serious crime, even organised crime and terrorism, cannot justify indiscriminate retention of metadata:

> "*while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention*

[161] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* [2000] ZACC 12; 2001 (1) SA 545 (CC); 2000 (10) BCLR 1079 (CC) ('*Hyundai*') at 52.

of all traffic and location data should be considered to be necessary for the purposes of that fight."[162]

155. Under RICA, everybody's metadata is retained, regardless of whether they are suspected of having committed a crime or not. As the CJEU has held, mandatory targeted retention of metadata may well be justifiable. But obliging companies to store everybody's data, all the time, "*just in case*", is not.

156. Third, the same purpose could be achieved through a less restrictive, more targeted regime for the retention of metadata. The onus is on the state to show that a targeted retention regime would not serve the goals of crime-fighting as well as the boundless retention of every single person's metadata.[163] Limiting whose metadata is retained, how long it is retained, when it can be accessed, as well as the safeguards for its storage would all be less restrictive means.

157. Lastly, under s 205 of the CPA, the state can access the metadata to investigate any crime, not only serious crimes and threats to national security. And it does so with an ordinary subpoena process on a very low standard of proof. That is totally inconsistent with international and comparative precedent.

---

[162] *Tele2/Watson* (n 128) at para 103.

[163] See *S v Makwanyane and Another* [1995] ZACC 3; 1995 (6) BCLR 665; 1995 (3) SA 391 at 102: '*[i]t is for the legislature, or the party relying on the legislation, to establish this justification, and not for the party challenging it to show that it was not justified.*' and, for example, *Johncom Media Investments LTd v M and Others* 2009 (4) SA 7 (CC) at para 30: '*The purpose could be better achieved by less restrictive means.*'

CONCLUSION

158. The scheme for the mandatory retention of metadata is inherently unconstitutional. However, in this application, this Court is limited to particular limited aspects of that scheme. What should it do? Two things.

159. First, it should declare those aspects challenged by the Applicants unconstitutional. In determining the Applicants' challenges this court should keep in mind that the serious nature of the violations set out above. The time limit on retention, and the safeguards for storage an absolute minimum that should be required.

160. Second, it should leave the door open for the intended challenge to the scheme as a whole. In deciding the case before it, this court can make clear that it is not precluding a future challenge to the principle of mandatory, blanket retention of metadata.

V BULK SURVEILLANCE

161. The Respondents admit that the intelligence services are engaging in unregulated bulk surveillance of foreign signals. The Applicants rightly point out that it is unlawful both because it is **unauthorised**, and because it is **unregulated**. It occurs without any limits, safeguards or meaningful oversight.

162. R2K and PI agree that unauthorised and unregulated bulk surveillance is unlawful. And they support the arguments advanced by the Applicant for why the NSIA does not authorise bulk surveillance of foreign signals.

163. But they go further. They contend that bulk surveillance will always be unconstitutional even if it is authorised and regulated. That is because bulk surveillance, like the blanket retention of metadata, is indiscriminate and untargeted, and allows the state to intercept, store, analyse and disseminate the most personal information about our lives – our emails, our social media, our diaries, our browsing history, where we travel, the movies we watch, the books we read. It is the most intrusive possible search, and it is conducted on everybody, all the time, without any suspicion that any of us have committed any crime. It can never be constitutionally justified.

164. But – as with the mandatory retention of metadata – that is not the case the Applicants make. They make the narrower case that assumes that properly authorised and regulated bulk surveillance could be constitutionally justifiable. In doing so, they do not capture the true scope of bulk surveillance, or the danger it poses to our democracy.

165. R2K and PI again ask this Court to keep the door open to the broader challenge. Accordingly, this Part covers the following topics:

165.1. The operation of bulk surveillance;

165.2. Why bulk surveillance limits the rights to privacy and free expression;

165.3. Why the limitation of privacy is unjustifiable; and

165.4. How this Court should decide the case.

OPERATION OF BULK SURVEILLANCE

166. The Government has provided scant detail about how its mass surveillance system operates. Based on the affidavit of the DG of the State Security Agency, the following emerges:

166.1. Bulk surveillance is employed for "*environmental scanning*" to search internet traffic "*for certain cue words or key phrases*".[164]

166.2. It is conducted by "*tapping or recording transnational signals*", including undersea fibre optic cables.[165]

166.3. The interception includes both the communication itself, and the information about the communication (the metadata).

166.4. Bulk surveillance "*is not directed at individuals*".[166] For that reason, it is not "*restricted by Foreign Signal Intelligence requirements*".[167]

166.5. Once data is intercepted, it is stored, and backup copies of all the data are automatically made. There are both internal storage, and external storage. The process of recording, copying and storing data is "*automated, executed and managed internally by the system.*"[168]

---

[164] State Security AA at para 130: Record p 795.

