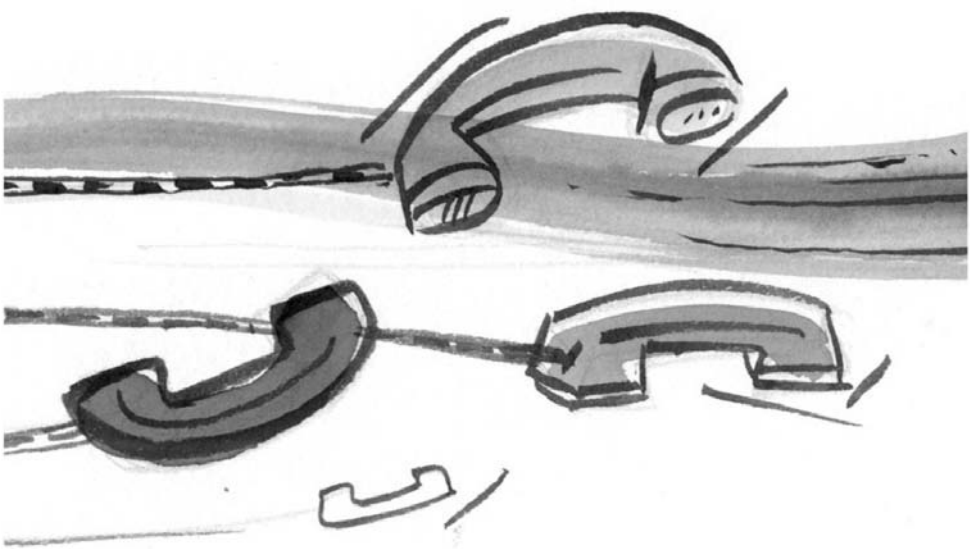
The Regulation of the Interception of Communications and Provision of Communication Related Information Act

Nazreen Bawa[1]



[1] The author would like to thank the following persons for reviewing parts of previous drafts: Lisa Thornton, Deshni Pillay, Tanya Scott, Fatimah Essop and Adele Erasmus.

Introduction

In November 1995, the South African Law Reform Commission[2] (SALC) undertook to review and rationalise South Africa's security legislation with specific regard to international norms, the interim Constitution[3] and the country's changed circumstances and requirements.

As part of this broad investigation, the SALC prioritised the area of interception and monitoring of communications for crime investigation and intelligence gathering, and it appointed a Project Committee to advise it and to consider documentation generated during the course of this investigation. The interception and monitoring of communications was prioritised, as sophisticated telecommunication services[4] were increasingly being used to perpetrate crime, especially organised crime, heists, and other serious violent crimes. In addition, the SALC was of the view that since the promulgation of the Interception and Monitoring Prohibition Act, 127 of 1992 (IM Act) on 1 February 1993, there had been an increase in the use of advanced telecommunications technologies, including cellular communications, satellite communications, computer communications through e-mail, as well as the electronic transfer of information and data. Furthermore, the considerable legal developments across the world regarding the interception of communications made a review of the IM Act necessary. The SALC took the approach that legal provision should be made for law-enforcement agencies to be equipped with the necessary tools to investigate crimes that used telecommunications directly, as well as other concomitant crimes, such as money-laundering. The SALC contended that a review of the existing legislation, in particular the IM Act, would ensure that emphasis would be on crime.[5]

As indicated in its long title, the IM Act is directed at prohibiting the interception of certain communications, monitoring certain conversations or communications, providing mechanisms for the interception of postal articles and communications as well as the monitoring of conversations or communications when a serious offence is committed or the security of South Africa is threatened. It deals with the issues of monitoring and interception separately. The primary objective of the IM Act is not crime prevention but the protection of confidential information[6] from illicit eavesdropping.[7] It allows the state to intercept and monitor conversations and communications under certain conditions and in accordance with directives issued in terms of the IM Act.

[2] Since the promulgation of the Judicial Matters Amendment Act, 55 of 2002 the South African Law Commission, as established by the South African Law Commission Act, 19 of 1973, has become the South African Law Reform Commission (hereinafter referred to as 'the SALC').

[3] Constitution of the Republic of South Africa, Act 200 of 1993.

[4] 'Telecommunication service' is defined in the Telecommunications Act, 103 of 1996 as including any service provided by means of a telecommunication system. A 'telecommunication system' is defined as any system or series of telecommunication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to rearrangement, composition or other processes by any means in the course of their transmission or emission or reception. 'Telecommunication', in turn, is defined as the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio, other electromagnetic waves, or any agency of a like nature, whether with or without the aid of tangible conductors.

[5] SALC Report *Review of Security Legislation Project 105: The Interception and Monitoring Prohibition Act (Act 127 of 1992)*, October 1999 (hereinafter referred to as 'the SALC Report') para 1.27.

[6] Although the IM Act did not define confidential information, in *Protea Technology Limited and Another v Wainer and Others* [1997] 3 B All SA 594, 603, the Court remarked as follows:

That expression must surely mean such information as the communicator does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessary or impliedly to be restricted. I think that there is a distinction between 'confidential' information and 'private' information.

