IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

Case No: CCT 278/19

Case No: CCT 279/19

In the matter between:

AMABHUNGANE CENTRE FOR INVESTIGATIVE JOURNALISM NPC	First Applicant
SOLE, STEPHEN PATRICK	Second Applicant
and	
MINISTER OF JUSTICE AND CORRECTIONAL SERVICES	First Respondent
MINISTER OF STATE SECURITY	Second Respondent
MINISTER OF COMMUNICATIONS	Third Respondent
MINISTER OF DEFENCE AND MILITARY VETERANS	Fourth Respondent
MINISTER OF POLICE	Fifth Respondent
THE OFFICE OF INSPECTOR-GENERAL OF INTELLIGENCE	Sixth Respondent
THE OFFICE FOR INTERCEPTION CENTRES	Seventh Respondent
THE NATIONAL COMMUNICATIONS CENTRE	Eighth Respondent
THE JOINT STANDING COMMITTEE ON INTELLIGENCE	Ninth Respondent
THE STATE SECURITY AGENCY	Tenth Respondent
and	
MEDIA MONITORING AFRICA TRUST	First Amicus Curiae
RIGHT2KNOW CAMPAIGN	Second Amicus Curiae

PRIVACY INTERNATIONAL Third Amicus Curiae

FILING SHEET

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

DATE FILED: 12 FEBRUARY 2020

DATE ON THE ROLL: 25 FEBRUARY 2020

DATED AT **JOHANNESBURG** ON THIS THE **12TH** DAY OF **FEBRUARY** 2020.

p.p.

LEGAL RESOURCES CENTRE
Attorneys for the Applicants
15th Floor, Bram Fischer Towers
20 Albert Street
Marshalltown
JOHANNESBURG
Tel: 011 836 9831
E-mail: david@lrc.org.za/
refilwe@lrc.org.za
Ref: D/Mtshali

TO: **THE REGISTRAR OF THE CONSTITUTIONAL COURT, BRAAMFORNTEIN**

AND TO: **WEBBER WENTZEL**
First and Second Applicants' Attorneys
90 Rivonia Road, Sandton
JOHANNESBURG
Tel: (011) 530 5232

Fax: (011) 530 6232

Email: Dario.milo@webberwentzel.com

Ref: Dario Milo / Makhotso Lengane / 3000547

AND TO: **THE STATE ATTORNEY, PRETORIA**

Fifth Respondent's Attorneys

SALU Building

216 Thabo Sehume Street

Private Bag X 91

PRETORIA

Ref: 2937/2017/Z52/MC

Tel: (012) 309 – 1630

Fax: 086 640 1943

Dx: 298 PRETORIA

Email: memakhubela@justice.gov.za / conkuna@justice.gov.za

Enq: M Makhubela

c/o: **THE STATE ATTORNEY, JOHANNESBURG**

12th Floor, North State Building

95 Albertina Sisulu Street (Cnr. Kruis Street)

JOHANNESBURG

Tel: (011) 330 7663

Fax: (011) 333 1683 / 086 507 2005

Email: HMaponya@justice.gov.za

Enq: H Maponya

AND TO: **THE STATE ATTORNEY, PRETORIA**

Third and Fourth Respondents' Attorneys

SALU Building

216 Thabo Sehume Street

Private Bag X91

PRETORIA

Ref: 2937/2017/Z52/MC

Tel: (012) 309 – 1630

Fax: 0860 640 1943

Dx: 298 PRETORIA

Email: memakhubela@justice.gov.za / conkuna@justice.gov.za

Enq: M Makhubela

AND TO: **THE STATE ATTORNEY, PRETORIA**

Second, Seventh, Eighth and Tenth Respondents' Attorneys

SALU Building

216 Thabo Sehume Street

Private Bag X91

PRETORIA

Tel: (012) 309 1543

Fax: (012) 309 1649/50

Ref: 5928/2019/Z65/MM

Email: MMotsau@justice.gov.za

AND TO: **POWER SINGH INCORPORATED**

First Amicus Attorneys

First Floor, 20 Baker Street

Rosebank

JOHANNESBURG

Tel: (011) 268 6811

Fax: 086 614 5818

Email: avani@powersingh.africa/ michael@powersingh.africa/

tina@powersingh.africa

Ref: PSIMM-202002

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

CCT 278/19

In the application of:

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

THIRD AMICUS CURIAE'S PRACTICE NOTE

NATURE OF PROCEEDINGS

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

2. There is also a contested appeal concerning the meaning of the National Strategic Intelligence Act 39 of 1994 (**NSIA**).

