Name: Catherine Kruyer
Student number: KRYCAT001
Qualification: LLM Public International Law
Title: 'Reforms to the laws on the surveillance of private communications
Supervisor: Cathleen Powell
Word count: 22 191
No. of pages: 88

DECLARATIONS:

1. **I am presenting this dissertation in partial fulfilment of the requirements for my degree.**
2. **I know the meaning of plagiarism and declare that all of the work in the dissertation, save for that which is properly acknowledged, is my own.**
3. **I hereby grant the University of Cape Town free licence to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever of the above dissertation.**

Signature	Signed by candidate	***Date:***	12 February 2024

TABLE OF CONTENTS

INTRODUCTION

The right to privacy is central to our constitutional order, founded on human dignity. The ability of the State to invade the privacy of our communications threatens the personal space within which we live "*our daily lives*".[1] As the Constitutional Court expressed in its landmark judgment on communications surveillance in *AmaBhungane*[2]: "*Today technology enables law enforcement agencies to . . . invade the 'intimate personal sphere' of people's lives, but also to maintain and cement its presence there, continuously gathering, retaining and – where deemed necessary – using information*."[3]

The Constitutional Court in *AmaBhungane* evaluated the law regulating communications surveillance – the Regulation of Interception of Communications and Provision of Communications-Related Information Act[4] ("RICA") – and declared RICA inconsistent with the Constitution in five respects. The judgment and order of the Constitutional Court necessitates extensive and wide-ranging amendments to RICA to cure the defects identified by the Court. The Constitutional Court suspended the declarations of invalidity to give Parliament an opportunity to cure the defects.

Moreover, the key principles recognised in the judgment of the Constitutional Court necessitate a more comprehensive review of RICA, which centres the right to privacy. The

---

[1] *NM v Smith* [2007] ZACC 6; 2007 (5) SA 250 (CC); 2007 (7) BCLR 751 (CC) at para 131 (dissenting judgment of O'Regan J).

[2] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* [2021] ZACC 3;2021 (3) SA 246 (CC); 2021 (4) BCLR 349 (CC) ("*Amabhungane*").

[3] Ibid at para 1.

[4] Act 70 of 2002.

Constitutional Court recognised that State surveillance of our personal communications is an invasive violation of the right to privacy.[5] It emphasized the importance of RICA containing adequate safeguards to ensure that there are no unnecessary invasions of the right to privacy.

The Legislature has taken steps to remedy the defects in RICA identified in the Constitutional Court's judgment and order. It has passed the Regulation of Interception of Communications and Provision of Communication-related Information Amendment Bill, 28B of 2023 ("**the Bill**"). The Bill has not yet been signed into law by the President. However, the Bill falls short of what is required to remedy RICA in several key respects and also makes no reform efforts beyond the Constitutional Court's order.

This thesis aims to consider the reforms required to cure the defects in RICA identified by the Constitutional Court in *Amabhungane*, as well as further reforms to existing laws required to ensure a human rights centric approach to communications surveillance in South Africa.

It is critical to understand the all-important context within which reforms to the legislative scheme must be considered. Surveillance of private communications constitutes a severe limitation of the right to privacy – and the interconnected rights of freedom of expression and dignity. In the context of a rights limitation, the rights of the subjects of surveillance must be balanced against the indisputably important aims of surveillance, being the investigation of serious crimes, public safety and national security. This requires that adequate safeguards be put in place to ensure that the rights of the subjects of surveillance are not limited more than is necessary and proportionate to the aims sought to be achieved by state surveillance.

[5] Ibid at para 24.

Chapter 1 sets out the South African legal landscape, starting with an analysis of the rights in the Bill of Rights that are implicated by state surveillance of personal communications. It turns then to look at the relevant legislative scheme governing surveillance, and provides a detailed explanation of the provisions of RICA.

Chapter 2 considers state surveillance of personal communications through the lens of international law, starting with a discussion of the international instruments enshrining the right to privacy and then unpacking the way in which this right has been interpreted in secondary sources.

Chapter 3 provides an account of the Constitutional Court's judgment in *Amabhungane* and provides an explanation of the constitutional defects in RICA identified therein.

This discussion is developed in Chapter 4, wherein recommendations are made to cure the defects in RICA. The Bill is critiqued and better reform measures are recommended through an amendment Bill appended as Appendix I.

Chapter 4 moves beyond the defects identified in *AmaBhungane* and considers the possibilities for further reforms in RICA, with a particular focus on improving transparency and accountability mechanisms in the Act.

CHAPTER ONE: THE SOUTH AFRICAN LEGAL LANDSCAPE

The Constitution

The Bill of Rights

The Constitution of South Africa guarantees everyone the right to privacy.[6] Section 14(d) of the Constitution provides that the right of every person to privacy includes the right not to have "*the privacy of their communications infringed*". The right to privacy has taken on special importance in South Africa given the country's history, which was characterised by "*systematised and egregious violations of personal privacy*".[7]

The right to privacy ensures that everyone is free from intrusions by the State and others in the intimate personal sphere of their lives.[8] The Constitutional Court explained that the right to privacy becomes "*more intense the closer it moves to the intimate personal sphere of the life of human beings and less intense as it moves away from that core*".[9] The intimate personal sphere, which is impervious to intrusions, includes one's home, personal life, beliefs and preferences.[10] However, as one moves into the public realm, engaging in communal relations

---

[6] Section 14 of the Constitution.

[7] *Mistry v Interim National Medical and Dental Council of South Africa* [1998] ZACC 10; 1998 (4) SA 1127 (CC); 1998 (7) BCLR 880 (CC) ("*Mistry*") at para 25.

[6] *Gaertner v Minister of Finance* [2013] ZACC 38; 2014 (1) SA 442 (CC); 2014 (1) BCLR 38 (CC) at para 47.

[9] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Limited In re: Hyundai Motor Distributors (Pty) Limited v Smit NO* [2000] ZACC 12; 2001 (1) SA 545 (CC); 2000 (10) BCLR 1079 (CC) ("*Hyundai*") at para 18.

[10] In *Mistry* above n 8 at para 27, the Constitutional Court explained that there exists—

> "a continuum of privacy rights which may be regarded as starting with a wholly inviolable inner self, moving to a relatively impervious sanctum of the home and personal life, and ending in a public realm where privacy would only remotely be implicated".

In this regard, the Constitutional Court cited with approval its earlier judgment in *Bernstein v Bester NNO* [1996] ZACC 2; 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC) at para 67.

and commercial and social activities, the protection afforded by the right to privacy diminishes accordingly.[11]

Private communications clearly fall within the intimate personal sphere or "*inner sanctum*" of a person and are thus at the very core of what is protected by the right to privacy.[12] As the Constitutional Court explained in *AmaBhungane*—

> "By nature, human beings are wont – in their private communications – to share their innermost hearts' desires or personal confidences, to speak or write when under different circumstances they would never dare do so, to bare themselves on what they truly think or believe."[13]

Surveillance of a person's private communications is an egregious violation of the right to privacy.[14] It also limits various other constitutional rights in addition to the right to privacy.

The Constitutional Court has also repeatedly reiterated that there is a strong relationship between the right to privacy and the right to human dignity.[15] The Constitutional Court has recognised that the right to freedom of expression is "*part of a web of mutually supporting*

---

[11] *Bernstein* ibid at para 67.

[12] This was recently confirmed by the Constitutional Court in *Amabhungane* above n 2 at para 24.

[13] Ibid at para 23.

[14] Ibid at para 24.

[15] Human dignity is a founding constitutional value enshrined in section 1(a) of the Constitution and section 10 of the Constitution provides that "[e]veryone has inherent dignity and the right to have their dignity respected and protected". The connection between the rights to privacy and dignity is recognised by O'Regan J in *Khumalo v Holomisa* [2002] ZACC 12; 2002 (5) SA 401 (CC); 2002 (8) BCLR 771 (CC). O'Regan J said, at para 27:

> "The right to privacy, entrenched in section 14 of the Constitution, recognises that human beings have a right to a sphere of intimacy and autonomy that should be protected from invasion. This right serves to foster human dignity."

rights", which includes the rights to dignity and privacy,[16] and "*is of the utmost importance in the kind of open and democratic society the Constitution has set as our aspirational norm*".[17]

The right to freedom of expression is also limited by RICA because surveillance impacts what people say and how they say it.[18] As the Constitutional Court explained, people make intimate communications in the belief that the communication is read or heard only by the person with whom they are communicating.[19] The Court stated:

> "It is that belief that gives them a sense of comfort – a sense of comfort either to communicate at all; to share confidences of a certain nature or to communicate in a particular manner."[20]

The Court further cautioned: "*Imagine how an individual in that situation would feel if she or he were to know that throughout those intimate communications someone was listening in or reading them*."[21]

Communications surveillance incentivises self-censorship and has a chilling effect on the exercise of the right to freedom of expression. It may similarly have a chilling effect on the

---

[16] *Case and Another v Minister of Safety and Security; Curtis v Minister of Safety and Security* [1996] ZACC 7; 1996 (3) SA 617; 1996 (5) BCLR 608 at para 27.

[17] *S v Mamabolo (E TV Intervening)* [2001] ZACC 17; 2001 (3) SA 409 (CC); 2001 (5) BCLR 449 (CC) at para 37.

[18] Section 16(1)(b) of the Constitution provides that "[e]veryone has the right to freedom of expression", which includes the "freedom to receive or impart information or ideas".

[19] *AmaBhungane* above n 2 at para 23.

[20] Ibid.

[21] Ibid.

inter-connected rights to assembly,[22] to freedom of association[23] and to make political choices.[24]

No right in the South African Bill of Rights is absolute. Rights may be limited provided that the limitation is justifiable under section 36 of the Constitution.[25] A rights limitation will only be justifiable if the purpose sought to be achieved by the measure is both rationally related and proportional to the limitation of the right and there are no less restrictive means that could achieve the same purpose.[26]

The onus is on the State to justify the limitation of the right to privacy that is occasioned by State surveillance of personal communications. In seeking to discharge this onus, sufficient information must be provided for a court to assess and evaluate the policy being pursued.[27]

---

[22] Section 17 of the Constitution.

[23] Section 18 of the Constitution.

[24] Section 19(1) of the Constitution.

[25] Section 36(1) of the Constitution provides:

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

[26] Sections 36(d) and (e). See *National Coalition for Gay and Lesbian Equality v Minister of Justice* [1998] ZACC 15; 1999 (1) SA 6 (CC); 1998 (12) BCLR 1517 at para 35.

[27] *Minister of Home Affairs v National Institute for Crime Prevention and the Reintegration of Offenders* [2004] ZACC 10; 2005 (3) SA 280 (CC); 2004 (5) BCLR 445 (CC) ("*NICRO*") at para 65.

In the clash between privacy rights and the purpose sought to be achieved by the State through surveillance of private communications, whether the limitation is justifiable will often turn on whether there are adequate safeguards to minimise the extent of the invasion of privacy rights.[28] Where there are no or inadequate safeguards, the purpose sought to be achieved is disproportionate to the limitation of the right.[29]

Security Services

Chapter 11 of the Constitution governs the security services of South Africa, which consist of the defence force, the police service and intelligence services.[30] Section 198 of the Constitution sets out the principles governing national security. These principles include peace and security; compliance with the law, including international law; and oversight by Parliament and the National Executive.[31] The Constitution requires the security services to "*act in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic*".[32]

[28] The Constitutional Court, in *Mistry* above n 8 at para 25, said:

> "The existence of safeguards to regulate the way in which State officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police State."

[29] Ibid at para 30.

[30] Section 199(1) of the Constitution.

[31] Sections 198(a), (c) and (d) of the Constitution.

[32] Section 199(5) of the Constitution.

The legislative scheme

There is a broad array of laws that have a bearing on communications surveillance in South Africa. However, two primary laws govern the State's surveillance of communications and communication-related information: RICA and section 205 of the Criminal Procedure Act.[33]

RICA

RICA is the primary legislation dealing with communications surveillance in South Africa.[34]

RICA creates a mechanism for lawful interception of communications. The interception of communications is prohibited unless the interception takes place in terms of RICA.[35] Outside of the mechanism for lawful interceptions created by RICA, it is an offence – carrying severe penalties – to intercept a communication during its occurrence or transmission.[36]

RICA creates a mechanism for targeted surveillance. It provides a framework for "separate, particular applications to surveil particular subjects".[37] It makes no provision for mass surveillance of the private communications of the public.

RICA regulates the surveillance of communications and communication-related information. RICA defines communication broadly so that it includes in-person conversations, phone calls,

---

[33] Act 51 of 1977.

[34] The long title of RICA provides, in relevant part, that the Act is intended "[t]o regulate the interception of certain communications . . . and the provision of certain communication-related information".

[35] Section 2 of RICA.

[36] Section 49(1) read with 51(1)(b)(i). A person convicted of unlawfully intercepting communications is liable to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

[37] Milo and Scott "The High-Wire: the Delicate Balance between Communications Surveillance, Constitutional Rights and the Media in South Africa" in Bosland and De Zwart (eds) *Watching Me, Watching You: Surveillance, Privacy and the Media* (LexisNexis, Cape Town 2016) at 259.

letters, emails and cell phone communications (data, text, visual or audio messages).[38] Communication has been described as the "*content of a message*".[39] Communicated-related information, commonly referred to as metadata, is information revealing the "origin, destination, termination, duration, and equipment" used in a phone call or message.[40] Metadata has been described as "*information about who sent a message to whom and when or where the message was sent*".[41] In other words, it is all the information about a call or message except the content thereof.

RICA prescribes limited legitimate aims for the interception of communications. It provides that any surveillance direction may only be issued in response to serious offences, threats to public health and safety, threats to national security or compelling national economic interests, organised crime or terrorism, property that is an instrumentality of a serious offence, or the proceeds of unlawful activities.[42]

RICA requires that surveillance be judicially authorised. It establishes a designated Judge, who is at the centre of the mechanism for lawful surveillance provided for in the Act.[43] The

[38] Section 1 of RICA defined "communication" as including both direct and indirect communication. See the definitions of "direct communication" and "indirect communication" in section 1 of RICA.

[39] Bakir, "'Veillant Panoptic Assemblage': Mutual Watching and Resistance to Mass Surveillance After Snowden" (2015) 3 *Media and Communications* 12.

[40] "Communication-related information" is defined in section 1 of RICA 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".

[41] Bakir above n 39.

[42] Section 16(5)(a), 17(4), 18(3) and 19(4) of RICA.