[7] *Lenco Holdings Ltd v Eckstein* 1996 (2) SA 693 (N) at 700; *S v Kidson* 1999 (1) SACR 338 (W) at 344.

During October 1999, after extensive public consultation, the SALC Report was submitted to the Minister of Justice and Constitutional Development for consideration. It included an extensive review of the IM Act and was compiled with reference to, and in comparison with, similar legislation in France, the Netherlands, Belgium, Germany, Britain, the United States, Hong Kong and Canada.[8] The comparison with international law illustrated that in the past decade many other countries had similarly reconsidered and reviewed their interception and monitoring legislation, predominantly for reasons relating to crime prevention and national security. Many of the aforementioned countries have developed new legislation to conduct surveillance and monitoring of communications (commonly known as 'wiretapping' or 'bugging').

The SALC was of the view that even though the IM Act compares favourably with its counterparts in other countries, it does not deal adequately with new technology (eg, the IM Act does not deal with the monitoring of employees' e-mail by employers). For that reason the SALC recommended that it be substantially repealed and replaced with new legislation.

To this end, the SALC recommended a new draft bill, which culminated in the promulgation of the Regulation of the Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 (ROICA) on 22 January 2003.[9] ROICA will come into operation on a date to be fixed by the President by proclamation in the Government Gazette.[10] ROICA was drafted in response to the increasing diversity and developments in communication technologies, globalisation of the telecommunications industry, and the convergence of the telecommunications, broadcasting and information technology industries, which inter alia include satellites, optical fibres, computers, cellular technology, e-mail, surveillance equipment, and the electronic transfer of information and data. ROICA sets out the circumstances under which government entities and other persons may or must intercept or monitor conversations, cellular text messages, e-mails, faxes, data transmissions and postal articles, and establishes that in all other circumstances, such interception or monitoring is prohibited.

Although the shift from the IM Act to ROICA was initiated ostensibly to equip law-enforcement officers in their battle against the types of crime that involve sophisticated technological advances, it also regulates virtually every aspect pertaining to the interception and monitoring of telecommunications both in the workplace and in the private sphere. This includes the monitoring and interception of employee e-mails by employers. In permitting such interception and monitoring, it is arguable that ROICA does not provide adequate safeguards to protect the privacy of employees in the workplace. This may result in a number of provisions of ROICA being susceptible to constitutional challenge. There is also the danger that the invocation of the provisions of ROICA, both in the employment context and by law-enforcement officers, may be abused in a manner that is inconsistent with the right to privacy and freedom of expression enshrined in the final Constitution.[11]

---

[8] SALC Report (note 5 above) chapters 3-10. The SALC had particular regard to the Law Reform Commission of Hong Kong *Privacy: Regulating Surveillance and the Interception of Communications* Consultation Paper 1996, http://www.info.gov.hk/info/pricon.htm and its comparative foreign review; see SALC Report (note 5 above) chapter 9. See also the SA Law Commission Discussion Paper 78 *Review of Security Legislation - The Interception and Monitoring Prohibition Act (Act 127 of 1992)* (November 1998) chapters 3-10 (hereinafter referred to as 'the SALC Discussion Paper').

[9] *Government Gazette* 24286 dated 22 January 2003. As recommended by the SALC, s 62(1) of ROICA will repeal the IM Act.

[10] s 63 of ROICA. As at July 2004, that date had not yet been proclaimed.

[11] Constitution of the Republic of South Africa Act, 108 of 1996.

ROICA subsumes monitoring into interception and permits greater latitude for the interception and monitoring of communication than was permitted in the IM Act. It makes detailed provision for the State to intercept and monitor communications. In doing so, ROICA also places onerous obligations (financial and otherwise) on the private telecommunications industry to assist the State in its interception and monitoring of communications. This is apparent in the comparison made between the relevant provisions in the IM Act and ROICA, as done below. The increase in obligation on the industry and the shifting of liability to the private sector may also result in the crippling of the smaller sectors of the telecommunications industry, with small service providers having to shut down due to an inability to meet obligations imposed by ROICA. In addition, neither the SALC nor the legislature has indicated what the implementation of ROICA will cost both government and the telecommunications industry.

This chapter focuses on the provisions of ROICA most relevant to telecommunications and is structured as follows: firstly brief consideration is given to the legislative and policy developments with specific regard to the findings of the SALC and the parliamentary process which preceded its enactment; secondly, the relevant constitutional framework, with particular regard to the rights to privacy and freedom of expression, is set out; thirdly, the general prohibition on interception and monitoring and the specific exemptions as contained in ROICA, including monitoring of signals and radio frequency spectrums, are considered; fourthly, the scope of the application of ROICA with reference to the objectives sought to be achieved, the issuance and execution of written and oral directions for interception, and entry warrants is discussed and, finally, consideration is given to the obligations that ROICA places on the telecommunications industry.