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

THE ISSUES THAT WILL BE ARGUED

4. Privacy International (**PI**) will make submissions concerning:

   4.1. Safeguards for the storage of metadata by phone operators (High Court Order 5); and

   4.2. The legality of bulk surveillance (High Court Order 6).

ESTIMATED DURATION OF ARGUMENT

5. PI estimates that it will require 15 minutes for oral argument.

NECESSARY PORTIONS OF THE RECORD

6. PI defers to the parties on which portions of the Record are necessary.

SUMMARY OF APPLICANTS' ARGUMENT

Safeguards for Metadata

7. PI will advance four arguments.

8. First, RICA requires the mandatory, blanket retention of metadata.

9. Second, this is extremely invasive of the right to privacy.

10. Third, it is inconsistent with South Africa's international obligations and comparative practice.

11. Fourth, the High Court's order is mistakenly limited to require safeguards for data intercepted by the state. It should be expanded to include metadata held by phone operators and internet service providers.

Bulk Surveillance

12. PI will advance four arguments to support confirmation of the High Court's order.

13. First, bulk surveillance entails the interception of virtually all internet traffic.

14. Second, this is a massive and systemic violation of the rights to privacy and freedom of expression.

15. Third, bulk surveillance is contrary to international law.

16. Fourth, the NSIA must be interpreted to avoid this violation. It must be interpreted

not to permit unregulated bulk surveillance. This Court should leave open whether bulk surveillance, even if regulated, can be constitutional.

AUTHORITIES ON WHICH SPECIAL RELIANCE WILL BE PLACED

1. *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).
2. *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights* A/HRC/39/29 (2018).
3. *Digital Rights Ireland (Judgment of the Court)* [2014] EUECJ C-293/12.
4. *Tele2 Sverige/Watson* [2016] EUECJ C-203/15.
5. *Carpenter v United States* 585 US ____ (2018); 138 SCt 2206.

MICHAEL BISHOP

PATRICK WAINWRIGHT

Counsel for Privacy International

Chambers, Cape Town

12 February 2020

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

CCT 278/19

In the application of:

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

THIRD AMICUS CURIAE'S WRITTEN SUBMISSIONS

TABLE OF CONTENTS

I INTRODUCTION

1. We live in a digital age. This has brought with it immense advantages and opportunities. But it has also enabled governments to conduct unprecedented and near total surveillance of its citizens. This application raises two ways in which the state spies on us all.

2. First, Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002 (**RICA**) requires all phone companies and internet service providers (**ISPs**) to store the metadata about all our communications for up to five years. Any prosecutor can access that information about any person relevant to the investigation of any crime. When stored over a period of time, and analysed by sophisticated software, this metadata reveals deep, personal details about a person. It can tell the state where we are at every minute of the day, who we talk to. It can reveal personal associations, secrets and beliefs.

3. This case raises the mandatory, blanket retention of metadata only tangentially. Part of the relief sought concerned the conditions under which phone operators keep and use this metadata. The High Court, erroneously, did not grant an order declaring RICA invalid for not providing adequate safeguards for the storage and use of this metadata. Privacy International (**PI**) argues that the High Court's Fifth Order should be amended to do so.

4. Second, RICA creates detailed requirements to actually intercept the content of a communication. But the National Communications Centre (**NCC**) has for years fragrantly violated that requirement. It has been conducting bulk surveillance of foreign signals. Again, the jargon fails to convey the sinister nature of the government's conduct.

5. Bulk surveillance means that the government is intercepting and analysing virtually all our internet traffic. Our emails, our Whatsapps, our calendars, our documents, our social media posts are all intercepted by the government. The government is doing this without any express

authorisation, and without any specific regulation.

6. It is easy to sound hyperbolic about the threat of this type of surveillance. But the impacts of bulk surveillance on people and society are real and alarming. It "*inculcates norms of pervasive, continual observation and tracking … [that] shape both behaviour and a sense of identity.*"[1] Without the space free of the government's eye, our sense of what it means to be human shifts. It affects how we interact with others too. This type of constant surveillance "*weakens the foundations of civil society*".[2] It destroys the private spaces that are necessary to create and strengthen the social fabric. If much of our lives are lived online, and the government sees everything we do online, it cannot but affect how we think, and how we act.

7. PI supports the High Court's Sixth Order that the current practice of unauthorised, unregulated bulk surveillance is unlawful. It asks that this Court declare it is a violation of the right to privacy.

8. These written submissions first address **mandatory blanket retention of metadata**, and then **bulk surveillance**. PI also endorses the written submissions of the Right2Know Campaign on the issue of post-surveillance notification, and the independence of the designated judge.