[43] "Designated Judge" is defined in section 1 of RICA as "any judge of a High Court discharged from active service under section 3 (2) of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act 47 of 2001), or

designated Judge is responsible for authorising all but one of the surveillance directions that may be sought and issued under RICA.[44]

RICA provides for an application to be made to the designated Judge for a direction for the interception of communications.[45] It also provides for an application to be made to the designated Judge for a direction concerning real-time communication-related information.[46] Where only archived communication-related information is sought, an application may be made to a magistrate or a High Court judge.[47] However, a combined application for interception directions and real-time or archived communication-related directions must be made to the designated Judge.[48]

Where an interception direction has been issued, further applications may be made to the designated Judge, including an application for a decryption direction, where the information intercepted is encrypted,[49] and an application for an entry warrant for the purpose of installing an interception device on the premises to facilitate interceptions.[50]

RICA does provide for communications to be intercepted, including for the purposes of determining location, without any prior judicial authorisation in cases of emergency.[51] The

---

any retired judge, who is designated by the Minister to perform the functions of a designated judge for purposes of this Act".

[44] Sections 16-8 and 20-2 of RICA.

[45] Section 16 of RICA.

[46] Section 17 of RICA.

[47] Section 19 of RICA.

[48] Section 18 of RICA.

[49] Section 21 of RICA.

[50] Section 22 of RICA.

[51] Sections 7 and 8 of RICA.

exceptional circumstances in which this is permitted include where the interception is directed at preventing serious bodily harm to the subject of the surveillance or any other person or where the interception is directed at determining the location of the subject of surveillance in cases of emergency where the life of the subject of any other person is endangered or serious injury has occurred or is likely to occur.[52] However, the designated Judge must be notified as soon as possible after the interception and provided with the results and the information obtained from the interception.[53]

RICA establishes interception centres under the control of the Office for Interception Centres, which are the only entities that may carry out interceptions in terms of the Act.[54] The interception centres carry out interceptions for law enforcement agencies.

Section 205 of the CPA

Outside of RICA, law enforcement officers have another means of obtaining communication-related information or metadata in terms of section 205 of the Criminal Procedure Act ("**CPA**").[55]

---

[52] Sections 7 and 8 of RICA.

[53] Sections 7(4)-(5) and 8(4)-(5) of RICA.

[54] Sections 32-3 of RICA.

[55] Section 205(1) of the CPA provides:

> "*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*

Section 205 of the CPA provides a subpoena mechanism for law enforcement officers to approach a magistrate or High Court judge to obtain real-time or archived communications-related information from a communications service provider.[56] This is a process for obtaining communications-related information that operates parallel to RICA and without the safeguards contained in RICA.[57]

CHAPTER TWO: INTERNATIONAL LAW

International law is critical to determining the extent of the State's human rights obligations in relation to the surveillance of private communications. First, the interpretation of the rights in the Bill of Rights must involve a consideration of international law.[58] Second, the measures that the State must take to respect, protect, promote and fulfil the rights in the Bill of Rights are informed by international law.[59] Third, the Constitution requires national security to be pursued in compliance with international law and requires our security services to act in

---

> *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*."

[56] Section 205 of the CPA should be read with section 15 of RICA. Section 15(1) of RICA provides:

> *"[T]he 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 preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act*."

[57] See Hunter and Mare "A Patchwork for Privacy: Communications Surveillance in Southern Africa" *Media Policy and Democracy Project* (6 May 2020), available at https://archive.org/details/patchwork-for-privacy-communication-surveillance-in-southern-africa/page/n1/mode/2up, at 11-2 and Hunter "Cops and Call Records: Policing and Metadata Privacy in South Africa" *Media Policy and Democracy Project* (27 March 2020), available at https://archive.org/details/2003-cops-and-call-records-metadata-and-policing.

[58] Section 39(1)(b) of the Constitution.

[59] See *Sonke Gender Justice NPC v President of the Republic of South Africa* [2020] ZACC 26; 2021 (3) BCLR 269 (CC) (*Sonke*) at paras 55-6 and *Glenister v President of the Republic of South Africa* [2011] ZACC 6; 2011 (3) SA 347 (CC); 2011 (7) BCLR 651 (CC) (*Glenister II*) at para 192.

accordance with both customary international law and international agreements binding on South Africa.[60]

International law, therefore, must be a guide to South Africa in reforming its laws on communications surveillance. It is not only binding sources of international law (customary law and binding international agreements) by which Parliament must be guided.[61] Non-binding sources of international law also provide a useful interpretive guide in relation to the rights in the Bill of Rights and the State's obligations.[62]

A number of key international agreements enshrining the fundamental right to privacy are binding on South Africa, including the Universal Declaration of Human Rights,[63] the International Covenant on Civil and Political Rights,[64] and the Convention on the Rights of the Child.[65] These agreements protect against "arbitrary interference" with a person's privacy.

The statements of international bodies, international human rights treaty bodies, human rights experts and regional human rights courts – giving meaning to these binding international agreements – make it clear that interference with the right to privacy through communications

[60] Section 198(c) and 199(5) of the Constitution.

[61] Customary international law is law in South Africa (section 232 of the Constitution). International agreements are binding on South Africa once they have been approved by the National Assembly and the National Council of Provinces (section 231(2) of the Constitution).

[62] See *Sonke* at paras 57 and 65. Non-binding sources of international law include international agreements that South Africa has not ratified, commentaries on treaties, and judicial decisions.

[63] Article 12 of the Universal Declaration on Human Rights, 10 December 1948.

[64] Article 17 of the International Covenant on Civil and Political Rights, 16 December 1966. The ICCPR was signed by South Africa on 3 October 1994 and ratified on 10 December 1998.

[65] Article 16 of the Convention on the Rights of the Child, 20 November 1989. The Convention was signed by South Africa on 29 January 1993 and ratified on 16 June 1995.

surveillance must be in accordance with the principles of legality, necessity and proportionality so as not to be arbitrary.

- The principle of legality requires that surveillance be conducted in terms of a legal framework that is sufficiently clear and precise, publicly accessible and comprehensive.[66]
- The principle of necessity requires that communications surveillance only be conducted when necessary and to achieve legitimate aims.
- The principle of proportionality requires that communications surveillance appropriately balance the interference with the right to privacy and the legitimate aims sought to be achieved and not unnecessarily intrude upon the right to privacy.

The United Nations General Assembly has adopted a number of resolutions on the Right to Privacy in the Digital Age.[67] The most recent Resolution, adopted in 2020, notes that communications surveillance "*must be consistent with international human rights obligations*" and recalls that States must ensure that any interference with the right to privacy "*is consistent with the principles of legality, necessity and proportionality*".

[66] See, for instance, the European Court of Human Rights in *Malone v the United Kingdom*, no 8691/79, § 67, ECHR 1984, in the context of communications surveillance:

> "*[T]he law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*."

[67] UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020). See also UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018) and UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014) (UN Resolution 2014).

The United Nations Office of the High Commissioner for Human Rights (OHCHR),[68] the UN Human Rights Council (HRC),[69] the Special Rapporteur on the Right to Privacy (Special Rapporteur on Privacy)[70] and the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur on Expression)[71] have echoed that the right to privacy may only be interfered with in accordance with the principles of legality, necessity and proportionality. Regional human rights courts have similarly stressed the importance of the principles of legality, necessity, and proportionality in evaluating the clash between the right to privacy and communications surveillance.[72]

To clarify the human rights obligations of States when conducting communications surveillance, international civil society organisations and experts developed the International Principles on the Application of Human Rights to Communications Surveillance ("**the Necessary and Proportionate Principles**").[73] The Necessary and Proportionate Principles were

[68] Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018) (UN Report 2018) at para 10.

[69] UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021) (UN Resolution 2021).

[70] Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (27 October 2019) at para 78.

[71] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019) at para 24.

[72] On the principle of legality, among others: *Big Brother Watch v The United Kingdom*, nos 58170/13 and 2 others, § 2 and 334, ECHR 2021.

On the principle of necessity, among others: *P.N. v Germany*, no 74440/17, § 69, ECHR 2020 and *Szabó and Vissy v Hungary*, no 37138/14, § 73, ECHR 2016.

On the principle of proportionality, among others: *Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources* , nos 293/12 and 594/12, § 46, ECHR 2014.

[73] The Necessary and Proportionate Principles are available at https://necessaryandproportionate.org/principles/.

launched at the UN Human Rights Council in 2013, and have since been adopted by over 600 organisations globally. They are frequently referenced in legislative reform debates.[74]

The Necessary and Proportionate Principles are based on established international human rights law and standards.[75] The Principles provide a framework to align communications surveillance laws and practices with State's human rights obligations and duties – offering robust protection of human rights.

CHAPTER THREE: THE AMABHUNGANE JUDGMENT

Background to the judgment

On 4 February 2021, the Constitutional Court of South Africa handed down judgment in the *AmaBhungane* matter, finding that the legislation that governs the surveillance of communications, RICA, is unconstitutional for failing to provide adequate safeguards to protect the right to privacy. The Constitutional Court also held that the State's practice of bulk surveillance is unlawful.

The challenge to the constitutionality of RICA was brought before the Gauteng Division of the High Court, Pretoria by the AmaBhungane Centre for Investigative Journalism NPC ("**AmaBhungane Centre**"), an investigative journalism organisation. The application was sparked by revelations that the private, confidential conversations between a prominent

[74] Electronic Frontier Foundation "Necessary & Proportionate: on the Application of Human Rights to Communications Surveillance", available at https://necessaryandproportionate.org/13-principles/.

[75] Electronic Frontier Foundation "Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance" (May 2014), available athttps://necessaryandproportionate.org/global-legal-analysis/.

investigative journalist, Mr Sam Sole, and a source in the National Prosecuting Authority were being surveilled.

The High Court upheld the AmaBhungane Centre's challenges to the constitutionality of RICA and held that the bulk surveillance carried out by the National Communications Centre ("NCC") is unlawful.[76] The matter came before the Constitutional Court for confirmation of the orders granted by the High Court.[77]

The Constitutional Court's judgment

The constitutionality of RICA

The Constitutional Court recognised that the right to privacy was at the heart of the matter and held that the surveillance of personal communications under RICA limits the right to privacy. Indeed, it is "a highly and disturbingly invasive violation of privacy"[78] because RICA:

1. does not differentiate between intimate personal communications and less personal communications;

2. does not differentiate between information that is relevant to the purpose of the interception and that which is not; and

[76] *Amabhungane Centre for Investigative Journalism NPC v Minister of Justice* 2020 (1) SA 90 (GP) ("*AmaBhungane High Court judgment*").

[77] The applicant, AmaBhungane, sought confirmation of the High Court's declarations of invalidity. The Minister of Police partially appealed the judgment and orders of the High Court. The Minister of State Security appealed the whole judgment and order of the High Court.

[78] Ibid at para 24.

3. permits the interception of communications of any person who communicates with the subject of surveillance notwithstanding that they are not themselves subjects of surveillance.[79]

The crux of the case before the Constitutional Court was thus whether the limitation of the right to privacy is justifiable under section 36 of the Constitution. The Court recognised that the interception of communications through RICA plays a central role in the State's ability to fulfil its constitutional obligations to "secure the nation, ensure that the public is safe and prevent serious crime".[80]

Notwithstanding the important purpose sought to be achieved through RICA, the Constitutional Court held that the limitation of the right to privacy is not justifiable because the egregious limitation is disproportionate to the purpose sought to be achieved. RICA does not do enough to reduce the risk of unnecessary intrusions – there are inadequate safeguards in RICA to limit the extent to which the right to privacy is impaired.

The Constitutional Court confirmed the High Court order declaring RICA unconstitutional and invalid in five respects.[81]

First, RICA fails to provide a mechanism for the subject of surveillance to be notified of the surveillance even after the surveillance has come to an end.[82]

[79] Ibid at paras 24 and 31.

[80] Ibid at para 30.

[81] Ibid at Order para 6.

[82] Ibid at para 48.

The Constitutional Court held that surveillance under RICA is susceptible to abuse because it "*takes place in complete secrecy*" without any notice given to the subject of the surveillance.[83] While pre-surveillance notification would defeat the purpose sought to be achieved by the surveillance,[84] post-surveillance notification would reduce the sense of impunity with which wrongful surveillance is undertaken without jeopardising the purpose sought to be achieved by surveillance.[85]

The absence of post-surveillance notification also implicates the rights of access to court (section 34) and to an appropriate remedy (section 38).[86] In the absence of any notification, a subject of surveillance will not be able to approach a court to determine whether an interception direction was applied for, granted and implemented in terms of the Constitution and RICA. In the event that it was not, they will not be able to seek appropriate relief for the violation of the right to privacy.[87]

Second, RICA fails to ensure adequate safeguards for the independence of the designated Judge.[88] That Judge, who authorises surveillance and is the "centrepiece" of RICA,[89] is appointed by the Minister of Justice, a member of the Executive, "*without the involvement of*

[83] Ibid at para 41.

[84] Ibid at para 41.

[85] Ibid at paras 45-6.

[86] Ibid at para 48.

[87] Ibid at paras 44-5.

[88] Ibid at para 94.

[89] Ibid at para 56.

any other person or entity". [90] In addition, the designated Judge's term of office is not fixed and has in practice been renewed. [91]

The Court held that the Constitution requires that the designated Judge have actual and perceived independence.[92] The Court recognised that the "*non-transparent, if not impenetrable, circumstances in which the power of issuing RICA surveillance directions is exercised make it singularly important that there be no apprehension or perception of lack of independence*".[93] The Court held that the lack of specificity in RICA on the designated Judge's appointment and extension of terms is not consistent with the constitutional requirement of independence.[94]

Third, RICA fails to provide adequate safeguards to protect the privacy rights of intended subjects of surveillance in an *ex parte* process.[95]

An application for an interception direction is considered and issued without notice to the intended subject of surveillance and without affording them a hearing.[96] The Court cautioned that the result of an *ex parte* process is that the designated Judge is required to consider and issue an interception direction on the basis of information which has been provided by the applicant State agency, and which the designated Judge is not in a position to meaningfully

[90] Ibid at para 92.

[91] Ibid at para 92.

[92] Ibid at paras 82-5.

[93] Ibid at para 84

[94] Ibid at para 92.

[95] Ibid at para 100.

[96] Ibid at para 95. See section 16(7)(a) of RICA.

interrogate.[97] The Court noted that the inadequacies in this process facilitate wrongful surveillance.