1. LEGISLATIVE AND POLICY DEVELOPMENT

1.1 The South African Law Reform Commission

The SALC Report was compiled after public comments were solicited from government departments, law-enforcement agencies, telecommunication service providers (TSPs), individuals and bodies representing the legal community. Comments were invited with respect to regulating the manufacture, distribution, possession and advertisement of wire or oral communication intercepting devices, third party surveillance, and on whether the new Act should be more prescriptive.[12]

On 27 November 1998, the SALC Discussion Paper was published for general information and comment. It contained a number of provisional recommendations as well as an initial draft Bill amending the IM Act.[13] Twenty-eight respondents commented in writing on the Discussion Paper. The Project Committee met on 29 May 1999 with parties representing the TSPs, law-enforcement, intelligence and security agencies. Their views, as well as those reflected in the written comments, were taken into account when the Project Committee made its recommendations reflected in the SALC Report. In particular, the SALC took the position that, in principle, interception and monitoring should

[12] SALC Report (note 5 above) paras 11.7-11.9; annexure D.
[13] SALC Report (note 5 above) para 11.6.

be prohibited when conducted without the knowledge or permission of the parties to a conversation or communication, and should not be a tool for acquiring confidential information concerning any person, body or organisation.[14]

1.2 Parliamentary process

The initial Interception and Monitoring Bill, 2001 (to replace the IM Act) that was introduced in 2001 in the National Assembly in accordance with section 75 of the final Constitution emanated from the SALC Report.[15] The main object of the Bill was to replace the existing IM Act with a new substantive Act, incorporating the recommendations made by the SALC.[16] The Bill was referred to the Portfolio Committee on Justice and Constitutional Development, which called for further written submissions. Interested parties made oral and written representations.[17]

The Bill that subsequently emerged from the parliamentary process contained most of the provisions of the IM Act (either in amended or un-amended form) as well as numerous new provisions aimed at further regulating the interception and monitoring of communications. It differed substantially from the version recommended by the SALC and contained a number of controversial new provisions, which were widely criticised in the media and in the submissions made to the Portfolio Committee for Justice and Constitutional Development. It is apparent from the Deputy Minister of Justice and Constitutional Development's address to Parliament at the second reading of the Bill that the main bases for the criticism were, first, that the Bill will infringe an individual's right to privacy and, secondly, that the division of costs between the State and the TSPs placed an onerous financial burden on the latter, which was unfair.[18]

Pursuant to this process, ROICA was signed into law on 30 December 2002.[19] The long title of ROICA states that its objects include inter alia the regulation of the interception and monitoring of communications, the interception of postal articles and communications, and the monitoring of communications in the case of a serious offence or if the security or other compelling national interests of the Republic are threatened. In addition, it prohibits the provision of certain telecommunications services that do not have the capacity to be monitored, and regulates authorised telecommunications monitoring.

2. CONSTITUTIONAL FRAMEWORK

The use of electronic equipment to intercept and monitor telecommunications constitutes a prima facie invasion of the right to privacy. A Court may find that, in regulating interception and monitoring, ROICA also infringes the right to freedom of expression and dignity.[20]

[14] SALC Report (note 5 above) xiii-xxiii.
[15] This Bill was published in *Government Gazette* 22582 dated 17 August 2001 [B50-2001].
[16] *Government Gazette* 22582 (note 15 above); Memorandum on the objects of the Interception and Monitoring Bill, 2001.
[17] The written representations had to be submitted by no later than 13 August 2001 and the public hearings were scheduled for the third parliamentary term of 2001.
[18] Deputy Minister of Justice and Constitutional Development *Address on the second reading in the National Assembly on the Regulation of Interception of Communication and Provisioning of Communication-related Information Bill*, 17 September 2002.
[19] *Government Gazette* 24286 (note 9 above).
[20] S v A 1971 (2) SA 293 (T) at 297; See also *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A), where it was held that the recording of confidential business meetings and offering the tapes for sale to a third party was held to be an invasion of privacy.

2.1 Rights

The rights contained in the Bill of Rights are not absolute. No hierarchy of rights exists. Rather, the rights have to be read and interpreted in the light of other competing and conflicting or even complementary rights contained in the Bill of Rights. In addition, rights are limited by the general limitation clause.[21]

Furthermore, some of the rights including the right to freedom of expression, which will be discussed in greater detail below, contain specific internal limitations. Also, rights must be interpreted with regard to relevant public international law and may be interpreted with regard to comparative foreign case law.[22]

2.2 The right to privacy

The right to privacy is a universally accepted right.[23] Under the South African common law, the invasion of private communications per se was regarded as an invasion of privacy.[24] Section 14 of the final Constitution provides everyone with a right to privacy, which includes inter alia the right not to have the privacy of their communications infringed. The scope of the right to privacy extends only to those aspects of life or conduct to which a legitimate expectation of privacy can be harboured.[25]