II MANDATORY BLANKET RETENTION OF METADATA

9. RICA mandates all phone operators and internet service providers to store all the metadata generated by their users for up to five years. It allows any prosecutor to access the metadata

---

[1] J Cohen 'Surveillance versus Privacy: Effects and Implications' in D Gray & S Henderson (eds) *The Cambridge Handbook of Surveillance Law* (2017) 455 at 460.

[2] Ibid at 465.

of any person to investigate any offence. This happens hundreds of time every day. This is mandatory blanket retention of metadata. Accumulated over time, metadata reveals a huge amount about a person. Their location, their friends, their habits, their associations, their beliefs. International bodies and courts have recognised the intense impact it has on our privacy and have declared it impermissible. PI believes it is unconstitutional.

10. This application does not directly concern the constitutionality of mandatory blanket retention of metadata. It concerns only whether RICA provides adequate safeguards for the retention of that metadata. But in order to make that assessment, PI submits the Court must understand just how corrosive of privacy this practice is. Safeguards for use and retention are the very minimum that can be required. Accordingly, this Part:

10.1. Explains how metadata is treated under **RICA**;

10.2. Demonstrates that it is an unjustifiable **limitation of privacy**; and

10.3. Contends for an amendment to the **High Court's order**.

METADATA UNDER RICA

11. PI has fully set out how RICA demands the retention of metadata in its affidavit.[3] All phone companies must maintain a record of communication-related information of every single communication by their users.[4] "*communication related information*" includes all information about a communication except its actual content.[5] It includes the who, when, how and where of the communication. That information must be stored in accordance with a directive issued by the

[3] R2K and PI FA at paras 102 117.

[4] RICA s 30(1)(b), read with the *Directives in Respect of Different Categories of Telecommunications Service Providers Made in Terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 Of 2002)*, published as GN 1325 of 2005.

[5] RICA s 1, read with the definition of "*indirect communication*". The same obligation will apply to ISPs when the Minister of Communications publishes a directive.

Minister, for up to five years.[6] The information can be accessed through a direction in terms of s 19 of RICA. Section 19 has several safeguards.[7]

12. However, this metadata can also be accessed outside of RICA, under s 205 of the Criminal Procedure Act 51 of 1977 (**CPA**).[8] Section 205 provides for a person to be subpoenaed to provide documents or answer questions before a magistrate with regard to any offence.[9] It is a routine tool of all criminal investigations. It is intended to be used to obtain archived communications related information.

13. Yet s 205 contains none of the safeguards in s 19 of RICA. A request under s 205 can be made to investigate any offence. It is not necessary to know the identity of the alleged offender. There is no requirement of "*reasonable grounds*", or that the information is "*necessary*" in order to investigate an offence. The applications can be made by a far wider swathe of prosecutors. Section 205 does not require the same detailed information to be placed before the judge or magistrate.

14. In practice, s 205 warrants are extremely easy to obtain. Indeed, the vast majority of metadata

---

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

[7] First, 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*". Second, the application can be made only by specified senior officials within the definition of "*applicant*" in RICA. Third, the application must include the detailed information set out in s 17(2). Fourth, the application is not made to the designated judge, but to "*a judge of a High Court, a regional court magistrate or a magistrate*". RICA s 19(1). However, if a judicial officer issues the direction, she must provide a copy to a designated judge,[7] who must ensure it is kept for at least five years. RICA ss 19(7) and (8).

[8] RICA s 15.

[9] Section 205 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)

The reference to RICA was added in 2002, with effect from 2005. Act 70 of 2002 s 59.

requests are not made in terms of s 19, but in terms of s 205.[10] The applications for subpoenas are generally determined on paper, in chambers by any magistrate or judge.[11]

15. 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.

LIMITATION OF PRIVACY AND EXPRESSION

16. 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, who we talk to. If a person has a cellphone – particularly a smart phone – metadata will literally track their movements minute by minute. This information is private, and its collection is invasive of the right to privacy.

17. In this section, we first show with reference to international and comparative law, that mandatory blanket retention of metadata under RICA violates the rights to privacy, and free expression. We then explain why the practice unjustifiably limit the right in South Africa.

International Law

[10] R2K and PI FA at para 116.

[11] R2K and PI FA at para 117. The way in which s 205 is used is apparent from the matter of *S v Miller and Others* 2016 (1) SACR 251 (WCC). 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 Notebook'*" which was "*used to collate data and to provide a visual link where similarities are found*". That analysis "*will show when particular cellphone numbers have been in contact with each other*". 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.*" Ibid at para 17.

