Constitutional Litigation Unit

16th Floor Bram Fischer Towers • 20 Albert Street • Marshalltown • Johannesburg 2001 • South Africa
PO Box 9495 • Johannesburg 2000 • South Africa
Tel: (011) 838 9831 • Fax: (011) 838 4273 • Website www.lrc.org.za
PBO No. 930003292
NPO No. 023-004

LRC
Legal Resources Centre

LEGAL RESOURCES CENTRE

SUBMISSION TO THE SPECIAL RAPPORTEUR ON THE PROTECTION AND PROMOTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION

THE SOUTH AFRICAN LEGAL FRAMEWORK GOVERNING THE RELATIONSHIP BETWEEN FREEDOM OF EXPRESSION AND THE USE OF ENCRYPTION

FEBRUARY 2015

Table of contents

Abbreviations 3

Introduction 4

Constitutional framework on the right to freedom of expression 5

Legislative framework regarding encryption 8

Overview 8

The Electronic Communications and Transactions Act 9

The Regulation of Interception of Communications and Provision of Communication-Related Information Act 12

The Conventional Arms Control Regulations 15

The National Strategic Intelligence Act 16

The Protection of Personal Information Act 17

The National Cybersecurity Policy Framework for South Africa 18

Relevant considerations when determining the scope of the right to freedom of expression as applied to encryption and anonymity 19

Conclusion 21

Abbreviations

CACR	Conventional Arms Control Regulations promulgated in terms of the National Conventional Arms Control Act 41 of 2002
ECTA	Electronic Communications and Transactions Act 25 of 2002
LRC	Legal Resources Centre
NCACA	National Conventional Arms Control Act 41 of 2002
NCPF	National Cybersecurity Policy Framework for South Africa
NSIA	National Strategic Intelligence Act 39 of 1994
POPI	Protection of Personal Information Act 4 of 2013
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
SSA	State Security Agency

Introduction

1. This is a submission prepared by the Legal Resources Centre ("**LRC**") for consideration by the Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression ("**the Special Rapporteur**"). This submission is in response to a call for information from the Special Rapporteur on national laws that permit or limit the use of encryption technologies or the ability of individuals to communicate anonymously online, as well as the scope of the right to freedom of expression as applied to encryption and anonymity.

2. The LRC is one of South Africa's oldest public interest law firms, focussing on human rights and constitutional law. The goals of the LRC are to promote justice, build respect for the rule of law, and contribute to socio-economic transformation in South Africa and beyond. In this regard, the LRC's clients are predominantly vulnerable and marginalised, including people who are poor, homeless and landless. The LRC is committed to assisting communities through strengthening knowledge, skills and experience, in order to assist communities to claim their fundamental economic, social and environmental rights.

3. The LRC has been involved in a number of landmark freedom of expression and access to information cases in South Africa, and has recently been involved in litigation in these areas before other regional bodies as well. In making this submission, the LRC does not purport to hold a mandate on behalf of all affected persons, or to be an expert in the field of encryption or the regulation of the internet. However, as will be seen from what is contained below, the focus of this submission is to provide the Special Rapporteur with the relevant South African legal framework that may be of assistance when preparing his report to the Human Rights Council.

4. This submission is set out as follows:

4.1. Firstly, we set out the constitutional framework of the right to freedom of expression, including the right to freedom of the media;

4.2. Secondly, we set out the relevant legislative framework governing encryption in South Africa; and

4.3. Lastly, we canvass what we consider to be some of the relevant considerations when determining the scope of the right to freedom of expression as applied to encryption and anonymity.

5. We deal with each of these in turn below.

Constitutional framework on the right to freedom of expression

6. Freedom of expression is a fundamental right contained in section 16 of the Constitution of the Republic of South Africa, 1996 ("**the Constitution**"). Section 16 states as follows:

> "1. Everyone has the right to freedom of expression, which includes -
> (a) freedom of the press and other media;
> (b) freedom to receive or impart information or ideas;
> (c) freedom of artistic creativity; and
> (d) academic freedom and freedom of scientific research.
> 2. The right in subsection (1) does not extend to -
> (a) propaganda for war;
> (b) incitement of imminent violence; or
> (c) advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm."