The formulation of the South African constitutional right to privacy was drawn primarily from American and Canadian jurisprudence, notwithstanding that their own constitutions do not expressly protect the privacy of communications. The United States' Fourteenth Amendment has been interpreted to include a general right to privacy.[26] In Olmstead v United States Justice Brandeis, in a dissenting judgment, adopted the principle of the 'right to be let alone' in the context of a wiretapping case.[27] At that stage, the right to privacy was founded on the basis of the protection of private property. The US Supreme Court declined to extend such protection to include the privacy of communication; instead, it upheld the wiretapping on the basis that there had been no seizure of tangible property and that the eavesdropping had taken place without any physical invasion of property. Many years later, in Katz v United States the US Supreme Court ruled that a warrant was required for intercepting telephone conversations. To obtain a warrant a compelling State interest had to be shown.[28]

In Financial Mail (Pty) Ltd v Sage Holdings Ltd although the issue before the Court was whether the appellants, who had come into possession of certain tapes, were entitled to publish information on them, and not whether telephone tapping itself was an invasion of privacy, the Court held that telephone tapping was a manifestly unlawful invasion of privacy.[29]

---

[21] s 36 of the final Constitution.
[22] s 35 of the final Constitution.
[23] The right to privacy is expressly guaranteed in the Universal Declaration of Human Rights (art 17), the International Covenant of Civil and Political Rights (art 17), the European Convention on Human Rights (art 8) and the American Convention on Human Rights (art 11) and a number of domestic Bills of Rights. In respect of the latter see LM du Plessis and J de Ville 'Personal Rights: Life, Freedom, and Security of the Person, Privacy and Freedom of Movement' in D van Wyk et al (eds) Rights and Constitutionalism (1994) 212.
[24] D McQuoid-Mason 'Privacy' in M Chaskalson et al (eds) *Constitutional Law of South Africa* (1996 3 rev 1998) 18-15.
[25] J de Waal, I Currie and G Erasmus *The Bill of Rights Handbook* 4 ed (2001) 269.
[26] De Waal et al (note 25 above) 267.
[27] 277 US 438 (1928).
[28] 389 US 347 (1967); GE Devenish *A Commentary on the South African Bill of Rights* (1999) 140.
[29] 1993 (2) SA 451 (A) at 462.

In Bernstein v Bester the right to privacy was characterised as lying along a continuum, where the more a person interrelates with the world, the more the right to privacy becomes attenuated.[30] In Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit NO (Hyundai) the Constitutional Court further elucidated on the Bernstein decision, stating that:

The right, however, does not relate solely to the individual within his or her intimate space. Ackermann J did not state in the above passage that when we move beyond this established 'intimate core', we no longer retain a right to privacy in the social capacities in which we act. Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the State unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.[31]

In addition, the distinction between substantive privacy rights and information privacy rights is essential in the consideration of the right to privacy of communications. Substantive privacy rights relate to controversial matters that impact on individuals or small groups of persons. Information privacy rights refer to the ability of persons to acquire, publish or employ information about others without their consent. Privacy of communications is generally regarded as falling into the latter category.[32] Any forms of information imparted by telecommunicated means, fall by definition within this category. The general prohibition on interception and monitoring emphasises and gives effect to the right to privacy, as entrenched in the Constitution, not to have the privacy of communications infringed.

As the right to information privacy is intended to curb the use by third parties of information imparted by way of confidential communications (or communications reasonably apprehended or expected to be confidential), there cannot be a subjective expectation of privacy by one party to a communication vis-à-vis another party to the same conversation.[33] Accordingly, parties to a communication are at liberty to use the information obtained to the extent that it is neither privileged nor imparted on the basis that it should remain confidential.

In Protea Technology Ltd v Wainer the respondents argued that the transcripts of telephone calls recorded by means of a surveillance device sought to be used as evidence against them were inadmissible on the basis that their use contravened the general prohibition against interception as contained in section 2 of the IM Act. The Court considered issues of privacy and found that the evidence was not inadmissible in civil proceedings. The Court rejected the argument that the evidence should be inadmissible on the basis that it contravened the respondents' right to privacy of their communications. It held that, in respect of telephonic conversations pertaining to the employer's affairs at the employer's business, there was no legitimate expectation of privacy and the employer was entitled to access such conversations. In other words, the Court held that privacy only extended where there existed a legitimate expectation to privacy, which had to be determined on an objective basis.[34]

[30] 1996 (2) SA 751 (CC).
[31] 2001 (1) SA 545 (CC) para 16.
[32] Devenish (note 28 above) 147-150.
[33] De Waal et al (note 25 above) 287.
[34] Protea (note 6 above).

In S v Kidson Cameron J held that the formulation in the Protea matter as to what constituted confidential information was overbroad and added that 'the information the communicator intended to restrict as confidential must be information upon which the law attributes the confidentiality'.[35]

In Waste Products Utilisation (Pty) Ltd v Wilkes and Another the defendants argued that as the tape recordings were made in contravention of the IM Act, the contravention precluded the admissibility of the tape recordings so obtained in breach of a statutory provision and in a manner which infringed the constitutional right to privacy.[36] The defendants did not argue that the contravention of the IM Act itself rendered the tape recordings inadmissible and this was accordingly not decided.