18. The United Nations Office of the High Commissioner for Human Rights (**OHCHR**), the UN Human Rights Council (**HRC**), and the Special Rapporteur of the Right to Freedom of Opinion and Expression (**Special Rapporteur**) have determined that mandatory, blanket retention of metadata is inconsistent with international law.

19. In two reports titled *The Right to Privacy in the Digital Age* – issued in 2014[12] and 2018[13] – **the OHCHR** has concluded that mandatory blanket retention of metadata "*'just in case' it is needed for government purposes … appears neither necessary nor proportionate.*"[14] The retention of 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.*"[15] The 2018 Report concluded that these laws "*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.*"[16]

20. In its 2016 periodic report on South Africa,[17] the **HRC** stated that it was "*concerned about the wide scope of the data retention regime under [RICA].*"[18] It recommended that South Africa should "*consider revoking or limiting the requirement for mandatory retention of data by third parties.*"[19] That concern was repeated in several other conclusions assessing states' compliance with the ICCPR.[20] In the United States, for example, it called on the US to "*[r]efrain from imposing*

---

[12] *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).

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

[14] *Right to Privacy in the Digital Age 2014* (n 12) at para 19

[15] Ibid.

[16] *Right to Privacy in the Digital Age 2018* (n 13) at para 18.

[17] *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).

[18] Ibid at para 42.

[19] Ibid at para 43.

[20] 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

mandatory retention of data by third parties".[21]

21. The Special Rapporteur has also recognised how mandatory data retention threatens free expression by limiting the ability to remain anonymous.[22] The practice "*has inevitably resulted in the State having everyone's digital footprint.*"[23]

European Law

22. In *Digital Rights Ireland Ltd v Ireland*[24] and *Tele2 Sverige/Watson*,[25] the Court of Justice for the European Union (**CJEU**) held that mandatory retention of metadata is incompatible with arts 7[26] and 8[27] of the Charter of Fundamental Rights of the European Union. Metadata – when stored in bulk over time – can "*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.*"[28] Collecting this data will make people feel "*that their private lives are the subject of constant surveillance.*"[29] When collected in bulk, metadata "*is no less sensitive,*

Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015).

[21] 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).

[22] 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.

[23] Ibid.

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

[25] *Tele2 Sverige/Watson* [2016] EUECJ C-203/15.

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

[27] 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.*"

[28] *Digital Rights Ireland* (n 24) at para 27. See also *Tele2 Sverige/Watson* (n 25) at para 99.

[29] *Digital Rights Ireland* (n 24) at para 37.

having regard to the right to privacy, than the actual content of communications."[30] This clearly limited privacy rights, but also limited the right to free expression because it would affect what means of communication people used, and how they used them.[31]

23. The Court recognised the important purpose of targeting serious crime, and accepted that mandatory blanket retention of metadata served that goal.[32] But it the limitation was not justified for two primary reasons. First, there were inadequate safeguards.[33] But second, the retention of data occurred "*without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.*"[34] 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.*"[35] It therefore constituted "*an interference with the fundamental rights of practically the entire European population.*"[36] Only targeted retention, for fighting serious crime, with limited retention of limited data is permissible in European law.[37] None of those limits are present in RICA.

24. The European Court of Human Rights (**ECtHR**) too has recognised that bulk retention of metadata is "*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*

---

[30] *Tele2/Watson* (n 25) at para 99.

[31] *Digital Rights Ireland* (n 24) at para 28.

[32] Ibid at paras 41-44.

[33] Ibid at para 66.

[34] Ibid at para 57.

[35] Ibid at para 58.

[36] Ibid. The issue has arisen again before the CJEU this year. *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (Case C-623/17); and the joined cases *La Quadrature du Net, French Data Network, and others v Premier ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées* (C-511/18 and C-512/18). R2K and PI FA at para 27. While judgment is outstanding, the Advocate General has endorsed the reasoning *Digital Rights Ireland* and *Tele2 Sverige*: mandatory retention of metadata is inconsistent with European rights. The Advocate-General's opinions in the four cases are available at: http://curia.europa.eu/juris/documents.jsf?num=C-623/17; http://curia.europa.eu/juris/documents.jsf?num=C-511/18; http://curia.europa.eu/juris/documents.jsf?num=C-512/18; http://curia.europa.eu/juris/documents.jsf?num=C-520/18.