Fourth, RICA provides no clarity on how information is managed once intercepted and obtained. RICA "*give[s] no clarity or detail on: what must be stored; how and where it must be stored; the security of such storage; precautions around access to the stored data (who may have access and who may not); the purposes for accessing the data; and how and at what point the data may or must be destroyed*".[98]

The Court cautioned that the absence of clarity concerning the management of information presents "*a real risk*" that the private information gathered may be accessed by persons or used for purposes other than those envisaged in RICA.[99]

Fifth, RICA fails to provide any additional safeguards when the intended subject of surveillance is a practising lawyer or journalist so as to minimise the risk of infringement of the confidentiality of lawyer-client communication and journalists' sources.[100]

The Court recognised that there is a need for special consideration to be given when the intended subject of surveillance is a lawyer or journalist.[101] The interception of the communications of lawyers and journalists is an egregious intrusion into privacy, and particularly so because it impacts on other important constitutional rights.[102] The right to

[97] Ibid at para 96.

[98] Ibid at para 107.

[99] Ibid at para 107.

[100] Ibid at para 119.

[101] Ibid at para 119.

[102] Ibid at para 119.

freedom of expression and the media protects the confidentiality of journalists' sources.[103] Legal professional privilege is a core part of the rights to a fair trial and fair hearing upon which the proper functioning of our legal system depends.[104]

The Constitutional Court suspended the declarations of invalidity for a period of three years to give Parliament an opportunity to cure the defects in RICA.[105] The Court held that justice and equity required it to grant appropriate interim relief, which would be applicable during the period of suspension, to militate the effect of the violation of the privacy right.[106]

The Constitutional Court granted interim reading-in relief requiring that:

- Post-surveillance notification be given within 90 days of the expiry of an interception direction or extension thereof.[107] Notification may be withheld where it would

[103] Ibid at para 115.

[104] Ibid at paras 116-7.

[105] Ibid at para 140 and Order para 7.

[106] Ibid at para 144.

[107] Ibid at Order para 8, which reads:

> "*During the period of suspension referred to in paragraph 7, RICA shall be deemed to include the following additional sections:*
>
> *. . .*
>
> *'Section 25A Post-surveillance notification*
>
> *(1) Within 90 days of the date of expiry of a direction or extension thereof issued in terms of sections 16, 17, 18, 20, 21 or 23, whichever is applicable, the applicant that obtained the direction or, if not available, any other law enforcement officer within the law enforcement agency concerned must notify in writing the person who was the subject of the direction and, within 15 days of doing so, certify in writing to the designated Judge, Judge of a High Court, Regional Court Magistrate or Magistrate that the person has been so notified.*
>
> *(2) If the notification referred to in subsection (1) cannot be given without jeopardising the purpose of the surveillance, the designated Judge, Judge of a High Court, Regional Court Magistrate or*

jeopardise the purpose of the surveillance, but there are clear restrictions on the withholding of notification.[108]

- Where the intended subject of surveillance is a practicing lawyer or a journalist, the designated Judge must be informed of this fact and must grant the surveillance direction only where it is necessary to do so and subject to conditions that are necessary to protect the confidentiality of lawyer-client communications or a journalist's sources.[109]

> *Magistrate may, upon application by a law enforcement officer, direct that the giving of notification in that subsection be withheld for a period which shall not exceed 90 days at a time or two years in aggregate*.'"

[108] Ibid.

[109] Ibid at Order para 8, which reads:

> "During the period of suspension referred to in paragraph 7, RICA shall be deemed to include the following additional sections:
>
> > 'Section 23A Disclosure that the person in respect of whom a direction, extension of a direction or entry warrant is sought is a journalist or practising lawyer
> >
> > (1) Where the person in respect of whom a direction, extension of a direction or entry warrant is sought in terms of sections 16, 17, 18, 20, 21, 22 or 23, whichever is applicable, is a journalist or practising lawyer, the application must disclose to the designated Judge the fact that the intended subject of the direction, extension of a direction or entry warrant is a journalist or practising lawyer.
> >
> > (2) The designated Judge must grant the direction, extension of a direction or entry warrant referred to in subsection (1) only if satisfied that it is necessary to do so, notwithstanding the fact that the subject is a journalist or practising lawyer.
> >
> > (3) If the designated Judge issues the direction, extension of a direction or entry warrant, she or he may do so subject to such conditions as may be necessary, in the case of a journalist, to protect the confidentiality of her or his sources, or, in the case of a practising lawyer, to protect the legal professional privilege enjoyed by her or his clients.'"

Bulk communication surveillance

Another question before the Constitutional Court was whether there is a legal basis for the state to conduct bulk surveillance. The National Communications Centre ("NCC") in Pretoria had been engaging in bulk surveillance by monitoring transnational signals to "*screen them for certain cue words or key phrases*". [110]

The Court described the NCC's bulk surveillance as involving the "*interception of all internet traffic that enters or leaves South Africa, including the most personal information such as emails, video calls, location and browsing history*".[111] The Court held that there is no law authorising the practice of bulk surveillance[112] and that the practice is accordingly unlawful and invalid.[113]

It remains an open question whether bulk surveillance – if a law is enacted to authorise the practice – is consistent with the Constitution.

---

[110] Ibid at para 4 and footnote 13. The Constitutional Court appears to have adopted the explanation of bulk surveillance that was provided by the respondents in the court a quo and accepted by the High Court.

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

[111] Ibid at para 124.

[112] Ibid at para 135. The principle of legality, a component part of the rule of law, requires that every exercise of public power have a basis in some law.

[113] Ibid at para 135.

CHAPTER FOUR: RECOMMENDATIONS FOR REFORMS TO CURE THE DEFECTS IDENTIFIED IN THE CONSTITUTIONAL COURT JUDGMENT AND ORDER IN *AMABHUNGANE*

While the Court found RICA to be inconsistent with the Constitution for failing to provide adequate safeguards to protect the right to privacy, the choice of safeguards is ultimately left to Parliament. However, the Court's judgment is instructive as to the features that the chosen safeguards must possess to adequately protect the right to privacy from unnecessary intrusions.

Parliament has now acted to remedy the defects identified by the Constitutional Court in *AmaBhungane*. However, the Bill that it has passed falls short of what is required by the Constitutional Court's judgment in numerous respects. In this Chapter, the deficiencies of the Bill are discussed and recommendations are made for better legislative reform.

An amendment Bill dealing with the defectes identified by the Constitutional Court accompanies this thesis as Appendix I. Its provisions are detailed and discussed in the recommendations sections of this Chapter.

Post-surveillance notification

Introduction

RICA provides that applications for surveillance directions must be considered and directions issued "*without any notice to the person … to whom the application applies and without hearing such person*".[114] The Constitutional Court declared this unconstitutional.

[114] Sections 16(7), 17(6), 18(3), 19(6), 20(6), 21(6) and 22(7) of RICA.

The Constitutional Court's judgment and order requires that the subject of surveillance be notified that they have been surveilled after the surveillance has come to an end.[115]. The Court did not dictate to Parliament the period within which the subject must be notified to cure the defect in RICA. However, the Court granted an interim order requiring notification to be given within 90 days of the surveillance coming to an end.

Discussion

A survey of comparable democracies with post-surveillance notification reveals that notification must be given within a well-defined, reasonable period of time.[116] In Japan, the legislation governing communications interceptions requires notification to be given to the subject of surveillance within 30 days of the surveillance being terminated.[117] Canada and the United States of America require post-surveillance notification to be given within 90 days.[118]

The Bill inserts a provision into RICA requiring that post-surveillance notification be given within 90 days of the surveillance coming to an end.[119] This appears to be a reasonable period, which aligns with the period of time provided for in comparative democracies.

While the Constitutional Court only considered the need for post-surveillance notification in the context of surveillance directions issued by the designated Judge in terms of sections 16, 17, 18, 20, 21 or 23, notification is equally required where surveillance is conducted without

[115] Ibid at Order para 6(b).

[116] Electronic Frontier Foundation "Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance" (May 2015), available at https://necessaryandproportionate.org/implementation-guide/, at 26.

[117] Act on Communications Interception for Criminal Investigation Act 137 of 1999, Article 30.

[118] Canadian Criminal Code, RSC, 1985, c. C-46, Part VI and Code of Laws of the United States of America ("US Code"), Title 18, section 2518(8)(d).

[119] Section 4 of Bill 28B, 2023 inserts section 25A(1) into RICA.

prior judicial authorisation in cases of emergency in terms of sections 7 and 8 of RICA. Indeed, there is a greater need for post-surveillance notification in these cases as surveillance conducted without prior judicial authorisation is more susceptible to abuse. The same notification requirements should apply to cases of emergency surveillance. The Bill has picked up on this omission in the Constitutional Court's judgment and order. The Bill requires that post-surveillance notification be given in the circumstance where surveillance was conducted in terms of section 7 or 8 of RICA.

However, Parliament departs from the spirit of the judgment of the Constitutional Court when it comes to the circumstances in which notification may be withheld.

The Constitutional Court makes it clear that post-surveillance notification must be the "default position".[120] The Court accepted that in exceptional circumstances notification may be withheld. In defining exceptional circumstances, the Court referred to the jurisprudence of the European Court of Human Rights, which requires that post-surveillance notification must be given "as soon as that can be done without jeopardising the purpose of the surveillance after the surveillance has been terminated".[121] This is a flexible standard that will depend on the facts of each case.

The Constitutional Court further emphasised that there are strict limits on the withholding of post-surveillance notification.[122]

[120] *AmaBhungane* above n 2 at para 48.

[121] Ibid at para 147.

[122] Ibid at para 148.

First, notification may only be withheld with authorisation from the designated Judge.[123] Authorisation for the withholding of notification for a period longer than the initial period after the surveillance has come to an end must be sought on application from the designated Judge. The applicant State agency seeking to withhold notification must establish on the facts of the case that the delay is justified.[124]

Second, the Court was emphatic that notification may not be withheld indefinitely.[125] This requires that there be clear provisions prescribing the time-period during which notification may be delayed and that any additional delays must be subject to the same process of authorisation. It further requires that there should be an upper time-limit for the withholding of notification.

While the Bill makes provision for the application to a designated judge for the withholding of the giving of notification "*for a period not exceeding 90 days at a time or two years in aggregate*", the Bill allows for the withholding of the giving of notification indefinitely where notification "*has the potential to impact negatively on national security*".[126] In such cases, the period for extension is left to the discretion of the designated judge and there is no upper time-limit for the withholding of notification. "National security" is a vague term and is not defined in RICA. The addition of this provision severely undermines the protections that the Constitutional Court sought to put in place through the requirement of post-surveillance

[123] Ibid at para 48.

[124] Ibid.

[125] Ibid at para 148.

[126] Section 4 of Bill 28B, 2023 inserts section 25A(2)(b) into RICA.

notification. The Bill is not adequate to end secrecy and impunity for abuses of the RICA-process.

Recommendations

It is recommended that RICA is amended to insert a new section in the Act headed “post-surveillance notification".

- Section 25A(1) prescribes that notification must be given to the subject of surveillance after the surveillance has come to an end, and within a period of 90 days. The provision is sourced from the Constitutional Court’s interim order in *AmaBhungane*. However, it includes provision for post-surveillance notification where surveillance is conducted under sections 7 and 8 of RICA.
- Section 25A(2) makes provision for applications for extensions of the period within which notification must be given. This provision is sourced from the Constitutional Court’s interim order in *AmaBhungane.*

Independence of the designated judge

Introduction

RICA fails to expressly provide for the designation or appointment of the designated Judge, as held by the Constitutional Court.

The Minister of Justice’s power to designate a Judge is implied in the definition of ‘designated judge’ in section 1 of RICA (read together with the other provisions of RICA on the functions of the designated Judge).[127] The absence of express provisions is, at least in some measure, to blame for the lack of specificity in RICA on the designated Judge’s appointment and extension

[127] Ibid at paras 76 and 78-9.

of terms. Detailed and specific provisions dealing with the appointment and term of office of the designated Judge are essential protections for independence.[128]

Discussion

The defect with regard to the appointment, as identified by the Constitutional Court, is that the designated Judge is appointed by the Minister of Justice and Correctional Services ("**Minister**") without any limits on the Minister's open-ended discretion.[129] No other person or entity is involved in the appointment of the designated Judge.[130] The Constitutional Court's judgment makes it clear that there is a special need for a transparent and accountable appointment process given the secrecy in which the designated Judge is required to operate.[131]

The Bill seeks to remedy this defect by requiring that the Minister designate a designated judge "*in consultation with the Chief Justice*".[132] Our courts have clarified that "in consultation" requires consensus – not merely that consideration be given to the view of the party consulted.[133]

However, it is not clear that this goes far enough given the importance of the position of the designated judge. The Constitutional Court has emphasised that the involvement of the Judicial Service Commission ("**JSC**") in appointments and the holding of a public interview process allows "*for public scrutiny, accountability and public trust*".[134] An appointment process that

[128] *Justice Alliance of South Africa v President of Republic of South Africa*[2011] ZACC 23; 2011 (5) SA 388 (CC); 2011 (10) BCLR 1017 (CC) ("*Justice Alliance*") at para 60.

[129] *AmaBhungane* above n 2 at para 92.

[130] Ibid.

[131] Ibid at para 93.

[132] Section 2 of Bill 28B of 2023 inserts section 15A(2) into RICA.

[133] *Public Servants Association of South Africa and Others v Government Employees Pension Fund and Others* [2020] 4 All SA 710 (SCA) at para 55.

[134] Ibid at para 91.

requires the Minister to appoint the designated Judge upon the recommendation of the JSC would adequately safeguard the independence of the designated Judge and ensure that there is public scrutiny of the appointment. The JSC is involved in the appointment process for judges who are appointed to the Constitutional Court, the Supreme Court of Appeal and certain specialised courts, notwithstanding that they are already judges.[135]

The other defect identified by the Constitutional Court relates to the failure to provide for the term of office of a designated judge.

The terms of office of specialised judges in comparative democracies fall across a range. In the United States of America, specialised judges on the Foreign Intelligence Service Court have a maximum term of seven years.[136] In the United Kingdom[137] and New Zealand,[138] judicial commissioners are appointed for a term of three years. On the one hand, a sufficiently lengthy term of office allows for the development and retention of expertise in the office of the designated Judge. On the other hand, a term of office that is too long may lead to "*case hardening*", where the designated Judge may lose their "*qualities of independence and external insight*" through a process of acclimatisation to the setting of security intelligence.[139] It is recommended that the designated Judge be appointed for a term of five years.