7. The South African Constitutional Court, the highest court in the country, has recognised the importance of the right to freedom of expression on a number of occasions. It has been described as a "*sine qua non for every person's right to realise her or his full potential as a human being, free of the imposition of heteronomous power*",[1] and "*essential to the proper functioning of our constitutional democracy*".[2] In South African National Defence Union v Minister of Defence and Another, the Constitutional Court stated that:[3]

> "Freedom of expression lies at the heart of democracy. It is valuable for many reasons, including its instrumental function as a guarantor of democracy, its implicit recognition and protection of the moral agency of individuals in our society and its facilitation of the search for truth by individuals and society generally."

8. Importantly, the special role that the media plays has also been frequently acknowledged by the South African courts:

8.1. In Khumalo v Holomisa, the Constitutional Court stated that:[4]

> "The print, broadcast and electronic media have a particular role in the protection of freedom of expression in our society. Every citizen has the right to freedom of the press and the media and the right to receive information and ideas. The media are key agents in ensuring that these aspects of the rights to freedom of information are respected";

8.2. Similarly, in National Media Ltd v Bogoshi, the Supreme Court of Appeal held that:[5]

> "[W]e must not forget that it is the right, and indeed a vital function, of the press to make available to the community information and criticism

---

[1] Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others 1996 (5) BCLR 609 (CC) at para 29.

[2] The Citizen 1978 (Pty) Ltd and Others v McBride (Johnstone and Others as Amici Curiae) 2011 (8) BCLR 816 (CC) para 141.

[3] 1999 (4) SA 469 (CC) at para 7.

[4] 2002 (5) SA 401 (CC) at para 22.

[5] 1998 (4) SA 1195 (SCA) at 1209.

> about every aspect of public, political, social and economic activity and thus to contribute to the formation of public opinion . . . The press and the rest of the media provide the means by which useful, and sometimes vital, information about the daily affairs of the nation is conveyed to its citizens";

8.3. The guarantee of media freedom is designed to serve the interest that all citizens have in the free flow of information "*which is possible only if there is a free press.*"[6] As was stated in South African Broadcasting Corporation v Director of Public Prosecutions:[7]

> "A vibrant and independent media encourages citizens to be actively involved in public affairs, to identify themselves with public institutions and to derive the benefits that flow from living in a constitutional democracy. Access to information and the facilitation of learning and understanding are essential for meaningful involvement of ordinary citizens in public life. This . . . reflects the foundational principle of democratic government which ensures accountability, responsiveness and openness."

9. The right to freedom of expression may only be limited on the basis of section 16(2) of the Constitution mentioned above, or in terms of a 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.[8]

---

[6] Midi-Television (Pty) Ltd t/a e-TV v Director of Public Prosecutions (Western Cape) 2007 (5) SA 540 (SCA) at para 6.

[7] 2007 (1) SA 523 (CC) at para 28.

[8] Section 36(1) of the Constitution; see Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International 2005 (8) BCLR 743 (CC) at para 47.

Legislative framework regarding encryption

Overview

10. There are no domestic controls on the export, import, downloading and use of encryption software in South Africa, and one does not need a permit or licence to use it unless it is being used for military purposes or comes from a military supplier.[9] As far as use by members of the public is concerned, there is largely unrestricted. There are, however, laws governing the suppliers of cryptography services:

11. In this submission, we will consider the following South African laws:

11.1. Firstly, the primary piece of legislation in this regard is the Electronic Communications and Transactions Act[10] ("**ECTA**"), and the Cryptography Regulations[11] promulgated in terms thereof;

11.2. Secondly, the Regulation of Interception of Communications and Provision of Communication-Related Information Act[12] provides the circumstances under which a decryption direction may be obtained by an appropriate person in order to obtain a decryption key or decryption assistance;

11.3. Thirdly, the Conventional Arms Control Regulations[13] ("**CACR**") promulgated in terms of the National Conventional Arms Control Act[14]

[9] See Michaelson "Cryptography laws in South Africa" (25 May 2012).