[37] *Tele2/Watson* (n 25) at para 108 (emphasis added).

interacted with".[38] The failure to apply the same safeguards to metadata that were applied to the content of communications was one of the reasons the ECtHR held the UK's bulk surveillance regime was inconsistent with the Charter.[39]

The United States

25. In *Carpenter v United States*[40] the US Supreme Court discussed the effect of a provision like s 205 which allowed the state to access stored metadata with relative ease.[41] Roberts CJ described the effect of the location data collected from phone companies as "*near perfect surveillance, as if it had attached an ankle monitor to the phone's user.*"[42] It grants the government "*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.'*"[43] Because phone companies stored the data for five years, it allowed the government to "*travel back in time to retrace a person's whereabouts.*"[44]

26. Roberts CJ summarised the impact as follows: "*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 . . . . Only the few without cell phones could escape this tireless and absolute*

---

[38] *Big Brother Watch and Others v The United Kingdom* [2018] ECHR 722 at para 356.

[39] Ibid at para 357.

[40] 585 US ____ (2018); 138 SCt 2206. See also *Riley v California* 573 US __ (2014); 134 SCt 2473 (*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. Chief Justice Roberts set out why the data cell phones store, including the metadata, demands privacy protection. 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.*" Ibid at 17. 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.'*" Ibid at 19-20.

[41] 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.

[42] *Carpenter* (n 40) at 13 (emphasis added).

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

[44] Ibid at 13.

surveillance."[45] The Supreme Court held that permitting access to this data without a warrant violated the Fourth Amendment to the US Constitution.

Unjustifiable

27. Mandating the retention, and permitting the easy access to, metadata is serious and systemic violation of the right privacy. It is not – as the state seeks to portray it – technical or impersonal information. It is information that concerns an "*individual's intimate personal sphere of life*".[46] Mandatory blanket retention of metadata is a serious limitation of the right to privacy.

28. 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 want to be able to use all means available to identify and prosecute the wrongdoers. But there are three reasons why this can never justify the scheme created by RICA.

29. 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 this Court in *Hyundai.*[47] Under RICA, everybody's metadata is retained, regardless of whether they are suspected of having committed a crime or not.

30. Second, the same purpose could be achieved through a less restrictive, more targeted regime

---

[45] Ibid at 13-14. *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. One: 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. Two: 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.

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

[47] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* [2000] ZACC 12; 2001 (1) SA 545 (CC); 2000 (10) BCLR 1079 (CC) at para 52. See also *Tele2/Watson* (n 25) at para 103.

for the retention of metadata. 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.

31. Third, 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 normalises the use of invasive metadata for everyday crime-fighting.

THE ORDER IS TOO NARROW

32. Before the High Court, the Applicants challenged two related elements that the High Court dealt with together:[48] (a) the absence of safeguards for the storage of interception data by the state; and (b) he length of time *and the absence of safeguards* for the storage of communications-related information by private, telephone companies.

33. The first challenge was directed at ss 35 and 37 of RICA which deal with the storage of interception data at "*interception centres*". The second challenge was to s 30(2)(a)(iii) of RICA which provides for the Minister of Communications to issue a directive on the retention of communication-related information.[49] The relief sought with regard to s 30(2)(a)(iii) was

---

[48] The Applicants' founding papers made it clear that they were concerned with both the period for which the communication-related information would be stored, and the conditions under which it would be stored. FA at para 89.2: Record Vol 1, p 48.

[49] RICA s 30(2)(a)(iii) reads:

> *"The Cabinet member responsible for communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and the telecommunication service provider or category of telecommunication service providers concerned, must, on the date of the issuing of a telecommunication service licence under the Electronic Communications Act, to such a telecommunication service provider or category of telecommunication service providers-*
>
> *(a) issue a directive in respect of that telecommunication service provider or category of telecommunication service providers, determining the- …*
>
> *(ii) type of communication-related information which must be stored in terms of subsection (1) (b) and the period for which ~~such information must be stored, which period may, subject to subsection (3), not be less than three years~~ and not more than five years from the date of the transmission of the indirect communication to which that communication-related information relate".*

simply that it is "*inconsistent with the Constitution and accordingly invalid*"[50]

34. The Respondents understood that the challenge to s 30(2)(a)(iii) was directed at the absence of safeguards for the storage of communications-related information by telecommunications service providers.[51] The High Court, too, appreciated that the attack on the absence of safeguards applied to both the holding of interception data by the state, and the use of communication-related information by phone operators.[52] Correctly so. The safeguards[53] are all equally applicable to protecting the vital privacy interests in metadata as they are to the content of communication.

35. The problem is this: The High Court's order is limited to the storage of interception data by the state. It does not extend to the storage of communication-related information by telecommunications service providers.[54] But both were attacked by the Applicants. And there is no difference – from the perspective of the rights to privacy and expression – between the retention of intercepted communications data by the state, and the retention of communications-related information by private companies.