The aforementioned decisions indicate that the right to privacy has been developed on a case-by-case basis with the content of the right being defined with specific reference to the facts of a particular case.

To determine whether the right to privacy has been infringed, a balance must be struck between the right of individuals to be left alone and the right of the State to infringe the individual's privacy in order to achieve some State objective, for example, crime prevention. The Constitutional Court adopted the view, as espoused by the United States, that individuals retain the right 'to be left alone by the state unless certain conditions are met'.[37] Further in Mistry v Interim Medical and Dental Council of South Africa and Others it was held that the more public the undertaking and the more closely it would be regulated, the more attenuated would the right to privacy be and the less intense any possible invasion.[38]

> [T]he regulation of electronic surveillance protects us from a risk of a different order, ie not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.

The reason for this protection is the realisation that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.[40]

In developing interception and monitoring legislation consistent with the values of the Constitution, there must be a balance between the need to make legislative provision equipping law-enforcement with the means to combat crime and the need to retain a modicum of privacy of communications. A number of foreign

[35] 1999 (1) SACR 338 (W).
[36] 2003 (2) SA 515 (W) at 550. *See also S v Naidoo and Another* 1998 (1) SACR 479 (N) and *Tap Wine Trading CC and Another v Cape Classic Wines (Western Cape) CC and Another* 1999 (4) SA 194 (C), where the reasoning of Heher J in *Protea Technology* (note 6 above) was approved. See also *S v Dube* 2000 (2) SA 583 (N) at 610.
[37] *Hyundai* (note 31 above).
[38] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC) para 27.
[39] *R v Thompson* [1990] 2 SCR 1111.
[40] *R v Duarte* [1990] 1 SCR 30 at 44.

jurisdictions in their interception laws provide for the establishment of a government body that has an obligation to provide reports publicly on the use of electronic surveillance. These reports would provide summary details about the number of uses of electronic surveillance, the types of crime they are authorised for, their duration and other information. Reports of this nature promote openness and transparency and limit any potential abuse of the right to privacy. They also act as an oversight on law-enforcement.

ROICA, however, does not provide for public reporting of information. Furthermore, there are no provisions made in ROICA, once an investigation has been completed, to inform individuals whether their communications had been intercepted or their transactional information collected that accessed. A duty to so inform may act as a further check on law-enforcement and counter-balance any invasion of the right to privacy.

2.3 The right to freedom of expression

Freedom of expression is a widely recognised right contained in a multitude of international instruments.[41] It has been applied not only in respect of the content of the information but also with reference to the means of transmission or reception, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.[42] In S v Mamabolo (E TV and Others Intervening) the following was said:

Freedom of expression, especially when gauged in conjunction with its accompanying fundamental freedoms, is of the utmost importance in the kind of open and democratic society the Constitution has set as our aspirational norm. Having regard to our recent past of thought control, censorship and enforced conformity to governmental theories, freedom of expression — the free and open exchange of ideas — is no less important than it is in the United States. It could actually be contended with much force that the public interest in the open market-place of ideas is all the more important to us in this country because our democracy is not yet firmly established and must feel its way. Therefore, we should be particularly astute to outlaw any form of thought control, however respectably dressed.[43]

Section 16(1) of the final Constitution protects free expression generally but also specifically provides for freedom of the press and media, the freedom to receive or impart information and ideas, artistic creativity, academic freedom and scientific research. Section 16(1) expressly protects the freedom of expression in a manner that does not warrant a narrow reading.[44] It protects speech and any form of

[41] Freedom of expression is expressly guaranteed in the Universal Declaration of Human Rights (art 19); the International Covenant of Civil and Political Rights (art 19), the European Convention on Human Rights (art 10); American Convention on Human Rights (art 13) and a number of domestic Bills of Rights. See also *Islamic Unity Convention v Independent Broadcasting Authority* 2002 (4) SA 294 (CC) para 28.

[42] *In Autronic AG v Switzerland* 12 EHRR 485 the European Court of Human Rights held that art 10(1) of the European Convention which provides for freedom of expression, applied not only to the content of the information but also to the means of transmission or reception, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.

[43] 2001 (3) SA 409 (CC) para 37; *Islamic Unity Convention v Independent Broadcasting Authority* (note 41 above) paras 25-36; *Phillips and Another v Director of Public Prosecutions, Witwatersrand Local Division, and Others* 2003 (3) SA 345 (CC) para 39.

[44] *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and Others* 2004 (1) SA 406 (CC) para 48.

[45] Devenish (note 28 above) 191; G Marcus and D Spitz '*Expression*' in Chaskalson et al (note 24 above) 20-17. See *Irwin Toys Ltd v Quebec (A-G)* [1989] 1 SCR 927 at 931 and 933 for the Canadian approach to 'speech' and 'expression'. The Canadian Supreme Court defined expression in terms of which 'activity is expressive if it attempts to convey meaning'. The Court found that not all expression will be protected. What constituted protected expression would be determined on a case-by-case approach.