[165] State Security AA at para 131: Record p 795.

[166] State Security AA at para 136: Record p 796.

[167] State Security AA at para 136: Record p 796.

[168] State Security AA at para 139: Record p 798.

However, the stored information can be accessed by "*authorised technical personnel*".[169]

166.6. However, the "*direction of communication can only accurately be determined by human intervention and analysis*".[170]

167. The explanation does not provide a full picture of how the bulk surveillance occurs. In particular, there is very little explanation of how the data is accessed, analysed and (if at all) deleted. Who is able to access the data? What criteria must be met in order to permit access? What criteria are used to discard data? What tools are used to analyse the data? Is the information shared with other domestic or foreign intelligence agencies? If so, under what conditions? Are the data stored indefinitely or are they deleted? If so, when?

168. All of this information is vital to assessing the nature and extent of the violation of the right to privacy. Yet it is absent precisely because the NCC operates in secrecy, and without a legal mandate.

169. Based on comparative information bulk surveillance happens in six stages.[171] At each stage, there is a substantial interference with the privacy of communications and private life.

169.1. **Interception** – The first step is to obtain a signal from a source, e.g. by tapping a fibre optic cable.

169.2. **Extraction** – The intercepted signals are then copied and converted into a digital stream so that the data can be reconstructed into an intelligible format.

---

[169] State Security AA at para 139: Record p 798.

[170] State Security AA at para 136: Record p 796.

[171] See Amicus FA at para 94.

169.3. **Filtering** – The data can then be filtered, including in real-time or shortly after interception. Information of potential interest may be selected at this stage through the use of a database of identifiers or selectors. Low value information, such as the content of video streaming from well-known commercial providers, may be discarded.

169.4. **Storage** – Information is retained in a database for potential future analysis or dissemination.

169.5. **Analysis** – Once held in databases, there can then be further querying, examining or data-mining of the information.

169.6. **Dissemination** – The product of the intercept may then be shared with or distributed to other persons, organisations or agencies. Sharing can also occur in earlier stages of the interception process, for example, by providing foreign agencies access to entire databases, which may store raw intercept material.

170. Based on the available evidence, it appears that the NCC follows a similar process.

171. The right to privacy is violated at each one of these stages – when data is intercepted, extracted, filtered, stored, analysed and disseminated.

LIMITATION OF THE RIGHT

172. Given the limited information available about bulk surveillance, it is impossible to determine the precise extent to which our right to privacy is being violated by

the Government. In fact, the absence of clear information compounds the violation.

173. The real problem with bulk foreign surveillance is that – even if it were permitted by domestic law – it would *still* impermissibly limit the right to privacy. The fundamental problem is that the state asserts the right to capture virtually all internet traffic that enters and leaves South Africa.

174. Because of the nature of internet communications, which rely on servers and service providers across the world, the ability to monitor "foreign" signals is, in fact, also the ability to monitor the internet communications originating or ending in South Africa. When a South African sends an email from South Africa to another South African in South Africa, that signal will often travel to a foreign server, through one of the undersea fibre optic cables that the state admits that it taps. The same is true when a South African visits a website, makes a Skype call, downloads a document from Dropbox, or accesses their online diary. All those communications are "foreign" and are liable to be intercepted by the NCC.

175. The Government does not shy away from this reality. It asserts that foreign signals intelligence "*includes any communication that emanates from outside the borders of [South Africa] and passes through or ends in the Republic*".[172] Indeed, the Director-General of Intelligence candidly admits that the NCC cannot even determine "*whether a communication emanates from outside the borders or simply passes through or ends in the Republic of South Africa.*"[173] Therefore, on the Government's own version, they are entitled to intercept,

[172] State Security AA at para 132: Record p 795.

[173] State Security AA at para 136: Record pp 796-7.

store, and analyse virtually all emails and internet traffic, without a warrant, and without statutory safeguards.

176. This is a palpable violation of the right to privacy. In the pre-digital age, it is the equivalent of allowing the state, without regulation, to make copies of every person's private communications, diaries, and libraries. When combined with the metadata attached to the content of communications, it can also allow the government to track a person's movements in the present, past and future.

177. While access to digital services is still so expensive it remains beyond the reach of many South Africans, as more and more South Africans gain access to the internet, a significant portion of our lives are lived online. We communicate online. We work online. We socialise online. We obtain our news, information and entertainment online. We use the internet to keep records and diaries, arrange travel, and conduct financial transactions. Much of this activity is conducted on mobile digital devices, which are seamlessly integrated into our personal and professional lives. They have replaced and consolidated our telephones, our filing cabinets, our wallets, our private diaries, our photo albums and our address books.

178. All of this information about our private and professional lives travels back and forth between individual computers and smartphones in South Africa, and servers located all over the world. And every time that information crosses the South African border, the NCC asserts a right to intercept, copy (repeatedly), store, access and analyse this information about our lives.