36. The Applicants have not appealed against this part of the High Court's order. However, PI submits that given the manner in which it was pleaded, it is within this Court's power to grant a "*just and equitable*" order that reflects the full extent of the constitutional violation.[55]

37. Accordingly, PI submits that Order 4 should be amended as follows:

---

[50] Notice of Motion prayer 1.3: Record Vol 1, p 2.

[51] Joint AA at paras 59-70: Record Vol 8, pp 775-9. See also RA at paras 49-52: Record Vol 10, p 1003.

[52] HC Judgment at para 89: Record Vol 15, pp 1498-9. The directives the High Court is referring to are the directives published in terms of section 30(2)(a) concerning the retention of communications-related information by phone operators. *Directives* (n 4).

[53] All the safeguards are set out in HC Judgment at para 98: Record Vol 15, p 1502.

[54] The order reads: "*RICA, especially sections 35 and 37, are inconsistent with the Constitution and accordingly invalid to the extent that the statute, itself, fails to prescribe proper procedures to be followed when ~~state officials~~ are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions.*" HC Order No 4: Record Vol 15, pp 1527-8.

[55] Constitution s 172(1)(b).

"*(1) RICA, especially sections 30, 35 and 37, is inconsistent with the Constitution and accordingly invalid to the extent that the statute, itself, fails to prescribe proper procedures to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions, and when a telecommunication service provider is examining, copying, sharing, sorting through, using, destroying and/or storing archived communications-related data;*

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

38. In addition, PI submits that this Court should leave open whether – even with the proper procedures in place – the mandatory, blanket retention of metadata can survive constitutional scrutiny. The issue is not currently before it, and it should not preclude a future challenge when international law suggests the practice is inherently impermissible.

III BULK SURVEILLANCE

39. The Respondents admit that the intelligence services are engaging in unregulated bulk surveillance of foreign signals. This means that the state – without any express permission from Parliament and without any limits or safeguards – is capturing all internet traffic that enters or leaves South Africa.

40. That is **almost all internet traffic** of South Africans. The vast majority of internet traffic crosses the Republic's borders. It includes the most personal information – our emails, our diaries, our documents, our video calls, our location, our browsing history. The Government has it all. For everybody with an internet connection. All the time. These words are being intercepted as I write them because this document is being simultaneously backed up on a server outside the Republic. It is a privacy violation of an almost unimaginable scale.

41. The Government's only justification is: *We will only use this information to fight crime. Trust us.* That

is no justification at all.

42. The High Court correctly upheld the Applicants' argument that the practice of bulk surveillance is unlawful because it is **unauthorised**, and **unregulated**. The Minister of State Security's appeal against that order is, for the reasons given by the Applicants, fatally defective.[56] This Court should not consider it.

43. However, if it does, this Court should uphold the High Court's order. PI advances four submissions:

43.1. Bulk surveillance is a serious violation of privacy;

43.2. It is contrary to international law;

43.3. Bulk surveillance cannot be justified; and

43.4. The NSIA must be interpreted not to permit bulk surveillance.

VIOLATION OF PRIVACY

44. The Government has provided scant detail about how its mass surveillance system operates.[57] That makes it impossible to determine the precise extent to which the right to privacy is being violated by the Government. In fact, the absence of clear information compounds the violation.

45. 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

[56] Applicants' Written Submissions at paras 121-3.

[57] See generally, R2K and PI FA at paras 143-147.

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, books a flight, makes a Skype call, downloads a document, or accesses their online diary. It follows, according to the state, that all those communications are "foreign" and are intercepted by the NCC.

46. 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*".[58] 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.*"[59] On the Government's own version, they intercept, store, and analyse *virtually all* emails and internet traffic, without a warrant, without any suspicion about the people whose communications they are intercepting, and without statutory safeguards.

47. 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 allows the government to track a person's movements.

48. This is the most personal possible information. It could include private medical information,[60] intimate communications, or sexual orientation.[61] It covers the most mundane matters, intrudes deep into "*the inner sanctum of a person, such as his/her family life, sexual preference and home environment*",[62] and sweeps up everything in between.

---

[58] State Security AA at para 132: Record Vol 8, p 802.

[59] State Security AA at para 136: Record Vol 8, pp 803-4.

[60] *NM and Others v Smith and Others* [2007] ZACC 6; 2007 (5) SA 250 (CC); 2007 (7) BCLR 751 (CC).

[61] *Le Roux and Others v Dey* [2011] ZACC 4; 2011 (3) SA 274 (CC) ; 2011 (6) BCLR 577 (CC).

[62] *Bernstein* (n 46) at para 67.