[10] Act 25 of 2002.

[11] GNR. 216 of 10 March 2006.

[12] Act 70 of 2002.

[13] GNR. 7969 of 28 May 2004.

[14] Act 41 of 2002.

("**NCACA**") regards matters in the field of armaments and defence in which a permit or licence may be required for encryption technology;

11.4. Fourthly, the National Strategic Intelligence Act[15] ("**NSIA**") deals briefly with the matter of encryption to the extent that it identifies the functions of the State Security Agency ("**SSA**");

11.5. Fifthly, the provisions of Protection of Personal Information Act[16] ("**POPI**") are an area in which it is expected that encryption is likely to play an important role once the legislation comes into force; and

11.6. Sixthly, the import of the National Cybersecurity Policy Framework for South Africa ("**NCPF**") is discussed briefly.

12. We deal with each of these in turn below.

The Electronic Communications and Transactions Act

13. As mentioned above, ECTA is the primary piece of legislation governing providers of cryptography services, with a number of provisions regarding cryptography providers contained in chapter V. A "*cryptography provider*" means "*any person who provides or proposes to provide cryptography services or products in the Republic*", and a "*cryptography service*" means:[17]

> "[A]ny service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring –
>
> (a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;
>
> (b) that the authenticity or integrity of such data or data message is capable of being ascertained;

[15] Act 39 of 1994.

[16] Act 4 of 2013.

[17] Section 1 of ECTA.

(c) the integrity of the data or data message; or

(d) that the source of the data or data message can be correctly ascertained".

14. Similarly, a "*cryptography product*" is defined as:

> [A]ny product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring -
>
> (a) that such data can be accessed only by relevant persons;
>
> (b) the authenticity of the data;
>
> (c) the integrity of the data; or
>
> (d) that the source of the data can be correctly ascertained".

15. Section 29 of ECTA requires the Director-General of the Department of Communications to establish and maintain a register of cryptography providers.[18] The register must record the name and address of the cryptography provider, a description of the cryptography service or cryptography product being provided, and such other particulars as may be prescribed to identify and locate the cryptography provider or its products or services adequately;[19] however, a cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.[20]

16. The Cryptography Regulations provide more detail on the information that must be contained in the register and the process for registration. Notably, in terms of regulation 2 of the Cryptography Regulations, there is a host of information in addition to that which is set out in section 29 that must be provided:

> "In addition to the information required in section 29 of the Act, an application for registration must
>
> (a) contain the following particulars to identify and locate the cryptography provider:
>
> (i) Telephone and fax number, web site and e-mail address;

[18] Section 29(1) of ECTA.

[19] Section 29(2) of ECTA.

[20] Section 29(3) of ECTA.

(ii) the constitutive documents of the applicant which are, in the case of a legal person, certified copies of the Memorandum and Articles of Association, certificate of incorporation, founding statement, partnership agreement or trust deed, and in the case of a natural person, a certified copy of his or her ID book or passport, as the case may be;

(iii) detailed profiles of trusted personnel of the applicant that have supervisory or managerial responsibilities;

(b) contain the following particulars to identify and locate the cryptography provider's products or services:

(i) physical address where a cryptography product is or will be produced, manufactured, created or distributed from;

(ii) physical address where a cryptography service is or will be rendered, delivered, sold, made available or distributed from;

(iii) full details of cryptography operations outsourced;

(iv) name, address and contact details of any other cryptography provider that provides a cryptography service or product to the cryptography provider;

(v) if the cryptography provider is a certification service provider, its certification practice statement and certificate policy;

(c) contain the particulars required by section 29 of the Act and paragraph (a) of this regulation, to identify and locate an entity to whom cryptography operations have been outsourced;

(d) contain particulars indicating whether the cryptography provider provides encrypted bugging and debugging equipment."

17. No person may provide cryptography services or products in South Africa until the particulars of that person have been recorded in the register in terms of section 29 of ECTA.[21] In terms of section 30(3) of ECTA, a cryptography service or product is regarded as having been provided in South Africa if it is provided (i) from premises in South Africa; (ii) to a person who is present in South Africa when that person makes use of the service or product; or (iii) to a person who uses the service or product for the purposes of a business carried on in South Africa or from premises in South Africa.