[46] s 16(2) puts some forms of expression, such as propaganda for war, incitement of imminent violence and certain forms of hate speech, outside the scope of the right.

human expression,[45] including communications and telecommunications.[46] Any restriction by means of interception and monitoring is prima facie an infringement of the right to communicate, and as such constitutes an infringement of the right to freedom of expression. In addition, to the extent that TSPs may decrease in number as a result of increasing costs of licensing or compliance with the stringent requirements contained in ROICA, communication may be impeded and provisions of ROICA may be regarded as being a prima facie on infringement of the right to freedom of expression.

The protection of freedom of expression extends not only to the content of the speech or communication but also to the means by which it is transmitted or received.[47] In other words, the content of the right protects the giving and receiving of 'information and ideas, artistic creativity, academic freedom and scientific ideas'.[48]

The right to receive information and ideas has been described as the 'passive' reception of information as well as its 'active' collection. This is interpreted to mean that an individual does not have the right to insist on receiving any specific communication or information.[49]

In Case v Minister of Safety of Security the majority of the Constitutional Court expressed some doubt as to whether the right to freedom of expression included the reception of ideas by the receiver.[50] Mokgoro J (in a minority view) found that the right to freedom of expression embraced the right to 'receive, hold and consume expression transmitted by others', and thus the right to freedom of expression protected both the speaker and the recipients of the communication.[51]

The specific enumeration of a right to receive information and ideas in the final Constitution removes any doubt as to whether the right to freedom of expression aims to protect only speakers or both speakers and listeners.[52] The definition contained in section 16(1)(b) of the final Constitution, which provides that everyone has the right to freedom of expression, which includes freedom to receive and impart information and ideas, is, however, more limited in scope than the interpretation adopted by Mokgoro J in respect of the right contained in the interim Constitution.[53]

Notwithstanding, in order to invoke the right to receive information on behalf of receivers, listeners, holders and consumers, reliance would have to be placed on the general right to free expression, rather than its specific enumeration as contained in section 16(1)(b) of the final Constitution.

In addition, privacy rights of third parties must be balanced against the right to freedom of expression, including the receipt of information. In the exercise of the latter right, an individual may not intrude on the privacy rights of another. The

[47] In *Retrofit (Pvt) Ltd v Posts and Telecommunications Corporation (Attorney-General) Intervening* (1995) 9 BCLR 1262 (Z) the Court held that in the particular circumstances pertaining to the corporation's monopoly over public telecommunication services within, into and from Zimbabwe, which prohibited the establishment by Retrofit of a public mobile cellular telephone service, was an infringement of the fundamental right to freedom of expression. In *TS Masiyiwa Holdings (Pvt) Ltd* and *Another v Minister of Information, Posts and Telecommunications* 1998 (2) SA 755 (ZS) it was held that the cumulative impact of the structure of the regulations and the failure to implement the relevant provisions with reasonable expedition constitutes an abridgement of the constitutionally protected freedom of expression.

[48] Marcus et al (note 45 above) 20-17.

[49] Y Burns *Communications Law* (2001) 76.

[50] 1996 (3) SA 617 (CC) para 90. This matter dealt with the right to freedom of expression as enumerated in the interim Constitution, and the majority of the Constitutional Court did not support the decision of Mokgoro J.

[51] *Case v Minister of Safety of Security* (note 50 above) para 25.

[52] De Waal et al (note 25 above) 315; Devenish (note 28 above) 210.

[53] *De Reuck* (note 44 above) para 49.

extent to which the right to receive information and the right to privacy interact in the area of interception and monitoring depends on what would qualify as 'expression' for the purpose of invoking the right. As already stated, this would require a case-by-case assessment. The extent to which the right may be limited depends on whether the limitation requirements set out in section 36 of the final Constitution are complied with. In interpreting the right in the context of the interception and monitoring of private communications to fulfil a State objective, a Court would have to balance the conflicting interests of the right of the persons to communicate and be able to receive a communication with the need of the State to have access to such communication.

2.4 The limitation of a right

The rights contained in the Bill of Rights are not absolute and may be limited in terms of section 36 of the Constitution, which provides that the rights entrenched in the Bill of Rights may be limited only in terms of a law of general application and 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. Reasonableness plays an important role in the application of this limitation clause. There is no absolute standard for determining reasonableness; it is a process that requires the balancing of different interests.[54] In Prince v President of the Law Society of the Cape of Good Hope it was stated:

> To pass constitutional muster, the limitation on the constitutional rights must be justifiable in terms of section 36(1) of the Constitution. The limitation analysis requires an enquiry into whether the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. In that enquiry, the relevant considerations include the nature of the right and the scope of its limitation, the purpose, importance and the effect of the limitation, and the availability of less restrictive means to achieve that purpose. None of these factors is individually decisive. Nor are they exhaustive of the relevant factors to be considered. These factors, together with other relevant factors, are to be considered in the overall enquiry. The limitation analysis thus involves the weighing up of competing values and ultimately an assessment based on proportionality.[55]

ROICA is a law of general application as contemplated in section 36 and any interception or monitoring, in accordance with ROICA, would have to be tested against the requirements of the limitation clause in order to determine whether it would pass constitutional muster. What constitutes a reasonable and justifiable limitation will depend on the circumstances of each case. For example, where a law-enforcement officer is likely to require access to information to reasonably fulfil a governmental objective in circumstances where the request is proportional to the objective sought to be achieved, and there is no less restrictive manner of achieving such objective, it is likely to pass constitutional scrutiny.