179. This traffic includes both the communication content itself, and the metadata. In this case, the metadata includes information about emails and other electronic communications, as well as browser history. It may, in some

instances, also include location data if the device is interacting with a server outside the Republic. For example, if a person uses Google Maps, the search information as well as their location may well be captured by bulk surveillance because the signal will travel to Google's servers that are located outside South Africa. The "*tireless surveillance*" that the US Supreme Court identified in *Carpenter* is enabled not only by the blanket retention of metadata, but by bulk surveillance.

180. For the reasons outlined earlier with regard to the mandatory blanket retention of metadata, bulk surveillance also limits the right to free expression. If I know that my communications will be intercepted by the state, I may not communicate, or may not communicate at all in the cheapest most efficient way. Constant state surveillance chills speech.

181. Of course, the fact that all this surveillance is unauthorised and unregulated exacerbates the problem. It means it is impossible to hold the intelligence services to account for even the most basic requirements. We simply do not know what data are being captured, stored and analysed. And there is no mechanism to prevent abuse. The effect of an absence of any regulatory framework is clear in the instances of abuse pointed out by the Applicants.[174]

182. To be clear, R2K and PI's position is that unregulated, untargeted surveillance of information, merely because it happens to cross South Africa's borders limits the right to privacy and the right to free expression. That is not to say that the intelligence services are prohibited from intercepting any foreign

[174] FA at paras 142-143: Record pp 65-69.

communication. But they can only do so in a way that is targeted and carefully regulated. The current regime exhibits neither of those features.

COMPARATIVE AND INTERNATIONAL PRACTICE

183. The Government makes little attempt to justify foreign bulk surveillance. Its primary defence seems to be that these practices are common in other jurisdictions. While mass surveillance systems exist in other countries, they are not unauthorised and unregulated in the way that the current South African system is. If a comparable foreign system is so unregulated and unauthorised, it would undoubtedly violate international law. Moreover, there are strong argument in international and European law that bulk surveillance is impermissible.

International Law

184. It is inconsistent with the International Covenant on Civil and Political Rights (ICCPR) to which South Africa is a party.[175] Article 17 of the ICCPR protects the right to privacy.[176] The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has noted that the right to privacy "*implies in principle that individuals*

[175] Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 ,entry into force 23 March 1976. Ratified by South Africa ratified on 10 December 1998.

[176] Article 17 reads:

> "*1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
>
> *2. Everyone has the right to the protection of the law against such interference or attacks.*"

have the right to share information and ideas with one another without interference by the State, secure in the knowledge that their communication will reach and be read by the intended recipients alone."[177]

185. Accordingly, "*[m]easures that interfere with this right must by authorized by domestic law that is accessible and precise and that conforms with the requirements of the Covenant. They must also pursue a legitimate aim and meet the tests of necessity and proportionality.*"[178] While the Special Rapporteur recognised the importance of preventing terrorism, he still warned that unregulated, indiscriminate bulk surveillance regimes violate the right to privacy;

> "*the technical reach of the programmes currently in operation is so wide that they could be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world. Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17.*"[179]

186. The United Nations High Commissioner for Human Rights noted that even

> "*[w]here there is a legitimate aim and appropriate safeguards … in place, … the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a*

[177] Submitted to the UN General Assembly on 23 September 2014 (A/69/397) at 58-9.

[178] Ibid.

[179] Ibid.

> *haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate*."[180]

187. Similarly, in the UN High Commissioner for Human Rights' 2018 Report, the Commissioner wrote:

> "*Many States continue to engage in secret mass surveillance and communications interception, collecting, storing and analysing the data of all users relating to a broad range of means of communication (for example, emails, telephone and video calls, text messages and websites visited). While some States claim that such indiscriminate mass surveillance is necessary to protect national security, this practice is "not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures*".[181]

188. The UNHCR's concern for the "*haystack*" is vital. Obviously bulk surveillance will turn up information that is useful for fighting crime. So too would allowing warrantless searches of people's homes. The Constitution prohibits those actions because fighting crime cannot justify any and all limitations of the right to privacy. And bulk surveillance permits innumerable violations of the haystack's privacy to find a single needle.

European Law

189. European law sets certain basic requirements for a surveillance measure to be lawful.

---

[180] Report of the Office of the United Nations High Commissioner for Human Rights submitted to the UN Human Rights Council on 30 June 2014 (A/HRC/27/37) at 25.

[181] *Right to Privacy in the Digital Age 2018* (n 18) at para 17.