18. As a general principle, the information contained in the register may not be disclosed to anyone other than an employee of the Department of

[21] Section 30(1) of ECTA.

Communications responsible for the keeping of the register.[22] However, this general principle may be departed from in certain instances:[23]

18.1. If the information is disclosed to a relevant authority investigating a criminal offence or for the purposes of any criminal proceedings;

18.2. If the information is disclosed to government agencies responsible for safety and security in the South Africa pursuant to an official request;

18.3. If the information is disclosed to a cyber-inspector;

18.4. If the information is disclosed in terms of sections 11 or 30 of the Promotion of Access to Information Act;[24] or

18.5. If the information is disclosed for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

19. It is a criminal offence not to comply with the abovementioned provisions of ECTA.[25]

The Regulation of Interception of Communications and Provision of Communication-Related Information Act

20. RICA seeks to regulate the interception of communications and provides the circumstances under which communications may be lawfully intercepted.[26] One such circumstance is if an interception direction is applied for and obtained in

[22] Section 31(1) of ECTA.

[23] Section 31(2) of ECTA.

[24] Act 2 of 2000.

[25] Section 32 of ECTA.

[26] Sections 3 – 11 of RICA.

terms of section 16 of RICA.[27] Only certain specified categories of persons may apply for an interception direction (typically persons involved with law enforcement, investigations and intelligence),[28] and an interception direction may only be issued by a judge.[29]

21. An interception direction may only be issued if:[30]

> "[T]he designated judge concerned is satisfied, on the facts alleged in the application concerned, that -
>
> (a) there are reasonable grounds to believe that -
>
> (i) a serious offence has been or is being or will probably be committed;
>
> (ii) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;
>
> (iii) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;
>
> (iv) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in –
>
> (aa) accordance with an international mutual assistance agreement; or
>
> (bb) the interests of the Republic's international relations or obligations; or
>
> (v) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary;
>
> (b) there are reasonable grounds to believe that –
>
> (i) the interception of particular communications concerning the relevant ground referred to in paragraph (*a*) will be obtained by means of such an interception direction; and
>
> (ii) subject to subsection (8), the facilities from which, or the place at which, the communications are to be intercepted are being used, or are about to be used, in connection with the relevant ground referred to in paragraph (*a*) are commonly used by the person or customer in respect of whom the application for the issuing of an interception direction is made . . ."

[27] Sections 2 and 16 of RICA.

[28] Section 1 of RICA.

[29] Section 16(4) of RICA.

[30] Section 16(5) of RICA.

22. A person who applies for and is eligible to obtain an interception direction may also apply for decryption direction.[31] The application for a decryption direction must contain various information, including:[32]

22.1. The identity of the decryption key holder to whom the decryption direction must be addressed;

22.2. A description of the encrypted information which is required to be decrypted;

22.3. The decryption key or decryption service which must be provided; and

22.4. The period for which the decryption direction is required.

23. In terms of section 21(4) of RICA, a decryption direction may only be issued under the following circumstances:

> "A decryption direction may only be issued –
>
> (a) if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that there are reasonable grounds to believe that –
>
> (i) any indirect communication to which the interception direction concerned applies, or any part of such an indirect communication, consists of encrypted information;
>
> (ii) the decryption key holder specified in the application is in possession of the encrypted information and the decryption key thereto;
>
> (iii) the purpose for which the interception direction concerned was issued would be defeated, in whole or in part, if the decryption direction was not issued; and
>
> (iv) it is not reasonably practicable for the authorised person who executes the interception direction concerned or assists with the execution thereof, to obtain possession of the encrypted information in an intelligible form without the issuing of a decryption direction; and
>
> (b) after the designated judge concerned has considered –
>
> (i) the extent and nature of any other encrypted information, in addition to the encrypted information in respect of which the decryption direction is to be issued, to which the decryption key concerned is also a decryption key; and

[31] Section 21(1) of RICA.