49. This surveillance is unauthorised and unregulated. No permission is sought. No legal limits are placed on how the data is captured, copied, stored, analysed, or distributed. It is impossible to hold the intelligence services to account for even the most basic requirements for possessing and using the most intimate information on all South Africans connected to the internet. We simply do not know what data are being captured, stored and analysed. And there is no mechanism to prevent abuse.

50. This type of unregulated, untargeted surveillance of all information, merely because it happens to cross South Africa's borders is an extreme limitation of the right to privacy. This conclusion is supported by comparative and international law.

INTERNATIONAL LAW

51. One of the Government's primary defence seems to be that these practices are common in other jurisdictions.[63] While mass surveillance systems exist in other countries, that does not mean they are lawful.

52. The **UN Special Rapporteur on Counter-Terrorism**[64] has concluded that measures that allow government interception of internet traffic "*must be 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.*"[65] While the Special Rapporteur recognised the importance of preventing terrorism, he warned that unregulated, indiscriminate bulk surveillance regimes are "*indiscriminately corrosive of online privacy and impinges on the very essence of the*

[63] See, for example, Joint AA at para 130: Record Vol 8, p 802.

[64] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (23 September 2014) UN Doc A/69/397 at 58-9.

[65] Ibid.

right guaranteed by [the right to privacy]".[66] They constitute "*the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world*".[67]

53. The **OHCHR** has similarly reasoned that bulk surveillance may "*be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime*". It has likened bulk surveillance to looking for a needle in a haystack – billions of communications are intercepted in order to find the few that are linked to serious crime. But that is insufficient justification: "*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.*"[68] In the 2018 Report, the OHCHR wrote that despite claims it is necessary to protect national security, "*indiscriminate mass surveillance … 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*".[69]

54. The OHCHR's concern for the "*haystack*" is vital. Obviously bulk surveillance will turn up information that is useful for fighting crime. So too would allowing random, 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. Bulk surveillance permits constant violation of the haystack's privacy in the hope of finding the needle.

55. As a general principle, the **ECtHR** does not accept that an invasive power is permissible merely because it is valuable in combating serious crime or terrorism.[70] Thus, in *Liberty and*

---

[66] Ibid.

[67] Ibid.

[68] *Right to Privacy in the Digital Age 2014* (n 12) at 25.

[69] *Right to Privacy in the Digital Age 2018* (n 13) at para 17.

[70] See *S and Marper v United Kingdom* (2009) 48 EHRR 50 (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. The Grand Chamber nonetheless held that the retention was a "*disproportionate interference*" with those individuals' private lives. Ibid at para 92); *MK v France* [2013] ECHR 341 (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.*" Ibid at para 13. Rather, it warned that the

Others v United Kingdom,[71] the ECtHR 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 to the person concerned, who must, moreover, be able to foresee its consequences for him*".[72] It held that the same requirement of foreseeability used for individual surveillance applies.[73] Applying this standard, the unregulated and unauthorised bulk surveillance conducted by the NCC would undoubtedly be unconstitutional.

56. 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[74] – but only if it is properly authorised and complies with minimum safeguards.

57. PI and the Legal Resources Centre are parties in one of those cases. Together with the other applicants, they have appealed to the Grand Chamber of the ECtHR. Judgment is outstanding. Their position is that bulk surveillance will *always* be an unjustifiable limitation of the right to privacy. Intercepting everybody's communications can never be justified, no matter how good the safeguards. It is necessarily inconsistent with the requirements of being authorised by law that is clear and precise, and with the requirements of necessity and proportionality.

---

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*". Ibid at para 37).

[71] [2008] ECHR 568.

[72] Ibid at para 59.

[73] Ibid at para 63.

[74] See, most recently, *Big Brother Watch* (n 38) at para 314; and *Centrum för Rättvisa v Sweden* [2018] ECHR 520.

58. But no matter the outcome of those cases, the current system which has no clear and precise basis in law, and no safeguards at all would, fall afoul of the standards consistently adopted by the ECtHR.[75] This Court should have no hesitancy in finding that system to be unconstitutional.

THE NSIA DOES NOT PERMIT BULK SURVEILLANCE

59. There is no express authorisation for the NCC's practice of bulk surveillance. RICA directly prohibits it. The Respondents are forced to seek solace in s 2(1)(a) of the National Strategic Intelligence Act 39 of 1994 (**NSIA**). The provision empowers the Agency "*to gather, correlate, evaluate and analyse domestic and foreign intelligence*". The High Court conducted a detailed textual analysis and concluded that s 2(1)(a) did not permit bulk surveillance.[76] It permits the traditional methods of intelligence gathering, not a massive surveillance programme of the entire populace. PI supports that textual analysis.