190. A potentially valuable power in combating serious crime or terrorism can still be arbitrary, disproportionate and incompatible with the rule of law. In *S and Marper v United Kingdom* the UK government submitted that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was of "*inestimable value*" and produced "*enormous*" benefits in the fight against crime and terrorism.[182] The Grand Chamber nonetheless held that the retention was a "*disproportionate interference*" with those individuals' private lives.[183]

191. Similarly, in *MK v France*, the Court rejected the justification given for the French national fingerprint database by the first instance court, that "*retaining the fingerprints was in the interests of the investigating authorities, as it provided them with a database comprising as full a set of references as possible*."[184] Rather, it warned that the logic of the French government's arguments "*would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant*".[185]

192. In *Liberty and Others v United Kingdom*,[186] the ECHR held that the British bulk surveillance system was inconsistent with the Charter. It held that the surveillance must be "*in accordance with the law*" which requires both that the surveillance has a "basis in domestic law", and that it meets a certain quality of law "*requiring that it should be compatible with the rule of law and accessible*

[182] (2009) 48 EHRR 50 at para 92.

[183] Ibid at para 135.

[184] [2013] ECHR 341 at para 13.

[185] Ibid at para 37.

[186] [2008] ECHR 568.

to the person concerned, who must, moreover, be able to foresee its consequences for him".[187] It held that the same requirement of foreseeability used for individual surveillance applies.[188]

193. There are two recent, not final judgments, where the ECHR has accepted that, with appropriate safeguards, bulk surveillance programs can fall within the "*margin of appreciation*" the Court affords to member countries to protect their national security[189] – but only if it is properly authorised and complies with minimum safeguards.

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

195. PI and the Legal Resources Centre are parties to the *Big Brother Watch* case which is currently before the Grand Chamber of the European Court on Human Rights. A hearing on the case will be heard on 10 July 2019.

196. In any event, the European Court case relies on the concept of "margin of appreciation" that is not applicable to the domestic evaluation of a constitutional violation.

197. Lastly, there is no doubt at all that the current system which has no safeguards at all would fall afoul even of the minimum safeguards for communications surveillance consistently adopted by the European Court on Human Rights.[190]

---

[187] Ibid at para 59.

[188] Ibid at para 63.

[189] See, most recently, *Big Brother Watch* (n 124) at para 314; and *Centrum för Rättvisa v Sweden* [2018] ECHR 520.

[190] See, for example, *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

This Court should have no hesitancy in finding that system to be unconstitutional and leave the question of whether bulk surveillance can ever be justified to be decided later.

DECIDING THE CASE

198. Given the nature of the Applicants' challenge, how should this Court decide this case? R2K and PI agree with the Applicants that the appropriate course is to declare that the current practice of unauthorised, unregulated bulk surveillance is unlawful because it is not authorised. However, in reaching that conclusion, R2K and PI submit this Court should also make the following findings.

199. First, the reason the NSIA does not authorise the current practice is not only – as the Applicants note – because there is no accessible, clear and precise law that authorise it and regulate it. It cannot permit unregulated bulk surveillance because if it did, it would be unconstitutional.

200. The NSIA, like all statutes, must be interpreted in terms of s 39(2) to promote the spirit, purport and objects of the Bill of Rights.[191] Interpreting the NSIA to authorise the current practice of unregulated bulk surveillance would be an interpretation that permits massive, systemic violation of the right to privacy. That interpretation is not required by the text of the NSIA, particularly when it is read in light of the limitations in RICA.

201. This Court should make it clear that unregulated bulk surveillance would be an unjustifiable limitation of the right to privacy, even if it were authorised.

---

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

202. Second, this Court should leave open the question of whether regulated bulk surveillance can be constitutionally justifiable. This is a matter on which there is debate internationally and, as noted in this submission human rights experts and courts like the CJEU have ruled mass surveillance to be inherently indiscriminate.

203. As the Constitutional Court has held, "*Our task as judges is not to pick and choose between the rights and wrongs, advantages and disadvantages, of different constituency models. Our responsibility is much narrower. It is to determine whether the model Parliament has in fact chosen passes scrutiny under the Bill of Rights.*"[192] This Court should declare that the current system of unauthorised and unregulated bulk surveillance is unconstitutional and unlawful.

[192] *Association of Mineworkers and Construction Union and Others v Chamber of Mines of South Africa and Others* [2017] ZACC 3; 2017 (3) SA 242 (CC); 2017 (6) BCLR 700 (CC) at para 51.

VII CONCLUSION

204. The type of surveillance authorised by RICA and unlawfully practiced by the state is inconsistent with international law and foreign best practice. There must be notification when it will no longer affect the investigation. There must be a truly independent judge. Metadata cannot be retained for everyone all the time. And the practice of bulk surveillance of our internet communications is unlawful and unconstitutional.

205. The Amici support the order sought by the Applicants.

_____

MICHAEL BISHOP

PATRICK WAINWRIGHT (PUPIL)

Counsel for the Amici

Legal Resources Centre

Cape Town

4 April 2018