[32] Section 21(2) of RICA.

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

24. A decryption key holder is required to comply with a decryption direction addressed to him or her, and must disclose the decryption key or provide the decryption assistance necessary to obtain access to the encrypted information specified in the decryption direction or to put the encrypted information into an intelligible form.[33] Any person who fails to comply with a direction issued in terms of RICA is guilty of a criminal offence.[34]

The Conventional Arms Control Regulations

25. As mentioned above, the CACR were promulgated in terms of the NCACA, which seeks to ensure a transparent, legitimate and effective process for arms control. In terms of section 13(1) of the NCACA, no person may trade in or possess the controlled items referred to in the CACR unless that person is registered and in possession of an appropriate permit.

26. The CACR set out the types of munitions that require permits, and the type of permit required. Although neither the NCACA nor the CACR refers to encryption or cryptography services, the CACR does state as follows at the beginning of the schedule:

> "General technology note
>
> The export of 'technology' which is 'required' for the 'development', 'production' or 'use' of items controlled in the Dual-Use List is controlled according to the provisions in each Category. This 'technology' remains under control even when applicable to any uncontrolled item."

27. This would affect, for instance, any decryption key necessary to decrypt information needed to use arms contemplated in CACR. There are, however,

[33] Section 21(1)-(2) of RICA.

[34] Section 51 of RICA.

several exceptions to this, in particular where the technology or software is in the public domain, or where it is designed for installation by the user without further substantial support by the supplier.

28. The NCACA and the CACR are two of the main laws identified by the NCPF as key to the regulation of the field of cryptography.

The National Strategic Intelligence Act

29. The purpose of the NSIA is to set out the functions of the national intelligence structures in South Africa. In 2013, the NSIA was amended by the General Intelligence Laws Amendment Act[35] to include cryptography services as part of the functions of the State Security Agency ("**SSA**").

30. As a result of this amendment, section 2(2)(b) of the NSIA was amended to include the following as functions of the SSA:

> "(i) to identify, protect and secure critical electronic communications and infrastructure against unauthorised access or technical, electronic or any other related threats;
>
> (ii) to provide cryptographic and verification services for electronic communications security systems, products and services used by organs of state;
>
> (iii) to provide and coordinate research and development with regard to electronic communications security systems, products and services and any other related services".

31. Accordingly, it is now squarely within the ambit of the SSA to provide cryptographic services for all government departments as well as other organs of state.

[35] Act 11 of 2013.

The Protection of Personal Information Act

32. Two of the key purposes for the enactment of POPI are to give effect to the constitutional right to privacy by safeguarding personal information,[36] and regulating the manner in which personal information may be processed by establishing conditions, in accordance with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.[37]

33. POPI contains eight conditions for the lawful processing of personal information.[38] For present purposes, the condition of particular relevance is condition 7 regarding security safeguards. In terms of this condition:[39]

> "A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent –
>
> (a) loss of, damage to or unauthorised destruction of personal information; and
>
> (b) unlawful access to or processing of personal information."

34. This condition further requires, *inter alia*, that the responsible party must take all reasonable measures to establish and maintain appropriate safeguards against the risks identified (which safeguards must be regularly verified and continually updated),[40] and that the responsible party must have due regard to "*generally*

[36] Section 2(a) of POPI.

[37] Section 2(b) of POPI.

[38] These conditions are as follows: accountability (section 8 of POPI); processing limitation (sections 9 to 12 of POPI); purpose specification (sections 13 to 14 of POPI); further processing limitation (section 15 of POPI); information quality (section 16 of POPI); openness (sections 17 to 18 of POPI); security safeguards (sections 19 to 22 of POPI); and data subject participation (sections 23 to 25 of POPI).

[39] Section 19(1) of POPI.

[40] Section 19(2)(b)-(d) of POPI.

accepted information security practices and procedures which may apply to it generally".[41]

35. Although POPI has been signed into law and certain sections have been brought into force, the sections regarding the conditions for the lawful processing of personal information have not as yet commenced. It has therefore also not been necessary for the information regulator or the courts to provide guidance on what is meant by "*appropriate safeguards*" or "*generally accepted information security practices and procedures*". It is, however, expected that in appropriate circumstances – and particularly in industries that make use of confidential or sensitive information, such as credit card details – it will be required that encryption mechanisms be put in place in line with international practice in order to meet the threshold imposed by this condition.