It is contemplated in ROICA that the interception and monitoring of

[54] *S v Steyn* 2001 (1) SA 1146 (CC) para 30 and the authorities cited in note 50.
[55] 2002 (2) SA 794 (CC) para 45; *S v Jordan (Sex Workers Education & Advocacy Task Force as Amici Curiae)* 2002 (6) SA 642 (CC) para 85.

communications may be authorised by a judge only if there are no other less intrusive ways to investigate a crime or obtain evidence. This means that one has to determine whether the contemplated interception or monitoring is less invasive than a physical search or any other method of investigation. Therefore, a judge, before issuing a directive, must take into account whether the necessary information could reasonably be acquired by any other means.

The infringement of privacy and freedom of expression is an inevitable result of the interception and monitoring of communications. The constitutionality of a number of the provisions in ROICA — some of which are discussed below — is open to legal challenge with the Courts having to determine whether they are reasonable and justifiable as contemplated in section 36 of the Constitution.

3. THE SCOPE OF THE APPLICATION OF ROICA

3.1 Objectives

The long title identifies the following objects sought to be achieved by ROICA -

- to regulate the interception of certain communications;
- to monitor signals, radio frequency spectrum and the provision of communication-related information;[56]
- to regulate the making of application for, and the issuing of, directions authorising the interception of communications, entry warrants and the provision of communication-related information;
- to regulate the assistance to be given by postal service providers (PSPs), TSPs and decryption key holders (DKHs), in the execution of directions and entry warrants;
- to prohibit the provision of telecommunication services that do not have the capability to be intercepted;
- to provide for certain costs to be borne by certain TSPs;
- to provide for the establishment of interception centres, the Office for Interception Centres and the Internet Service Providers Assistance Fund;
- to prohibit the manufacturing, assembling, possessing, selling, purchasing or advertising of certain equipment; and
- to create offences and to prescribe penalties for such offences.

Its objectives are more far-reaching when compared with the IM Act. Unlike the IM Act, section 1 of ROICA defines 'communication' as including both a direct communication (non-electronic)[57] and an indirect communication (electronic).[58]

[56] s 1 of ROICA defines communication-related information as information that, among others, identifies the origin, destination, termination and duration of an indirect communication generated or received by a customer of a TSP, for example, information pertaining to who was called from a cellular number, where the call was made and the duration of the call.

[57] s 1 of ROICA defines a 'direct communication' as either an oral communication, other than an indirect communication between two or more persons, which occurs in the immediate presence of all the persons participating in that communication, or an utterance by a person who is participating in an indirect communication if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication. These would include face-to-face discussions between two or more persons and telephonic conversations overheard by a third party who is in the company of one of the callers.

[58] s 1 of ROICA defines an 'indirect communication' as the transfer of information, including a message or any part of a message, whether in the form of speech, music or other sounds, data, text, visual images whether animate or not, signals, or radio frequency spectrum or in any other form that is transmitted in whole or in part by means of a postal service or a telecommunication system.

Indirect communications include telephone conversations, the contents of an e-mail transmission,[59] facsimile, SMS, postal communication, and the downloading of information from the Internet. ROICA deals differently with the interception and monitoring of direct and indirect communications.

ROICA is aimed primarily at regulating the interception and monitoring of telecommunication surveillance of both direct and indirect communications by law-enforcement officers and agencies (as defined in section 1 of ROICA), for the purpose of gathering evidence during the investigation of crimes and in the interests of maintaining justice, public health or safety, national security or to achieve similar objectives. It stipulates the circumstances under which law-enforcement officers may apply to a designated judge for the issuance of an interception direction. It prescribes how these directions are to be executed. Section 1 of ROICA defines a designated judge as any judge of a High Court discharged from active service under section 3(2) of the Judges' Remuneration and Conditions of Employment Act, 47 of 2001, or any retired judge so designated by the Minister to perform the functions of a designated judge in ROICA.[60] Although only designated judges may issue directions and entry warrants, directions for archived-related information may be issued by any judge or magistrate exercising their powers under any other law, for example, section 205 of the Criminal Procedure Act, 51 of 1977.

It is clear from the objectives contained in ROICA that, although its primary focus is assisting law-enforcement officers in procuring information required to combat crime, it also regulates interception and monitoring in the private sphere. This chapter considers the business environment and the regulation of employee communications by an employer as regulated by ROICA.

3.2 Interception

The IM Act deals separately with interception and monitoring; ROICA deals with interception and monitoring in the same way. Section 2(1)(a) of the IM Act prohibits the interception of communications before, during and after it is in progress. The IM Act does not prohibit interception of a communication:

- if the interception is not intentional;
- if the dispatcher knows that his or her communication is being intercepted or gives prior permission for such interception (the exception applies only to the dispatcher and not the recipient or intended recipient); or
- if the communication is not electronic (ie 'transmitted by telephone or in any other manner over a telecommunications line').