---

[135] See section 174(4) and 174(6) of the Constitution and section 19(1) of the Electoral Commission Act 51 of 1996.

[136] US Code, Title 50, section 1803(d).

[137] Section 228(2) of the Investigatory Powers Act 2016. The term of office is renewable.

[138] Section 117 read together with section 1(1) of Part 1 of Schedule 3 of the Intelligence and Security Act 2017. Judicial commissioners are referred to as Commissioners of Intelligence Warrants. They advise the Minister on prior authorisation of surveillance measures. The term is renewable.

[139] Report on the Democratic Oversight of the Security Services, no 388 / 2006, European Commission for Democracy through Law (Venice Commission) 2007 ("Venice Commission report") at para 213.

In addition, a fixed and non-renewable term of office is an essential guarantor of adequate independence, as was confirmed by the Constitutional Court in *Justice Alliance*.[140] The Court recognised that an extension of a term of office "*may be seen as a benefit*" and that the public may reasonably assume that "*extension may operate as a favour that may influence those judges seeking it*."[141]

The Constitutional Court, in a trio of cases, *Justice Alliance*, *Glenister II* and *Helen Suzman Foundation*, similarly recognised that renewable terms of office are antithetical to adequate independence.[142] "*Renewal invites a favour-seeking disposition from the incumbent*" and induces the incumbent to "*adjust her approach to the enormous and sensitive responsibility of her office with regard to the preference of the one who wields the discretionary power to renew or not renew the term of office*".[143]

The Bill provides for a non-renewable fixed term for a designated judge not exceeding seven years.[144] It further provides that the designation of a designated judge will come to an end upon: (i) the completion of their period of tenure; (ii) the acceptance by the Minister, in consultation with the Chief Justice, of a request to resign; or (iii) the death of the judge.[145] The

[140] *Justice Alliance* above n 127 at para 90. The Constitutional Court held, at para 85, that section 176(1) of the Constitution "does not allow Parliament to single out any individual Constitutional Court judge" on the basis of their individual identity or position within the Court for extension of their term.

[141] Ibid at para 75.

[142] *Glenister II above n 58* at para 249; *Justice Alliance* above n 127 at para 73; and *Helen Suzman Foundation v President of the Republic of South Africa* [2014] ZACC 32; 2015 (2) SA 1 (CC); 2015 (1) BCLR 1 (CC) ("*Helen Suzman Foundation*") at paras 78-82.

[143] *Helen Suzman Foundation* ibid at para 81.

[144] Section 2 of Bill 28B-2023 inserting section 15D(1).

[145] Section 2 of Bill 28B of 2023 inserting section 15D(2).

Bill, however, makes no provision for the removal of the designated judge on account of incapacity or misconduct.

Recommendations

It is recommended that a provision be inserted into RICA providing for the appointment and term of office of designated judges.

- The definition of "designated judge" is RICA is amended to define a designate judge as judge appointed in terms of section 1A of RICA
- Section 1A is inserted to provide for the designation of a designated judge. The Minister must designate a designated judge on the advice of the Judicial Service Commission. This provision is sourced from section 174(6) of the Constitution.
- Section 1A(2) is inserted to provide for the term of office of a designated judge. The term of office is non-renewable and must not exceed a period of seven years. This provision aligns with the Bill.
- Section 1A(3) is inserted to provide for the circumstances in which the term of office of a designated judges comes to an end. This provision is sourced from the Bill, but it goes further than the Bill in that it provides for removal in circumstances of a finding by the Judicial Service Commission that the judge suffers from incapacity, is grossly incompetence, and is guilty of gross misconduct.

Ex parte issue

Introduction

The Constitutional Court's order requires Parliament to establish safeguards to protect the privacy rights of individuals in a process in which surveillance directions are sought and issued without notice being given or a hearing being afforded to the intended subject of surveillance.

Before the Constitutional Court, the AmaBhungane Centre argued that the fact that the intended subject of surveillance is not given any notice or the opportunity of being heard requires some form of adversarial process to ensure that their interests are properly protected and all issues ventilated before an order is made.[146]

The Constitutional Court held that there were inadequate safeguards in RICA to address the fact that surveillance directions are sought and obtained *ex parte*.[147] The Court, however, left the choice of safeguards to Parliament,[148] while recognising that an adversarial process is one possible mechanism by which privacy rights may be adequately safeguarded.[149]

Discussion

One possible mechanism for introducing adversariality – suggested by the Amabhungane Centre – is the introduction of a public advocate who would "represent and advance the interests and rights of the subject of surveillance in order to test the propositions put forward by the law enforcement agencies".[150] The Constitutional Court in *AmaBhungane*, while recognising that the use of public advocates in comparative democracies means that less restrictive means do exist, elected not to comment on the participation of a public advocate as a potential safeguard – preferring to leave the selection of safeguards to Parliament.[151]

The ECHR has, on a number of occasions, recognised the use of some kind of security-cleared advocate as a means of minimising the infringement of the right to a fair hearing in cases where

[146] *AmaBhungane* above n 2 at para 97 sets out the applicant's argument.

[147] Ibid at para 100.

[148] Ibid at para 99.

[149] Ibid at para 99.

[150] Applicant's Heads of Argument, case no CCT 278/19, Constitutional Court,at para 80.1.

[151] *AmaBhungane* above n 2 at para 99.

proceedings are conducted or some evidence is heard in secret.[152] In addition, the Commissioner for Human Rights of the Council of Europe recommends that States consider the introduction of "*security-cleared public interest advocates into surveillance authorisation processes*" to represent the interests of intended subjects of surveillance. [153]

In the context of prior authorisation of surveillance measures, security-cleared advocates are a means to balance legitimate security interests and the right of the intended subjects of surveillance to a fair hearing. A security-cleared advocate is able to challenge the evidence placed before the decision-maker in an application for a surveillance direction without jeopardising the secrecy of the direction sought. However, the effectiveness of security-cleared advocates, in the circumstance where they are unable to consult with or obtain information from the intended subject of the surveillance direction, has been called into question.[154]

A survey of comparative democratic countries reveals different models of security-cleared advocates who are able to represent the interests of an intended subject of surveillance in authorisation proceedings. Most importantly, there is a distinction between systems that require the appointment of an amicus curiae – whose function it is to assist the court – and those that require the appointment of a special advocate – whose function is to represent the interests of the subject of surveillance.

---

[152] *Chahal v UK*, no 22414/93, § 131, ECHR 1997; *A v The United Kingdom*, no 3455/05, § 217, ECHR 2009;; *Tinnelly & Sons Ltd and McElduff v The United Kingdom*, nos 20390/92 and 21322/93, § 78, ECHR 78.

[153] Commissioner for Human Rights, Council of Europe "Democratic and Effective Oversight of National and Security Services" (May 2015) at 12, available at https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb (Commissioner's Recommendations). See also Commissioner for Human Rights, Council of Europe "Positions on Counter-Terrorism and Human Rights Protection" (5 June 2015), available at https://rm.coe.int/16806db6b2.

[154] Venice Commission Report above n 136 at para 226.

In the United States of America, an *amicus curiae* (a friend of the court) is appointed to assist the Foreign Intelligence Surveillance Court in adjudicating applications to conduct foreign surveillance.[155] An *amicus curiae* is appointed to assist the court rather than to specifically represent the intended subject of surveillance.[156] The appointment of an *amicus curiae* is not the default, but occurs only where the FIS Court considers the appointment of an *amicus curiae* to be appropriate.[157]

In the United Kingdom[158] and Canada,[159] special advocates act in the interests of parties excluded from *ex parte* proceedings. The role of a special advocate is to protect the interests of the affected person.[160] Special advocates are the default and do not appear at the discretion of the court. Having received approval from the ECHR, special advocates are now also used in Hong Kong, New Zealand and Australia.[161]

Various authors have identified best practices relating to the way in which security-cleared advocates are used to balance fairness and secrecy. Best practices are those features that maximise fairness to the intended subject of surveillance without unduly jeopardising secrecy and national security.[162]

---

[155] USA Freedom Act 2015 (US Code, Title 50, section 1803(i)).

[156] Jackson "In a World of Their Own: Security-cleared Counsel, Best Practice, and Procedural Tradition" (2019) 46 *Journal of Law and Society* 130.

[157] US Code, Title 50, section 1803(i)(2)(B).

[158] See, for instance, the Special Immigration Appeals Commission Act, 1997 and the Prevention of Terrorism Act, 2005 (repealed).

[159] See, for instance, the Immigration and Refugee Protection Act, 2001.

[160] Hudson and Alati "Behind Closed Doors: Secret Law and the Special Advocate System in Canada" (2019) 44 *Queen's Law Journal* 1 at 12.

[161] Jackson above n 151 at 120.

[162] Ibid at 121; Cole andVladeck "Navigating the Shoals of Secrecy: A Comparative Analysis of the Use of Secret Evidence and 'Cleared Counsel' in the United States, the United Kingdom, and Canada" in Lazarus et al (eds) *Reasoning Rights: Comparative Judicial Engagement* (Bloomsbury, London 2014) at 171.

Most pertinently, the best practices identified include giving security-cleared advocates access to all information on the affected person held by the security agency.[163] The Canadian Supreme Court in *Charkaoui II*,[164] recognised that the efficacy of the special advocate system in Canada depends on special advocates being given access to all information relating to the affected person.[165]

The Bill, however, has not introduced any mechanism to deal with the risks of an ex parte process. The Bill introduces a review judge whose function it is to consider and either confirm, vary or set aside any decision made by a designated judge in terms of RICA.[166] However, it is not clear how the introduction of an automatic review by another judge will resolve the defect identified by the Constitutional Court. The review judge faces the same constraints as a designated judge, as he or she will have only have the same information that was available to the designated judge who issued the surveillance direction.

Recommendations

This thesis recommends the introduction of a special, security-cleared advocate into the process for the authorisation of surveillance directions as a means to resolve the conflict between the right to a fair hearing and national security. The provisions are drawn from Canada's Immigration and Refugee Protection Act, 2001 and the United Kingdom's Special Immigration Appeals Commission Act, 1997.

---

[163] Jackson ibid at S122.

[164] *Charkaoui v Canada (Citizenship and Immigration)* 2008 SCC 38 ("*Charkaoui II*").

[165] Ibid at para 2. The Immigration and Refugee Protection Act has now been amended to limit the scope of the duty of disclosure.

[166] B 28B-2023 section 2 inserting section 15(B) and 15©.

- Sections 23C(1) to (3) are inserted to provide for the appointment of special advocates. The Minister is required, in consultation with the Chief Justice, to publish a list of persons who may act as special advocates in the Government Gazette. The persons listed must be legal practitioners as defined in the Legal Practice Act.[167] The designated judge may appoint a person from the published list to act as a special advocate in any proceedings for a surveillance direction. The special advocate is appointed to protect the interests of the intended subject of surveillance.
- Section 23(4) provides that the applicant for a surveillance direction must provide the special advocate with all the information and other evidence that has been provided to the designated judge as well as with all other information that is within the applicant's possession and that is relevant to the application, but which has not been provided to the designated judge. In this way, the special advocate will have access to information that has not been seen by the designated judge.
- Section 23C(5) provides that the special advocate may make oral or written submissions with respect to the information and other evidence provided to them by the applicant for a surveillance direction.
- Section 23C(6) places restrictions on special advocates relating to the disclosure of information provided to them under subsection (4).

Information management

Introduction

The Constitutional Court declared RICA inconsistent with the Constitution to the extent that it fails to "*adequately prescribe procedures to ensure that data obtained pursuant to the*

[167] Act 28 of 2014.

interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data".[168]

The ECHR in *Weber v Germany* set out six 'minimum safeguards' for the protection of the right to privacy in the context of targeted communications surveillance. Three of the safeguards relate to the proper management of information obtained through surveillance. These safeguards require that the law clearly set out: "the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed".[169]

Discussion

Storage

RICA – as currently formulated – confers a discretion on the Director of the Office for Interception Centres to prescribe the information to be kept by the head of an interception centre as well as the period for and manner in which the information is to be kept.[170] Although the information that must be stored must include "the particulars" relating to applications for surveillance directions and surveillance directions issued as well as "the results obtained from

[168] *AmaBhungane* above n 2 at Order para 6(d).

[169] *Weber and Sanravia v Germany*, no 54934/00, § 95, ECHR 2008 (Weber).

[170] Sections 35(1)(f) and (g) of RICA.

every direction executed at that interception centre",[171] this does not require the actual applications or directions to be stored.[172] These provisions are deleted by the Bill.[173]

The Constitutional Court made it clear that what information must be stored cannot be left to the discretion of any person.[174] It must be prescribed in RICA. The ECHR and the Special Rapporteur on Expression have also emphasised the importance of keeping strict records of interceptions to enable proper oversight and minimise the risk of abuse.[175]

The ECHR's jurisprudence determines that the "mere retention and storage" of private information has a direct impact on the right to privacy "irrespective of whether subsequent use" is made of it.[176] The ECHR has highlighted that information obtained through communications interceptions must be stored securely so as to minimise the risk of the information being accessed by persons other than those contemplated in the law.[177]

RICA should be amended to provide clear details as to what information must be stored as well as where and how the information must be stored.

---

[171] Section 35(1)(f)(ii) of RICA (emphasis added).

[172] *AmaBhungane* above n 2 at para 102.

[173] Section 5 of B 28B-2023 deletes sections 35(f) and (g) of RICA.

[174] Ibid at para 103.

[175] *Roman Zakharov v Russia*, no 47143/06, § 272, ECHR 2015; and Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019) at para 50.

[176] *Trajkovski and Chipovski v North Macedonia*, nos 53205/13 and 63320/13, § 51, ECHR 2020.

[177] *Roman Zakharov* above n 167 at 253; and *Kennedy v The United Kingdom*, no 26839/05, § 163, ECHR 2010.

Use and communication

The ECHR, in *Zakharov v Russia*[178] and in *Kennedy v The United Kingdom*,[179] determined that certain clear rules on the use and communication of intercepted information minimise the risk of unnecessary intrusions into the right to privacy. The rules highlighted by the ECHR include: The information obtained may only be disclosed to persons who have the "appropriate security clearance" and who genuinely "need to know" the information for the performance of their duties; and only the information strictly needed for the performance of the recipient's duties may be disclosed.[180]

RICA should be amended to set out who may have access to information obtained through communications interceptions and under what conditions those persons may have access to the information. It should be made clear that intercepted information may not be shared beyond those who genuinely have a need to know it. RICA should further be amended to provide for steps to ensure that only the information that a person strictly needs to know is disclosed to them. Records should also be required to be kept of who has had access to intercepted information, when and for what purpose so as to minimise the risk of abuses. Limitations should be placed on the copying of intercepted information and records kept of copies made to ensure that the information remains secure.