60. But interpretation is not only about the text. The NSIA must, in terms of s 39(2), be interpreted to promote the spirit, purport and objects of the Bill of Rights. Courts "*must prefer interpretations of legislation that fall within constitutional bounds over those that do not, provided that such an interpretation can be reasonably ascribed to the section.*"[77] Related to this requirement is the principle that laws that limit constitutional rights must be clear and precise about the extent to which they do so. Laws that fail to provide officials with the necessary guidance,[78] or citizens with knowledge of where their rights begin and end[79] are constitutionally suspect.

---

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

[76] High Court Judgment at paras 148-162: Record Vol 15, pp 1518-23.

[77] See *Hyundai* (n 47).

[78] *Dawood and Another v Minister of Home Affairs and Others* [2000] ZACC 8; 2000 (3) SA 936 (CC); 2000 (8) BCLR 837 (CC).

[79] *Moyo and Another v Minister of Police and Others* [2019] ZACC 40; 2020 (1) BCLR 91 (CC).

61. Interpreting the NSIA to authorise the current practice of unregulated bulk surveillance would be inconsistent with these basic principles. It would authorise a massive, systemic violation of the rights to privacy and free expression. It would be manifestly unconstitutional. That is the opposite of what s 39(2) demands.

62. But the problem with the current practice of unregulated bulk surveillance is not only that it does not have a statutory foundation. The more fundamental problem is that it an unjustifiable limitation of the right to privacy. PI submits this Court should hold that unregulated bulk surveillance is both unlawful and unconstitutional.

63. Lastly, this Court should leave open the question of whether regulated bulk surveillance can be constitutionally justifiable. Regulated bulk surveillance is practiced internationally, but it is also contrary to international human rights law. Courts are still determining if – and if so under what conditions – bulk surveillance can ever be permissible in democratic societies.

64. If Parliament chooses to enact a law that expressly authorises the practice, this Court can then determine whether it is constitutional and, if so, what safeguards are required.

MICHAEL BISHOP

PATRICK WAINWRIGHT

Counsel for Privacy International

Chambers, Cape Town

12 February 2020

IN THE CONSTITUTIONAL COURT OF SOUTH AFRICA

CCT 278/19

In the application of:

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

THIRD AMICUS CURIAE'S TABLE OF AUTHORITIES

Legislation and Regulations

1. Criminal Procedure Act 51 of 1977.

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

3. National Strategic Intelligence Act 39 of 1994.

4. *Directives in Respect of Different Categories of Telecommunications Service Providers Made in Terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 Of 2002)*, published as GN 1325 of 2005.

Cases

1. *Bernstein and others v Bester and others* NNO 1996 (2) SA 751 (CC).

2. *Dawood and Another v Minister of Home Affairs and Others* [2000] ZACC 8; 2000 (3) SA 936 (CC); 2000 (8) BCLR 837 (CC).

3. *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).

4. *Le Roux and Others v Dey* [2011] ZACC 4; 2011 (3) SA 274 (CC); 2011 (6) BCLR 577 (CC).

5. *Moyo and Another v Minister of Police and Others* [2019] ZACC 40; 2020 (1) BCLR 91 (CC).

6. *NM and Others v Smith and Others* [2007] ZACC 6; 2007 (5) SA 250 (CC); 2007 (7) BCLR 751 (CC).

7. *S v Miller and Others* 2016 (1) SACR 251 (WCC).

International Treaties and Reports

1. *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).

2. *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).

3. *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

4. *Human Rights Committee Concluding observations on the fourth periodic report of the United States of America* CCPR/C/USA/CO/4 (2014).

5. International Covenant of Civil and Political Rights

6. *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.

7. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (23 September 2014) UN Doc A/69/397.

8. Universal Declaration of Human Rights

Foreign and International Cases

1. *Big Brother Watch and Others v The United Kingdom* [2018] ECHR 722 at para 356.

2. *Carpenter v United States* 585 US ____ (2018); 138 SCt 2206.

3. *Centrum för Rättvisa v Sweden* [2018] ECHR 520.

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

5. *Liberty and Others v United Kingdom* [2008] ECHR 568.

6. *MK v France* [2013] ECHR 341

7. *Riley v California* 573 US __ (2014); 134 SCt 2473

8. *S and Marper v United Kingdom* (2009) 48 EHRR 50

9. *Tele2 Sverige/Watson* [2016] EUECJ C-203/15.

10. *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

Academic Authority

1. J Cohen 'Surveillance versus Privacy: Effects and Implications' in D Gray & S Henderson (eds) *The Cambridge Handbook of Surveillance Law* (2017) 455 at 460.