36. The remaining provisions under POPI are expected to come into operation in due course once the office of the information regulator has been established.

The National Cybersecurity Policy Framework for South Africa

37. Lastly, the NCPF was a draft document developed by the Justice, Crime Prevention and Security Cluster in South Africa in an effort to create a framework for the investigation and combatting of cybercrime.

38. Of relevance to the matter of encryption, it is noted in the NCPF that "*there are an ever-increasing number of cryptographic devices, cryptographic software and users and requiring secure communications and the geographic spread of locations of these devices*".[42] The NCPF goes on to state as follows:[43]

[41] Section 19(3) of POPI.

[42] NCPF at para 8.1.

> "The NCPF notes that various attempts at regulating cryptography were initiated as a way of developing a coherent and integrated approach to this matter.
>
> . . .
>
> Taking into consideration the abovementioned legislation, there is a need to:
>
> (a) Review the existing legislation and regulations thereof; and
>
> (b) Develop an integrated regulatory framework for cryptography in the Republic."

39. However, although the NCPF was approved by the South African cabinet in 2012, there have yet to be any steps taken to implement it.[44]

Relevant considerations when determining the scope of the right to freedom of expression as applied to encryption and anonymity

40. As a point of departure, we note that we are of the view that encryption is an important and necessary tool, both for issues such as banking and e-commerce but also in the protection of rights, including the right to privacy, the right to freedom of expression and the right to freedom of the media. In addition to being used by the state, encryption is also frequently and meaningfully used by journalists, human rights activists, refugees and whistle blowers. We note the experience in various other countries that have made effective use of encryption technology to access websites that have been blocked or to circumvent state-led efforts to censor what was being said by civil society movements. If encryption were to be prohibited (as has been proposed in the United Kingdom and Pakistan, for instance), coupled with the permissibility of the interception of

[43] NCPF at paras 8.2-8.3.

[44] Sabinet "Cabinet approves National Cybersecurity Policy Framework" (12 March 2012); see also IT Web "Cybercrime clampdown in the works" (22 January 2015).

communications by state agencies, this would inevitably have a chilling effect on the free flow of information.

41. In the public interest arena, encryption is a particularly important tool for members of the media who can use it to render data meaningless to unwanted readers and to protect transmitted data against interception. The media can make effective use of encryption to share information with effective anonymity and without surveillance, particularly where the information concerned may reveal abuses by members of government or state agencies.

42. The submission above should not be understood to mean that we do not consider there to be justifiable circumstances under which a decryption direction, for instance, may be obtained. We are, however, concerned that the process as it presently stands in South Africa contemplates an *ex parte* procedure without due notice either to the cryptographer or, more importantly, the person who has obtained the cryptography services to put up a case as to why the direction should not be granted. The standard of proof required, that being that the judge must be reasonably satisfied, is also not a high threshold to meet. Although it has not received much attention in the South African courts to date, there certainly appears to be the potential for manifest abuse.

43. In our view, it should be open to individuals to use whatever technology they choose to secure their communications, and the state should not interfere with the use of encryption technologies or compel the provision of encryption keys except in the most egregious circumstances. In this regard, we would note further that in terms of the South African law, there is an urgent need for a rationalisation of the laws, with a particular focus on ridding the legislation of the vagueness regarding the circumstances under which the disclosure of encryption-related information can be compelled.

Conclusion

44. As set out above, we have canvassed the South African constitutional and legislative framework for the matters presently under consideration by the Special Rapporteur. We have also presented our views on the appropriate scope of the right to freedom of expression as applied to encryption and anonymity. The LRC appreciates the opportunity to make this submission, and would like to thank the Special Rapporteur for his consideration of this. Please do not hesitate to contact us should you require any further information or assistance.

AVANI SINGH

LEGAL RESOURCES CENTRE

FEBRUARY 2015