Deletion

The United Nation High Commissioner for Human Rights has determined that the circumstance in which the information obtained must be deleted should be "*clearly defined, based on strict*

[178] *Roman Zakharov* above n 167.

[179] *Kennedy* above n 169.

[180] *Roman Zakharov* above n 167 at 253 and *Kennedy* idat para 163.

necessity and proportionality".[181] In *Weber v Germany*, the ECHR noted two important factors in reducing the interference with the right to privacy to an "*unavoidable minimum*": the requirement that information be destroyed as soon as it is no longer needed for the purpose for which it was obtained and the requirement that regular reviews of whether the conditions for destruction are met be performed.[182]

In *Zakharov v Russia*, the ECHR determined that any information obtained through interception that is not relevant for the purpose for which the interception was carried out should be destroyed immediately.[183] The retention of irrelevant information is an unjustifiable infringement of the right to privacy.

RICA should be amended to clearly define the circumstances in which intercepted information must be destroyed and to provide for regular reviews of whether the conditions for destruction are met. It should also be amended to provide steps to ensure that irrelevant information gathered through communications interceptions is separated and destroyed immediately.

The Bill – regretfully – does not impose any requirements with respect to information management. Instead, it provides that the procedures to be followed regarding information management must be prescribed in Regulations to be made by the Minister.[184] It then sets out certain principles for the safeguarding of data that must be taken into account in developing these procedures. Given how critical clear provisions on information management are to the

[181] UN Report 2018 above n 67 at para 37.

[182] *Weber* above n 162 at para 132.

[183] *Roman Zakharov* above n 167 at 255.

[184] Section 7 of Bill 28B of 2023 inserting section 37A into RICA.

proper safeguarding of intercepted material, provisions dealing with this should be contained in RICA and not left for subordinate legislation.

Recommendations

It is recommended that a provision be inserted into RICA headed "Management of information". The provisions in section 27A are sourced from the United Kingdom's Investigatory Powers Act, 2016, and the jurisprudence discussed above.

- Section 27A(1) provides clear restrictions on the access to, disclosure of and copying of material obtained under direction issued in terms of RICA.
- Section 27A(2) requires strict record keeping on the persons whom have had access to the material or to whom the material has been disclosured as well as of the copies that have been made of the material.
- Section 27(3) defines the authorised purposes for which material may be retained, used, disclosed, and copied.
- Section 27(4) to (6) requires the deletion of material obtained in terms of a direction issued under the Act immediately if it is not needed for any authorised purpose or as soon as it is no longer needed for any authorised purpose.

Lawyers and Journalists

Introduction

The Constitutional Court's judgment and order requires Parliament to amend RICA to provide additional safeguards when the intended subject of surveillance is a practising lawyer or journalist so as to minimise the risk of infringement of the confidentiality of lawyer-client communication and journalists' sources.

The Court granted extensive reading-in relief which will apply in the interim until such time as the defect in the Act is remedied by Parliament. The interim relief granted by the Court emphasises that the designated Judge must be made aware of the fact that the intended subject of surveillance is a practicing lawyer or a journalist before issuing any surveillance direction or warrant.[185] It imposes a higher standard for the granting of a surveillance direction or warrant where the intended subject is a journalist or practicing lawyer – it may be granted only if the designated Judge is "*satisfied that it is necessary to do so, notwithstanding the fact that the subject is a journalist or practising lawyer*."[186] It also empowers the designated Judge to impose special conditions on the surveillance to protect confidential information.[187]

The Bill largely mirrors the wording of the Constitutional Court's interim reading-in order with one very notable exception.[188] The Bill does not introduce a higher standard for the authorisation of surveillance where the intended subject is a journalist or practicing lawyer. There are a number of other critical safeguards missing from the Bill.

Discussion

The interim relief granted by the Constitutional Court reflects the principles established in the jurisprudence of the ECHR on communications surveillance and professional confidentiality and privilege.

[185] *AmaBhungane* above n 2 at Order para 8(1).

[186] Ibid at Order 8(2).

[187] Ibid at Order 8(3).

[188] Section 3 of B 28B-2023 inserts section 23A headed "*Disclosure that person in respect of whom direction, extension of direction or entry warrant is sought is journalist or practising lawyer".*

The ECHR has set out the general principles on the protection of journalists' sources and lawyer-client communications.[189] The most important safeguard is authorisation by an independent authority who must be provided with sufficient information and material to be in a position to weigh the "potential risks and respective interests".[190] The ECHR has established a higher standard for the authorisation of surveillance where the intended subject is a journalist or a practicing lawyer – there must be a "requirement in the public interest overriding the principle of protection" of professional confidentiality or privilege.[191] The ECHR has also determined that it must be open to the authorising authority to "make a limited or qualified order" so as to protect confidential information from being revealed.[192]

The jurisprudence of the ECHR in this regard has been adopted in legislative reform efforts in comparative democracies. For example, in the United Kingdom, a warrant for the interception of communication that is subject to legal privilege may only be granted if: there are "exceptional and compelling circumstances that make it necessary";[193] the public interest in obtaining the information outweighs the public interest in confidentiality; and there are no other means by which the information may reasonably be obtained.[194]

The interim relief crafted by the Constitutional Court, which follows jurisprudence of the ECHR, should have provided salutary guidance to Parliament regarding the amendments to RICA required to provide additional safeguards where the intended subject is a practicing lawyer or

---

[189] *Big Brother Watch* above n 71 at paras 442-5.

[190] Ibid.

[191] Ibid at para 444 and *Sedletska v Ukraine*, no 42634/18, § 62, ECHR 2021.

[192] *Big Brother Watch* ibid at para 445.

[193] Section 27(4)(a) of the Investigatory Powers Act.

[194] Sections 27(4)(a) and 27(6) of the Investigatory Powers Act.

journalist. Unfortunately, the need for a higher standard for material subject to legal privilege or confidential journalistic material appears to have been missed in the Bill.

There are further additional safeguards necessary to ensure adequate protection for journalistic confidential material and material subject to legal privilege, which were not considered in the Constitutional Court's judgment, and which have been overlooked in the legislative reform process.

First, additional safeguard around information management are required where the information is journalistic confidential material or subject to legal privilege – both at the stage of authorisation of the interception direction and at the stage where it is determined whether to retain information.

Under the United Kingdom's legislative regime, when the interception is authorised, there must be specific arrangements made for the handling, retention, use and destruction of information obtained which is subject to legal privilege or that is confidential journalistic material.[195] The United Kingdom also prescribes additional safeguards regarding information management after information has been intercepted if such information is subject to legal privilege.[196] Information that is subject to legal privilege may only be retained with the authorisation of the Investigatory Powers Commissioner and the Commissioner may impose such conditions as the Commissioner considers necessary for the purpose of protecting the public interest in the confidentiality of information subject to legal privilege.[197]

[195] Section 27(4)(b) and section 28(3) of the Investigatory Powers Act.

[196] Section 55 of the Investigatory Powers Act.

[197] Sections 55(1) to 55(4) of the Investigatory Powers Act.

Second, the focus on lawyers and journalists, as the subject of surveillance directions is too narrow. It ignores the cases in which another person is the subject of the surveillance direction, but communicates with a lawyer or journalist. Special protections ought to apply to confidential or privileged communications sent to lawyers or journalists.

To deal with these cases, RICA should require the interception of legally privileged material or journalistic confidential material to be reported to the designated judge. Access to intercepted communications that are subject to legal privilege or journalistic confidentiality should be made dependent on a prior review carried out by the designated Judge who will be able to limit access to what is strictly necessary for the purpose of attaining the objective of the investigation.[198]

Finally, the Bill also ignores other professions that are equally in need of special protections. The Constitutional Court highlighted that it did not consider other professions that may be equally deserving of special protection, because the issue was not before it.[199] This is something to which Parliament ought to have given consideration. The communications of Members of the National Assembly and provincial legislatures,[200] judges, and human rights defenders are also deserving of special protection. They too perform "social roles which are part and parcel of the fabric of a society".[201]

---

[198] *Kopp v Switzerland*, no 23224/94, § 74, ECHR 1998.

[199] *AmaBhungane* above n 2 at para 120. See also para 121, in which the Constitutional Court declined to consider whether civil society actors are deserving of special protection because it was not in the interests of justice to decide the matter as a court of first instance and because the matter was not properly before it.

[200] See, for instance, section 26 of the United Kingdom's Investigatory Powers Act 2016, which imposes additional safeguards where an order is sought for the interception of a communication sent by or intended for a Member of Parliament.

[201] *AmaBhungane High Court Judgment* above n 75 at para 112.

Recommendations

It is recommended that RICA is amended to insert a new section in the Act headed "*additional safeguards to protect the confidentiality of journalists' sources and legal professional privilege*".

- The inserted section 23A(1) requires disclosure to the designated judge that the intended subject of the surveillance direction is a journalist or practicing lawyer. This provision is sourced from the Bill.
- The inserted sections 23A(2) and (3) require a higher standard for the authorisation of a surveillance direction where the intended subject is a journalist or practicing lawyer. Section 23A(2) introduces a requirement that there must be "*exceptional and compelling circumstances*" that make it necessary to grant the surveillance direction notwithstanding that the subject is a journalist or practicing lawyer. Section 23A(2) clarifies that such exceptional and compelling circumstances only exist where the public interest in obtaining the information outweighs the public interest in the protection of legal privilege or the confidentiality of journalists' sources and where there are no other means by which the information may reasonably be obtained. These provisions are sourced from the Constitutional Court's interim order in *AmaBhungane* and from sections 27 and 28 of the United Kingdom's Investigatory Powers Act.
- The inserted section 23A(4) makes provision for the designated judge to make conditions as may be necessary to protect confidential journalistic material and material subject to legal privilege. This specifically includes conditions relating to the handling, retention, use and destruction of communications. These provisions are drawn from the Bill and section 27 and 28 United Kingdom's Investigatory Powers Act.

- The insert sections 23A(5) to (7) deal with cases in which the subject of a surveillance direction communicates with a journalist or a practicing lawyer. These provisions require the designated judge to be informed, as soon as reasonably practicable, when communications between the subject of a surveillance direction and a journalist or practicing lawyer are intercepted. If the designated judge is not satisfied that there are exceptional and compelling circumstances making it necessary to retain the communication, he or she must direct that the communication is destroyed. If the designated judge is so satisfied, he or she may impose conditions on the handling, retention, use and deletion of the communication. These provisions are drawn from section 55 of the United Kingdom's Investigatory Powers Act.[202]

It is further recommended that RICA is amended to insert a new section into the Act headed: "*Additional safeguard relating to elected representatives, judges and human rights defenders*".

- The additional safeguards introduced in section 23B mirror those relating to journalists and practicing lawyers in sections 23A(1) to (4), but amended as appropriate.
- Section 23B(1) requires disclosure to the designated judge that the intended subject of the surveillance direction is a member of the National Assembly or of a provincial legislature, a judge of the Constitutional Court, the Supreme Court of Appeal or the High Court of South Africa, or a human rights defender.
- Section 23B(2) requires a higher standard for the authorisation of a surveillance direction where the intended subject is an elected representative, judge or human rights defender. The judge must grant the surveillance direction only if satisfied that it necessary to do so, notwithstanding the public interest in the confidentiality of the

[202] See, in particular, section 55 of the Investigatory Powers Act, 2016.

communications of such persons. This standard is not as high as for journalists and practicing lawyers, but nonetheless requires the designated judge to give consideration to the public interest in the confidentiality of the communications.

- Section 23B(3) empowers the designated judge to impose conditions as may in his or her view be necessary to protect the confidentiality of the communications of elected representatives, judges or human rights defenders.
- Section 1 is amended to insert a definition for "human rights defender". The definition of human rights defender is drawn from Article 1 of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms.[203]

CHAPTER FIVE: RECOMMENDATIONS FOR FURTHER LEGISLATIVE REFORMS BEYOND *AMABUNGANE*

The Constitutional Court's order in *AmaBhungane* deals only with the five respects in which RICA is inconsistent with the Constitution that came before the Court for confirmation. A broader comprehensive review of RICA is required in light of the Court's emphasis on the importance of adequate safeguards in the legislation governing communications surveillance to protect the right to privacy. The reform should adopt a human rights centric approach and centre the right to privacy.

[203] Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, 8 March 1999

The Bill, however, does not seek to make any critical amendments to RICA beyond the areas for reform highlighted in the Constitutional Court's judgment and order. In this section, areas for further reform, overlooked in the Bill, are considered.

Transparency

Surveillance by the state

Transparency and openness are founding constitutional values,[204] and are governing principles for the government[205] and the public administration.[206] The Constitution provides that everyone has a right to access any information held by the State.[207] In *Brümmer*, the Constitutional Court noted that the importance of this right cannot be gainsaid "*in a country which is founded on values of accountability, responsiveness and openness".* [208] The Court also held that "*[t]o give effect to these founding values, the public must have access to information held by the State*".[209]

Secrecy facilitates abuses of power and rights violations. The Constitutional Court, in *AmaBhungane*, recognised that the complete secrecy in which communications surveillance under RICA is conducted "*points to a lack of 'mechanisms for accountability and oversight'*".[210]

---

[204] Section 1(d) of the Constitution.

[205] See various provisions of the Constitution: sections 57(1)(b) and section 59(1) (National Assembly); section 72 (National Council of Provinces); sections 116(1)(b) and 118(1)(a) (Provincial Legislatures); and sections 152(1)(a) and (e), section 154(2) and 160(4)(b) (Local Government).

[206] Section 195(1) of the Constitution (Public Administration).

[207] Section 32(1) of the Constitution.

[208] *Brümmer v Minister for Social Development* [2009] ZACC 21; 2009 (6) SA 323 (CC); 2009 (11) BCLR 1075 (CC) at para 62.

[209] Ibid.

[210] *AmaBhungane* above n 2 at para 93, see also paras 39 and 41.

International law requires that States be transparent about the surveillance of private communications. The UN High Commissioner for Human Rights states that—

> "State authorities and oversight bodies should also engage in public information about the existing laws, policies and practices in surveillance and communications interception . . . open debate and scrutiny being essential to understanding the advantages and limitations of surveillance techniques."[211]

The Special Rapporteur on Expression determined that "*States should be completely transparent about the use and scope of communications surveillance techniques and powers*" and that "*States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance*".[212] The United Nations Human Rights Committee's 2016 report on RICA recommends that South Africa "*increase the transparency of its surveillance policy*".[213]

The Global Principles on National Security and the Right to Information ("The Tshwane Principles")[214] aim to provide guidance on the State's authority to withhold information on national security grounds. The Tshwane Principles are based on established international and national law and practices, and were put together by 22 organisations in consultation with over 500 experts, including four special rapporteurs. The Tshwane Principles establish that

[211] UN Report 2018 above n 167.

[212] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013) at para 91.

[213] Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016).

[214] Open Society Justice Initiative "The Global Principles on National Security and the Right to Information", (12 June 2013), available at https://www.justiceinitiative.org/publications (Tshwane Principles).

information about surveillance is of particularly high public interest "*given its special significance to the process of democratic oversight and the rule of law*".[215] It therefore considers that there is a very strong presumption that information about surveillance "*should be public and proactively disclosed*".[216]

On surveillance, the Tshwane Principles provide that "*[t]he public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance*".[217] It notes that this information includes: "*the identity of each government entity granted specific authorization to conduct particular surveillance each year; the number of surveillance authorizations granted each year to each such entity; the best information available concerning the number of individuals and the number of communications subject to surveillance each year; and whether any surveillance was conducted without specific authorization and if so, by which government entity*."[218]

The designated Judge is required to provide annual reports to Parliament's Committee on Intelligence – the Joint Standing Committee on Intelligence.[219] However, the reports provided by the designated Judge have been criticised as lacking the detail and consistency required for

[215] Tshwane Principles at 9.

[216] Ibid at 9 and 10.

[217] See Principle 10: "Categories of Information with a High Presumption or Overriding Interest in Favor of Disclosure" (ibid at 21).

[218] Tshwane Principles at 13.

[219] Section 3(a)(iii) of the Intelligence Services Oversight Act 40 of 1994.

effective public oversight.[220] There are no requirements in the legislative scheme concerning what the designated Judge's reports should contain.

The Necessary and Proportionate Principles – that framework of the UN Human Rights Council, discussed above – contain detailed guidance as to what should be included in transparency reports. Reports should include the following:

- "total number of each type of request, broken down by legal authority and requesting State actor, be it an individual, government agency, department, or other entity, and the number of requests under emergency procedures;
- total number and types of responses provided (including the number of requests that were rejected);
- total numbers for each type of information sought;
- total number of users and accounts targeted;
- total number of users and accounts affected;
- total number of times delays in notification were requested, the number of times that a delay was granted, and the number of times a delay was extended;
- compliance rate, provided as a percentage of total requests received and total requests complied with;
- legal challenge rate, provided as a percentage of total requests received and total challenged;
- number of investigations into filed complaints and the results of those investigations; and

[220] Mutung'u "South Africa Country Report" in Roberts *Surveillance Law in Africa: a Review of Six Countries* (Institute of Development Studies 2021); citing Duncan *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (Wits University Press, Johannesburg 2018) at 93.

- remedies ordered and/or actions taken in response to any investigations."[221]

Effective public oversight requires the release of sufficient and precise information to enable the public to assess where surveillance powers are being used lawfully and in a manner that is necessary and proportionate. It is also essential that the information "be explained quantitatively as well as qualitatively" so that the way in which communications surveillance is conducted is easy to understand.[222]

Communications service providers

The rights in the Bill of Rights apply horizontally[223] – imposing obligations on natural and juristic persons – and the right of access to information in section 32 expressly includes the right of access to any information that is held by "*another person*" (i.e. other than the state) and that is "*required for the exercise or protection of any rights*".[224] This has been interpreted as conferring a right of access to information held by "*any person*" and thus operating within "a wide and potently encompassing field".[225]

International law clearly requires that communications service providers be able to publicly disclose information about State requests for access to information held by them. The UN General Assembly has passed a resolution calling on States "*[t]o take steps to enable business enterprises to adopt adequate voluntary transparency measures with regard to*

[221] Electronic Frontier Foundation above n 74 at 33-4.

[222] Ibid.

[223] Section 8(2) of the Constitution.

[224] Section 32(1)(b) of the Constitution.

[225] *My Vote Counts NPC v Speaker of the National Assembly and Others* [2015] ZACC 31 ("*My Vote Counts I*") at para 106 (minority judgment of Cameron J).

requests by State authorities for access to private user data and information".[226] This is echoed by the UN Human Rights Council.[227] The Special Rapporteur on Expression has determined that States should enable service providers to "*publish records of State communications surveillance*."[228] The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet has similarly determined that service providers should be able to publicly disclose "*information on at least the types of requests they receive and the number of requests*".[229] RICA prohibits communications service providers, including telecommunications companies, from publicly disclosing any information on surveillance directions issued in terms of the Act or the fact that a communication has been intercepted or communication-related information has been provided.[230] This even precludes the publication of aggregated statistics relating to the interception of communications and the provision of communication-related information.[231] Preventing communications service providers from publicly disclosing this information precludes the public from gaining access to information about how RICA is being implemented.[232] This contributes to a "circle of secrecy" around communications surveillance

[226] UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020) at para 7.

[227] UN Resolution 2021 at para 6.

[228] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013) at para 92.

[229] The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013) at para 169.

[230] Sections 42(2) and (3) of RICA.

[231] Mare "An Analysis of the Communications Surveillance Legislative Framework in South Africa" *Media Policy and Democracy Project* (November 2015) at 26.

[232] Right2Know "The Surveillance State: Communications Surveillance and Privacy in South Africa" *Media Policy and Democracy Project* (March 2016) at 26.

in South Africa.[233] RICA should be amended to enable communications service providers to publish aggregate information on the orders that they receive for interception of communications and provision of communication-related information.[234] All communications service providers should publish transparency reports at regular intervals.[235] Moreover, communication service providers must be required to make detailed information on the surveillance orders that they receive available to all oversight bodies.

ACCOUNTABILITY AND OVERSIGHT

Accountability, which is closely linked to transparency, is similarly a foundational constitutional value.[236] Effective oversight is necessary to ensure that the State "remains accountable to those on whose behalf it exercises power".[237] The primary purpose of oversight mechanisms fostering accountability is to avoid the misuse of power.[238] This is particularly critical where State officials exercise power in conditions of secrecy, as is the case with communications surveillance.

The UN General Assembly and Human Rights Council have both emphasized the importance of "*independent, effective, adequately resourced and impartial*" oversight mechanisms "*capable of ensuring transparency, as appropriate, and accountability for State surveillance of*

[233] Ibid.

[234] Eskens et al "10 Standards for Oversight and Transparency of National Intelligence Services" *Journal of National Security Lax* 8 (2016) 553 at 553-4.

[235] Mare "Communication Surveillance in Namibia: an Exploratory Study" *Media Policy and Democracy Project* (November 2019) at 28.

[236] Section 1(d) of the Constitution.

[237] *Khumalo v MEC for Education, KwaZulu-Natal* [2013] ZACC 49; 2014 (5) SA 579 (CC); 2014 (3) BCLR 333 (CC) at para 29.

[238] Venice Commission report above n 136 at para 76.

communications".[239] The Special Rapporteur on Privacy similarly recommends the establishment of oversight bodies to carry out an effective review of "any privacy-intrusive activities" carried out by the State.[240] The UN High Commissioner for Human Rights has determined that there should be independent oversight bodies to "proactively investigate and monitor" the conduct of communications surveillance.[241]

Intelligence services should be subject to a range of types of accountability. [242] The UN Good Practices on Oversight Institutions provide that intelligence services should be overseen by a "*combination of executive, parliamentary, the judicial and specialised oversight institutions*".[243] The combined mandates of oversight bodies must cover "*all aspects of the work of intelligence services*" including the lawfulness and the effectiveness of their activities.[244] Civil society and the media also contribute to accountability by playing a monitoring role.

The UN Good Practices on Oversight Institutions provide that oversight institutions should have "*the power, resources and expertise to initiate and conduct their own investigations and have full and unhindered access to the information, officials and installations necessary to fulfil their mandates*".[245]

---

[239] UN Resolution 2014 at para 4 and UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019) at para 6.

[240] Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (16 October 2019) at para 46.

[241] UN Report 2018 above n 67 at para 40.

[242] Venice Commission report above n 136 at para 73.

[243] Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism "Compilation of Good Practices for Intelligence Agencies and their Oversight" *Geneva Centre for the Democratic Control of Armed Forces* (5 August 2011) (Good Practices)at 10 (Practice 6).

[244] Good Practices ibid and Eskens et al above n 220 (Standard 1).

[245] Good Practices ibid (Practice 7) and Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, UN Doc A/HRC/16/51/Add.3 (15 December 2010) (Scheinin Report).

The existing law in South Africa provides for the following oversight mechanisms:

- Parliamentary oversight conducted by the Joint Standing Committee on Intelligence; and
- Office of the Inspector General of Intelligence, which is empowered to monitor the civilian intelligence services.[246]

While there are oversight mechanisms for the implementation of RICA in place, these mechanisms need to be strengthened to ensure effective oversight.

Independent reporting mechanism

The UN High Commissioner has emphasised the importance of oversight be "institutionally separated" from authorisation.[247] The reports on RICA provided to the Joint Standing Committee on Intelligence for parliamentary oversight are produced by the designated Judge. There is accordingly inadequate separation between oversight and authorisation. The reports on State surveillance of communications in terms of RICA are produced by the same authority who hears applications for and issues surveillance directions. Duncan has raised concerns that the reports could be partial and purely statistical instead of analytic as a result.[248] RICA should be amended to provide for an independent reporting mechanism.[249] It is critical that this independent reporting mechanism be provided with all the information necessary to perform effective oversight.

[246] The Office of the Inspector General of Intelligence is established in terms of the Intelligence Services Oversight Act.

[247] UN Report 2018 above n 68 at para 40.

[248] Duncan above n 207, cited in Mutung'u above n 207 at 178.

[249] Mutung'u ibid at 173.

Judicial oversight

International law requires that surveillance measures not only be authorised by an independent authority, but also be supervised and reviewed by an independent authority. The United Nations High Commissioner for Human Rights has determined that "*[s]urveillance measures … 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 they have been terminated*."[250]

The ECHR has on numerous occasions held that supervision by an independent authority should occur at three stages: "*when the surveillance is first ordered, while it is being carried out, or after it has been terminated*".[251] In *Big Brother Watch*, the ECHR stated that—

> "the process must be subject to 'end-to-end safeguards', meaning that . . . an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken."[252]

On-going oversight

RICA provides that the designated Judge who issued a surveillance direction or warrant may require the applicant to report to him or her at intervals on the progress that has been made towards achieving the objectives of the direction or warrant or any other matter.[253] However, this does not go far enough. RICA does not expressly require the designated Judge to supervise the surveillance measures authorised in terms of the Act.

---

[250] UN Report 2018 at para 39.

[251] *Liblik v Estonia*, nos 173/15 and 5 others, § 130, ECHR 2019. and *Klass v Germany*, no 5029/71, ECHR 1978.

[252] *Big Brother Watch* above n 71 at para 350.

[253] Section 24 of RICA.

As explained by Judge Pinto de Albuquerque in *Big Brother Watch*—

> "Judicial oversight should not stop at the start of the operation of the interception. Were the actual operation of the system of interception hidden from the judge's oversight, the initial intervention of a judge could be easily undermined and deprived of any real effect, rendering it a merely virtual, deceptive safeguard. On the contrary, the judge should accompany the entire process, with a regular and vigilant examination of the necessity and proportionality of the interception order, in view of the intercept data obtained."[254]

To adequately safeguard the right to privacy, RICA needs to be amended to require the designated Judge to supervise the execution of all surveillance directions and warrants issued by the Judge to ensure that these measures are carried out in compliance with the surveillance directions and warrants and are necessary and proportionate.

The separate stages of surveillance, including the collection, storage and use of intercepted communications, should be subject to the oversight of the designated Judge.[255] The designated Judge, who provides on-going oversight, must have the power to end a surveillance measure.[256] RICA does empower the designated judge to cancel a surveillance direction or warrant where she is not provided with a report on progress or where she is satisfied that the objectives of the direction or warrant have been achieved.[257]

[254] Ibid at para 26 (emphasis added).

[255] Eskens et al above n 220 at 553-4 (Standard 2).

[256] Ibid (Standard 5).

[257] Section 25 of RICA.

After-the-fact oversight

RICA makes no provision for an automatic review of surveillance measures after they have come to an end. The Constitutional Court in *Amabhungane* considered that automatic judicial review through an inexpensive, speedy and effective process may be necessary to protect the right to privacy from unnecessary invasions.[258] The Court was of the view that post-surveillance notification on its own is not likely to adequately safeguard the right to privacy.[259] This is because most people in South Africa are not able to afford to approach the courts to vindicate their right to privacy.[260]

Although the Court did not find that the absence of a mechanism for automatic review renders RICA inconsistent with the Constitution,[261] the Court recommended automatic review as a possible safeguard to be adopted to ensure that the communications surveillance system sufficiently safeguards the right to privacy.[262] The Court suggested that this could be in the form of automatic review in an informal process.[263] The Court, however, stated that the details of an automatic review process, if adopted, should be left to Parliament.[264]

[258] *AmaBhungane* above n 2 at paras 49-52.

[259] Ibid.

[260] Ibid at para 49.

[261] Ibid at para 52.

[262] Ibid at para 54.

[263] Ibid at para 49.

[264] Ibid.

In *Big Brother Watch*, Judge Pinto de Albuquerque stated that the *ex post facto* review should be triggered by the notification to the subject of surveillance, and that the review should take place in a "fair and adversarial judicial procedure".[265]

The Constitutional Court's judgment makes it clear that the automatic review that it envisage is one in which the subject of the surveillance would be able to participate in some meaningful way. It says "*Automatic review is a complementary mechanism tied to notification*".[266]

RICA should be amended to create a mechanism for automatic review of surveillance measures as soon as notification has been provided to the subject of surveillance. It is recommended that a specialist tribunal be established to carry out this review function.[267]

The subject of the surveillance should also be entitled to make representations to the tribunal to ensure a fair procedure. In review proceedings, State agencies are likely to justify the non-disclosure of certain information to the subjects of surveillance on the grounds of national security. This thesis therefore recommends the appointment of special, security-cleared advocates, who will have access to all relevant information, to assist the subject of surveillance in review proceedings before the tribunal. Special, security-cleared advocates are considered to be most effective in adversarial proceedings where the surveillance measure is known to the subject, but some information cannot be disclosed to the subject.[268]

---

[265] *Big Brother Watch* above n 71at paras 17 and 27.

[266] AmaBhungane at para 52.

[267] McIntyre "Judicial Oversight of Surveillance: the Case of Ireland in Comparative Perspective" in Scheinin et al (eds) *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar Publishing, Cheltenham 2016) and Venice Commission report above n 136 at para 260.

[268] Venice Commission report above n 136 at para 226.

A specially tailored tribunal – with assistance of special advocates – is particularly useful in this context – given the sensitive nature of the information involved.

Effective remedies

The Constitution requires that subjects of surveillance have access to an appropriate remedy for unlawful or wrongful invasions of their right to privacy.[269] This was recognised by the Constitution Court in *AmaBhungane*.[270] The jurisprudence of the Constitutional Court makes it clear that "an appropriate remedy" requires effective relief.[271]

The ECHR, in *Big Brother Watch*, explained the relevance of the powers that an authority possesses to determining whether a remedy is effective.[272] It emphasised that the decisions of the authority must be legally binding,[273] and that the authority must have the power to order the cessation of unlawful surveillance measures and the destruction or deletion of any information obtained or stored unlawfully.[274] International human rights bodies and experts have similarly emphasised that an effective remedy must be capable of ending on-going rights violations and effectively vindicating the right violated.[275]

---

[269] Section 38 of the Constitution.

[270] *AmaBhungane* above n 2 at paras 44 and 48.

[271] *Fose v Minister of Safety and Security* [1997] ZACC 6; 1997 (3) SA 786 (CC); 1997 (7) BCLR 851 (CC) at para 69.

[272] *Big Brother Watch* above n 71 at para 359.

[273] Ibid. See also *Segerstedt-Wiberg v Sweden*, no. 62332/00, § 120, ECHR 2006 and also *Leander v Sweden*, no 9248/81, § 81-3, ECHR 1987, where the inability to make legally binding decisions undermined the effectiveness of the remedy offered.

[274] *Big Brother Watch* above n 71 at para 359.

[275] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014) at para 41 and Commissioner's Recommendations above n 148 at para 12.

While RICA imposes sanctions for unlawful surveillance, it does not provide any remedies to persons unlawfully surveilled. A subject of surveillance has access to remedies in terms of the common law and a court's broad just and equitable remedial discretion in terms of section 172(1)(b) of the Constitution. However, these remedies are only available in proceedings before a court.

The specialist tribunal imbued with the power to review surveillance measures after-the-fact must have the power to declare a measure unlawful and to provide for redress if it finds that the measures are being / have been carried out unnecessarily or disproportionately, or in a manner that does not comply with the surveillance direction.[276]

Parliament should amend RICA to confer remedial powers on the authority tasked with automatically reviewing surveillance measures as well as on courts in proceedings reviewing surveillance measures. They should have the power to make any order that is just and equitable, including orders directing: the cessation of any unlawful surveillance activities; the destruction or deletion of unlawfully obtained or stored information; and the payment of compensation.

Access to information

It is not only notification of the fact that a subject has been surveilled that is needed to enable the subject of surveillance to exercise their right of access to courts and to an effective remedy.[277] Information about the surveillance is also necessary to put the subject in a position to assess whether the surveillance may have been unlawful or wrongful and, if this appears to

[276] Eskens et al above n 220 (Standard 5).

[277] Sections 34 and 38 of the Constitution.

be the case, to challenge the surveillance and obtain an effective remedy. The Constitutional Court's judgment in *AmaBhungane* makes it clear that information about surveillance is required for the subject to make "*an informed decision whether to litigate for the vindication of rights*".[278]

The ECHR has held that remedies are only available to "persons who are in possession of information about the interception of their communications".[279] The effectiveness of any available remedies is undermined by the absence of "*an adequate possibility to request and obtain information about interceptions from the authorities*".[280] A legal scheme that does not provide an adequate opportunity to access information about surveillance does not provide an effective remedy against wrongful or unlawful surveillance.[281]

The subject of surveillance should be provided with information about the surveillance once the subject has been notified of the surveillance. This is supported by the jurisprudence of the ECHR, which repeatedly emphasises that "*as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned*."[282]

RICA neither requires any information about surveillance to be provided to the subjects of surveillance nor provides a mechanism for subjects to request and obtain any information about the surveillance even after the surveillance has come to an end. RICA prohibits and

---

[278] *AmaBhungane* above n 2 at para 103.

[279] *Roman Zakharov* above n 167 at para 298.

[280] Ibid.

[281] Ibid.

[282] *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*,no 62540/00, § 90, ECHR 2007 (emphasis added). See also *Weber* above n 162 at para 135.

criminalises the disclosure of "*any information*" about surveillance directions or about the interception of communications or provision of communication-related information.[283]

The only mechanism available to subjects to obtain information once notified that they have been surveilled is a request for information in terms of the Promotion of Access to Information Act.[284] However, the state may refuse to provide access to information under certain grounds listed in PAIA, which may frustrate efforts to obtain information.[285] The subject of surveillance may be able to obtain information through the mechanism contained in Rule 53 of the Uniform Rules of Court, if they launch a review of the decision in the High Court. The same restrictions on access to information do not apply to information to be provided as part of the record of a decision under Rule 53. However, this requires the subject of surveillance to launch a review application in the High Court at great expense. As explained above, many subjects of surveillance may not be able to vindicate their rights by accessing a court. Access to information should thus be specifically regulated under RICA to provide sufficient specificity and clarity as to what information should be provided to the subject of surveillance.

The Constitutional Court's judgment sets out the information that a subject of surveillance requires to exercise their fundamental rights.[286] This information includes the applications for any surveillance directions, the surveillance directions issued and the results of the surveillance.[287] Parliament should amend RICA to clearly set out that the subject of surveillance

[283] Sections 42(1), 42(3) and 51 of RICA.

[284] Act 2 of 2000.

[285] See sections 34 to 45 of PAIA.

[286] *AmaBhungane* above n 2 at para 103.

[287] Ibid at para 103.

is entitled to this information as soon as notification of the surveillance has been given and to create a mechanism for subjects to request and obtain any further information.

Access to reasons

RICA empowers the designated Judge to issue various surveillance directions. However, nowhere does RICA require the designated Judge to give reasons for his or her decision to issue a surveillance direction.

In addition to information about the surveillance, the reasons given by the designated Judge are critical to enable the subject of surveillance to determine whether the surveillance direction unnecessarily intrudes upon their right to privacy and, if this appears to be the case, to challenge the direction.

The ECHR has made it clear that the provision of "*relevant and sufficient reasons*" for the decision to authorise surveillance measures by the relevant judicial authority is an essential safeguard to protect the right to privacy.[288] In *Liblik v Estonia*, the ECHR stated that the requirement to set out the relevant reasons in decisions authorising surveillance measures is an important safeguard "*ensuring that the measures are not ordered haphazardly, irregularly or without due and proper consideration*".[289] In the same case, the ECHR emphasised the importance of giving reasons at the initial authorisation stage.[290] The provision of reasons after surveillance has been authorised and carried out undermines the effectiveness of the

[288] *Berlizev v Ukraine*, no 43571/12, § 40, ECHR 2021 and *Hambardzumyan v Armenia*, no. 43478/11, § 26 and 43-4, ECHR 2019.

[289] *Liblik* above n 244 at para 136.

[290] Ibid at para 140.

obligation to provide reasons.[291] It also, of course, introduces the risk of after-the-fact reasons being generated.

Parliament should amend RICA to clarify that the designated Judge is required to provide reasons for his or her decisions granting surveillance directions and that such reasons are to be provided at the time of authorisation. Moreover, the subject of surveillance should be entitled to the designated Judge's reasons, together with the information detailed above, as soon as notification of the surveillance has been given.

CONCLUSION

It is clear that RICA falls short of the robust legal framework required to adequately guard against arbitrary and unlawful intrusions into the privacy of our communications. The judgment and order of the Constitutional Court in *Amabhungane* provides a good starting point for a significant law reform effort. However, more comprehensive reforms are required to ensure that the right to privacy is adequately safeguarded.

[291] Ibid at para 141.

APPENDIX I

REPUBLIC OF SOUTH AFRICA

REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION AMENDMENT BILL, 2024

GENERAL EXPLANATORY NOTE:

[ ] Words in bold type in square brackets indicate omissions from existing enactments.

_____Words underlined with a solid line indicate insertions in existing enactments.

BILL

*To amend the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, so as to insert certain definitions; to provide for the designation and tenure of independent designated judges; to provide for adequate safeguards to protect the confidentiality of journalists' sources and legal professional privilege; to provide for adequate safeguards where the subject of surveillance i***s** *an elected representative, a judge or a human rights defender; to provide for the appointment of special advocates to protect the interests of the intended subject of surveillance; to provide for post-surveillance notification; to provide for procedures to be followed for processing, examining, copying, sharing, disclosing, sorting through, using, storing or destroying of any data; and to provide for matters connected therewith.*

PARLIAMENT of the Republic of South Africa enacts, as follows: —

Amendment of section 1 of Act 70 of 2002, as amended by section 1 of Act 48 of 2005, as amended by section 97 of Act 36 of 2005, as amended by section 36 of Act 1 of 2011 and section 53 of Act 11 of 2013

1. Section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002) (hereinafter referred to as the ''principal Act''), is hereby amended—

(a) by the substitution for the definition of ''designated judge'' of the following definition:

''**designated judge'** means any judge of a High Court discharged from active service under section 3(2) of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act 47 of 2001), or any retired judge, who is appointed in terms of section 1A of this Act to perform the functions of a designated judge for purposes of this Act'';

(b) by the insertion after the definition of ''fund'' of the following definition:

"**human rights defender**" means a person who individually and in association with others, acts to promote and to strive for the protection and realization of human rights and fundamental freedoms at the national and international levels."

Insertion of section 1A in Act 70 of 2002

2. The following sections are hereby inserted after section 1 of the principal Act:

"**Designated judge**

1A. (1) The Minister must designate a judge as contemplated in section 1 as a designated judge on the advice of the Judicial Services Commission, by notice in the Gazette.

(2) The tenure of a designated judge is for a non-renewable period not exceeding seven years.

(3) The designation of a judge contemplated in subsection 1 comes to an end upon the—

(a) completion of the period contemplated in subsection 2;

(b) acceptance by the Minister, in consultation with the Chief Justice, of a request to resign; or
(c) death of the judge; or
(d) the Judicial Service Commission finds that the judge suffers from an incapacity, is grossly incompetent or is guilty of gross misconduct."

Insertion of Chapter 3A in Act 70 of 2002

3. The following sections are hereby inserted after section 23 of the principal Act:

"**Additional safeguards to protect the confidentiality of journalists' sources and legal professional privilege**

23A. (1) Where the person in respect of whom a direction, extension of a direction or entry warrant is sought in terms of section 16, 17, 18, 19, 20, 21, 22 or 23, whichever is applicable, is a journalist or practising lawyer, the application must disclose to a designated judge the fact that the intended subject of the direction, extension of a direction or entry warrant is a journalist or practising lawyer.
(2) The designated Judge must grant the direction, extension of a direction or entry warrant referred to in subsection (1) only if satisfied that there are exceptional and compelling circumstances that make it necessary to do so, notwithstanding the fact that the subject is a journalist or practising lawyer.
(3) For the purposes of subsection (2), there cannot be exceptional and compelling circumstances that make it necessary to grant the direction, extension of a direction or entry warrant referred to in subsection (1) unless–
(a)the public interest in obtaining the information that would be obtained outweighs the public interest in the protection of the confidentiality of journalists' sources or legal professional privilege; and
(b)there are no other means by which the information may reasonably be obtained.
(4) If a designated judge issues the direction, extension of a direction or entry warrant, she or he may do so subject to such conditions as may be necessary, in the case of a journalist, to protect the confidentiality of her or his sources, or, in the case of a practising lawyer, to protect the legal professional privilege enjoyed by her or his clients, including specific arrangements for the handling, retention, use and destruction of intercepted communications.
(5) Where the subject of a direction issued under this Act communicates with a journalist or practicing lawyer, the law enforcement officer who executes the direction must, as soon as is reasonably practicable, inform a designated judge of the interception of any communication that may compromise the confidentiality of journalists' sources or legal professional privilege.
(6) Unless the designated judge considers that exceptional and compelling circumstances, as contemplated in subsections 2 and 3, make it necessary to retain the communication referred to in subsection 5, he or she must direct that the item is destroyed.
(7) If the designated judge considers that exceptional and compelling circumstances, as contemplated in subsections 2 and 3, make it necessary to retain the communication referred to in subsection 5, he or she may impose conditions, as may be necessary, on the handling, retention, use and deletion of the communication.

Additional safeguards relating to elected representatives, judges and human rights defenders

23B. (1) Where the person in respect of whom a direction, extension of a direction or entry warrant is sought in terms of section 16, 17, 18, 19, 20, 21, 22 or 23, whichever is applicable, is –

(a) A member of the National Assembly or a provincial legislature;

(b) A judge of the Constitutional Court, Supreme Court of Appeal or High Court of South Africa; or

(c) A human rights defender,

the application must disclose to a designated judge the fact that the intended subject of the direction, extension of a direction or entry warrant is such a person.

(2) The designated Judge must grant the direction, extension of a direction or entry warrant referred to in subsection (1) only if satisfied that it necessary to do so, notwithstanding the public interest in the confidentiality of the communications of the persons referred to in subsection (1)(a), (b) and (c).

(3) If a designated judge issues the direction, extension of a direction or entry warrant, she or he may do so subject to such conditions as may be necessary to protect the confidentiality of the communications of the persons referred to in subsection (1)(a), (b) and (c), including specific arrangements for the handling, retention, use and destruction of intercepted communications."

The appointment of special advocates to safeguard the interests of the intended subject of surveillance

23C. (1) The Minister shall, in consultation with the Chief Justice, publish a list of persons who may act as special advocates by notice in the Gazette.

(2) For the purposes of subsection (1), only a legal practitioner as defined in Legal Practice Act 28 of 2014 may act as a special advocate.

(3)The designated judge must appoint a person from the list referred to in subsection 1 to act as a special advocate to protect the interests of the intended subject of surveillance in any proceedings for a direction, extension of a direction or entry warrant in terms of section 16, 17, 18, 19, 20, 21, 22 or 23.

(4) An applicant for a direction, extension of a direction or entry warrant referred to in subsection (3) shall within a period set by the designated judge –

(a) provide the special advocate with a copy of all the information and other evidence that is relevant to the application, on which the application is based and that has been provided to the designated judge; and

(b) provide the special advocate with a copy of any other the information that is within the applicant's possession and that is relevant to the application, but on which the application is not based and that has not been provided to the designated judge.

(5)A special advocate may make oral and written submissions with respect to the information and other evidence provided by the applicant for a direction, extension of a direction or entry warrant referred to in subsection (3).

(6) No person shall disclose any information or other evidence that is disclosed to them under subsection (4) and that is confidential."

Insertion of section 25A in Act 70 of 2002

4. The following section is hereby inserted after section 25 of the principal Act:

‘‘**Post-surveillance notification**

25A. (1) Within 90 days of the date of expiry of a direction or extension thereof issued in terms of section 7, 8, 16, 17, 18, 19, 20, 21 or 23, whichever is applicable, the applicant that obtained the direction or, if not available, any other law enforcement officer within the law enforcement agency concerned must notify, in writing, the person who was the subject of the direction and, within 15 days of doing so, certify in writing to a designated judge, Judge of a High Court, Regional Court Magistrate or Magistrate that the person has been so notified.
(2) If the notification contemplated in subsection (1) cannot be given without jeopardising the purpose of the surveillance, a designated judge, Judge of a High Court, Regional Court Magistrate or Magistrate may, upon application by a law enforcement officer, direct that the giving of notification in that subsection be withheld for a period which must not exceed 90 days at a time or two years in aggregate.”

Insertion of section 37A in Act 70 of 2002

5. The following section is hereby inserted after section 37 in the principal Act:

‘‘**Management of information**

27A. (1) Arrangements must be in force for material obtained under a direction issued in terms of this Act to ensure that each of the following is kept to the minimum that is necessary for the authorised purposes referred to in subsection (3) —
(a) the number of persons to whom any of the material is disclosed or otherwise made available;
(b) the extent to which any of the material is disclosed or otherwise made available;
(c) the extent to which any of the material is copied;
(d) the number of copies that are made.
(2) Records must be kept of the following:
(a) the type of material that is retained;
(b) the persons whom had access to any of the material;
(b) the persons to whom any of the material is disclosed or otherwise made available; and
(d) the number of copies that are made and the manner of storage of all copies.
(3)For the purposes of this section something is necessary for the authorised purposes if, and only if—
(a) it is, or is likely to become, necessary on any of the grounds on which a direction or extension is issued in terms of section 16, 17, 18, 19, 20, 21 or 23;
(b) it is necessary for facilitating the carrying out of any functions under this Act of the applicant for a direction issued in terms of this Act;
(c) it is necessary for facilitating the carrying out of any functions of a designated judge in relation to this Act; or

(4) Any material obtained under a direction issued in terms of this Act that is not needed for the purposes for which the direction was issued or for any of the authorised purposes in subsection (3) must be destroyed immediately.
(5) Every copy made of any of material obtained under a direction issued (if not destroyed earlier) must be destroyed as soon as there are no longer any relevant grounds for retaining it.
(6) There are no longer any relevant grounds for retaining a copy of any material if:

(a) the retention is no longer necessary, and is not likely to become necessary, for any of the purposes for which the direction was issued; and
(b) the retention is no longer necessary for any of the authorised purposes referred to in subsection (3).”

BIBLIOGRAPHY

South African legislation

1. Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002.
2. Criminal Procedure Act 51 of 1977.
3. Electoral Commission Act 51 of 1996.
4. Intelligence Services Oversight Act 40 of 1994.

International treaties

1. Convention on the Rights of the Child, 20 November 1989.
2. International Covenant on Civil and Political Rights, 16 December 1966.
3. Universal Declaration on Human Rights, 10 December 1948.

Foreign legislation

1. Act on Communications Interception for Criminal Investigation Act 137 of 1999 (Japan).
2. Canadian Criminal Code, RSC, 1985, c. C-46 (Canada).
3. Code of Laws of the United States of America, Title 18 (USA).
4. Code of Laws of the United States of America, Title 50 (USA).
5. Immigration and Refugee Protection Act, 2001 (Canada).
6. Intelligence and Security Act 2017 (New Zealand).
7. Investigatory Powers Act 2016 (UK).

8. Prevention of Terrorism Act, 2005 (UK).

9. Special Immigration Appeals Commission Act, 1997 (UK).

South African cases

1. *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* [2021] ZACC 3; 2021 (3) SA 246 (CC); 2021 (4) BCLR 349 (CC).
2. *Amabhungane Centre for Investigative Journalism NPC v Minister of Justice* 2020 (1) SA 90 (GP).
3. *Bernstein v Bester NNO* [1996] ZACC 2; 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC).
4. *Brümmer v Minister for Social Development* [2009] ZACC 21; 2009 (6) SA 323 (CC); 2009 (11) BCLR 1075 (CC).
5. *Case and Another v Minister of Safety and Security; Curtis v Minister of Safety and Security* [1996] ZACC 7; 1996 (3) SA 617; 1996 (5) BCLR 608.
6. *Fose v Minister of Safety and Security* [1997] ZACC 6; 1997 (3) SA 786 (CC); 1997 (7) BCLR 851 (CC).
7. *Gaertner v Minister of Finance* [2013] ZACC 38; 2014 (1) SA 442 (CC); 2014 (1) BCLR 38 (CC).
8. *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Limited In re: Hyundai Motor Distributors (Pty) Limited v Smit NO* [2000] ZACC 12; 2001 (1) SA 545 (CC); 2000 (10) BCLR 1079 (CC).
9. *Glenister v President of the Republic of South Africa* [2011] ZACC 6; 2011 (3) SA 347 (CC); 2011 (7) BCLR 651 (CC).

10. *Helen Suzman Foundation v President of the Republic of South Africa* [2014] ZACC 32; 2015 (2) SA 1 (CC); 2015 (1) BCLR 1 (CC).
11. *Justice Alliance of South Africa v President of Republic of South Africa*[2011] ZACC 23; 2011 (5) SA 388 (CC); 2011 (10) BCLR 1017 (CC).
12. *Khumalo v Holomisa* [2002] ZACC 12; 2002 (5) SA 401 (CC); 2002 (8) BCLR 771 (CC).
13. *Khumalo v MEC for Education, KwaZulu-Natal* [2013] ZACC 49; 2014 (5) SA 579 (CC); 2014 (3) BCLR 333 (CC).
14. *Minister of Home Affairs v National Institute for Crime Prevention and the Reintegration of Offenders (NICRO)* [2004] ZACC 10; 2005 (3) SA 280 (CC); 2004 (5) BCLR 445 (CC) ("*NICRO*").
15. *Mistry v Interim National Medical and Dental Council of South Africa* [1998] ZACC 10; 1998 (4) SA 1127 (CC); 1998 (7) BCLR 880 (CC).
16. *My Vote Counts NPC v Speaker of the National Assembly and Others* [2015] ZACC 31
17. *National Coalition for Gay and Lesbian Equality v Minister of Justice* [1998] ZACC 15; 1999 (1) SA 6 (CC); 1998 (12) BCLR 1517 (CC).
18. *NM v Smith* [2007] ZACC 6; 2007 (5) SA 250 (CC); 2007 (7) BCLR 751 (CC).
19. *Public Servants Association of South Africa and Others v Government Employees Pension Fund and Others* [2020] 4 All SA 710 (SCA)
20. *S v Mamabolo (E TV Intervening)* [2001] ZACC 17; 2001 (3) SA 409 (CC); 2001 (5) BCLR 449 (CC).
21. *Sonke Gender Justice NPC v President of the Republic of South Africa* [2020] ZACC 26; 2021 (3) BCLR 269 (CC).

Decisions of regional and foreign courts

1. *A v The United Kingdom*, no 3455/05, ECHR 2009.
2. *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*,no 62540/00, ECHR 2007.
3. *Berlizev v Ukraine*, no 43571/12, ECHR 2021.
4. *Big Brother Watch v The United Kingdom*, nos 58170/13 and 2 others, ECHR 2021.
5. *Chahal v UK*, no 22414/93, ECHR 1997.
6. *Charkaoui v Canada (Citizenship and Immigration)* 2008 SCC 38.
7. *Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources*, nos 293/12 and 594/12, ECHR 2014.
8. *Hambardzumyan v Armenia*, no. 43478/11, ECHR 2019.
9. *Kennedy v The United Kingdom*, no 26839/05, ECHR 2010.
10. *Klass v Germany*, no 5029/71, ECHR 1978.
11. *Kopp v Switzerland*, no 23224/94, ECHR 1998.
12. *Leander v Sweden*, no 9248/81, ECHR 1987.
13. *Liblik v Estonia*, nos 173/15 and 5 others, ECHR 2019.
14. *Malone v the United Kingdom*, no 8691/79, ECHR 1984.
15. *P.N. v Germany*, no 74440/17, ECHR 2020.
16. *Roman Zakharov v Russia*, no 47143/06, § 272, ECHR 2015.
17. *Sedletska v Ukraine*, no 42634/18, ECHR 2021.
18. *Segerstedt-Wiberg v Sweden*, no. 62332/00, ECHR 2006.

19. *Szabó and Vissy v Hungary*, no 37138/14, ECHR 2016.

20. *Tinnelly & Sons Ltd and McElduff v The United Kingdom*, nos 20390/92 and 21322/93, ECHR 78.

21. *Trajkovski and Chipovski v North Macedonia*, nos 53205/13 and 63320/13, ECHR 2020.

22. *Weber and Sanravia v Germany*, no 54934/00, ECHR 2008.

Books

1. Cole and Vladeck "Navigating the Shoals of Secrecy: A Comparative Analysis of the Use of Secret Evidence and 'Cleared Counsel' in the United States, the United Kingdom, and Canada" in Lazarus et al (eds) *Reasoning Rights: Comparative Judicial Engagement* (Bloomsbury, London 2014) at 171.

2. Duncan *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (Wits University Press, Johannesburg 2018) at 93.

3. McIntyre "Judicial Oversight of Surveillance: the Case of Ireland in Comparative Perspective" in Scheinin et al (eds) *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar Publishing, Cheltenham 2016)

4. Milo and Scott "The High-Wire: the Delicate Balance between Communications Surveillance, Constitutional Rights and the Media in South Africa" in Bosland and De Zwart (eds) *Watching Me, Watching You: Surveillance, Privacy and the Media* (LexisNexis, Cape Town 2016) at 259.

5. Mutung'u "South Africa Country Report" in Roberts *Surveillance Law in Africa: a Review of Six Countries* (Institute of Development Studies 2021).

Journals articles

1. Bakir, "'Veillant Panoptic Assemblage': Mutual Watching and Resistance to Mass Surveillance After Snowden" (2015) 3 *Media and Communications* 12.
2. Eskens et al "10 Standards for Oversight and Transparency of National Intelligence Services" *Journal of National Security Lax* 8 (2016) 553.
3. Hudson and Alati "Behind Closed Doors: Secret Law and the Special Advocate System in Canada" (2019) 44 *Queen's Law Journal* 1.
4. Jackson "In a World of Their Own: Security-cleared Counsel, Best Practice, and Procedural Tradition" (2019) 46 *Journal of Law and Society* 130.

United Nations reports and resolutions

1. UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021).
2. UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020).
3. UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020).
4. Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (27 October 2019).

5. Report of the Special Rapporteur on the Right to Privacy, UN Doc A/HRC/40/63 (16 October 2019).
6. UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019).
7. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019).
8. UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/73/179 (17 December 2018).
9. Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).
10. Concluding Observations on the Initial Report of South Africa, Human Rights Committee, UN Doc CCPR/C/ZAF/CO/1 (27 April 2016).
11. UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/69/166 (18 December 2014).
12. Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014).
13. Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013).
14. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013).

15. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism "Compilation of Good Practices for Intelligence Agencies and their Oversight" *Geneva Centre for the Democratic Control of Armed Forces* (5 August 2011).
16. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, UN Doc A/HRC/16/51/Add.3 (15 December 2010).

Further reports

1. Mare "Communication Surveillance in Namibia: an Exploratory Study" *Media Policy and Democracy Project* (November 2019).
2. Mare "An Analysis of the Communications Surveillance Legislative Framework in South Africa" *Media Policy and Democracy Project* (November 2015).
3. Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts, no 839/2016, European Commission for Democracy through Law 2016.
4. Report on the Democratic Oversight of the Security Services, no 388 / 2006, European Commission for Democracy through Law 2007
5. Right2Know "The Surveillance State: Communications Surveillance and Privacy in South Africa" *Media Policy and Democracy Project* (March 2016).

Internet sources

6. Applicant's Heads of Argument, case no CCT 278/19, Constitutional Court, available at https://collections.concourt.org.za/handle/20.500.12144/36631?show=full.

7. Commissioner for Human Rights, Council of Europe "Democratic and Effective Oversight of National and Security Services" (May 2015), available at https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb.

8. Commissioner for Human Rights, Council of Europe "Positions on Counter-Terrorism and Human Rights Protection" (5 June 2015), available at https://rm.coe.int/16806db6b2.

9. Electronic Frontier Foundation "Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance" (May 2014), available at https://necessaryandproportionate.org/global-legal-analysis.

10. Electronic Frontier Foundation "Necessary & Proportionate: on the Application of Human Rights to Communications Surveillance", available at https://necessaryandproportionate.org/13-principles/.

11. Electronic Frontier Foundation "Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance" (May 2015), available at https://necessaryandproportionate.org/implementation-guide/.

12. Hunter and Mare "A Patchwork for Privacy: Communications Surveillance in Southern Africa" *Media Policy and Democracy Project* (6 May 2020), available at https://archive.org/details/patchwork-for-privacy-communication-surveillance-in-southern-africa/page/n1/mode/2up.

13. Hunter “Cops and Call Records: Policing and Metadata Privacy in South Africa” *Media Policy and Democracy Project* (27 March 2020), available at https://archive.org/details/2003-cops-and-call-records-metadata-and-policing.

14. Open Society Justice Initiative “The Global Principles on National Security and the Right to Information”, (12 June 2013), available at https://www.justiceinitiative.org/publications.