The IM Act does not define 'intercept' or 'interception'. Section 1 of ROICA defines 'intercept' as 'the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of the communication available to a person

[59] s 1 of ROICA defines 'contents' in the context of any communication as including any information concerning the substance, purport or meaning of that communication, that is, the actual communication and the contents of the intention contained in the communication.

[60] Since the inception of the IM Act, however, only one retired judge had been appointed for all the Divisions of the High Court and that judge has been considering all applications for interception and monitoring (SALC Report (note 5 above) para 2.3). Ostensibly, the use of retired judges for this purpose is to ensure that the judge would not be the same judge who would eventually hear the matter in the Court in which intercepted communications are sought to be produced in evidence.

other than the sender or recipient or intended recipient of that communication and includes the -

- monitoring of any such communication by means of a monitoring device;
- viewing, examination or inspection of the contents of any indirect communication; and
- diversion of any indirect communication from its intended destination to any other destination.

Interception has a corresponding meaning. A reference in ROICA to the interception of a communication does not include a reference to the interception of any indirect communication that is broadcast or transmitted for general reception.[61]

Section 1 of ROICA defines an interception device as 'any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus to intercept any communication' and includes monitoring devices. It specifically excludes:

(a) any instrument, device, equipment or apparatus or any component thereof
  (i) furnished to the customer by a telecommunication service provider in the ordinary course of his or her business and which is used by the customer in the ordinary course of his or her business; [62]
  (ii) furnished by such customer for connection to the facilities of such telecommunication service and used in the ordinary course of his or her business;
  (iii) being used by a telecommunication service provider in the ordinary course of his or her business; or
(b) a hearing aid or similar device being used to correct below normal hearing to not better than normal.

The Minister of Justice and Constitutional Development may, by notice in the Government Gazette, declare any electro-magnetic, acoustic, mechanical or other instrument, device or equipment capable of being used as interception devices, as listed equipment.[63] As a consequence, no person is allowed to manufacture, assemble, possess, sell, purchase or advertise such listed equipment unless granted a certificate of exemption under section 46 of ROICA.[64] This is consistent with the approach adopted in the United States, where the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices are prohibited.[65] In contrast, the French regulate the trade of surveillance devices by decree and provide a list of devices intended to pick up conversations at a distance. After consultation with the Conseil d'Etat, the manufacture, importation, possession, display, offering, rental or sale of such devices is listed by ministerial authorisation.[66]

[61] s 2(3) of ROICA.
[62] s 1 of ROICA defines a 'customer' as any person to whom a TSP provides a telecommunication service or who has entered into a contract with a TSP for the provision of a telecommunication service, including a pre-paid telecommunication service.
[63] s 44 of ROICA.
[64] s 45(2) read with s 46 of ROICA.
[65] Omnibus Crime Control and Safe Streets Act 1968, now codified as 18 USC §§ 2510-2520 (1994).
[66] SALC Report (note 5 above) para 2.24.

For purposes of ROICA, interception of a communication takes place in South Africa if, in the case of a direct communication, it is effected by conduct within South Africa or, in the case of an indirect communication, in the course of its transmission by means of a postal service or telecommunication system.[67] In respect of indirect communications, section 1(2)(b) of ROICA provides that 'the time during which an indirect communication is being transmitted by means of a telecommunication system includes any time when the telecommunication system by means of which such indirect communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it'. This provision is similar to that found in the prohibition on interception in the IM Act, which expands the ambit of interception and thus the ambit of the prohibition. It appears that the drafter intended to extend the ambit of interception and, therefore, also the ambit of the prohibition up to end-user computers.

3.3 Monitoring

'Monitor' is defined in the IM Act to include 'recording of conversations or communications by means of a monitoring device', and 'monitoring device' is defined as 'any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication'. It proscribes the intentional monitoring of a conversation or a communication by way of a monitoring device so as to gather confidential information concerning any person, body or organisation.[68] The prohibition on monitoring, however, does not apply:

- if the monitoring is not intentional; and
- if the monitoring is for any reason other than to 'gather confidential information'.

Section 1 of ROICA encompasses monitoring within its definition of 'intercept' and similarly, interception devices include all monitoring devices. ROICA does, however, extend the definition of 'monitor' as provided for in the IM Act to include the listening to, or recording of, communications by means of a monitoring device. Section 1 of ROICA also defines a monitoring device more precisely than the IM Act. It includes any electronic, mechanical or other instrument, device, equipment or apparatus, to listen to or record any communication. In terms of this definition, a computer would constitute a 'monitoring device' in that it can be used, either on its own or in combination with a modem, to 'listen to' or to record a communication. Most monitoring devices would also be considered as interception devices.

[67] s 1(2)(a) of ROICA.
[68] s (1) of the IM Act. The *Shorter Oxford Dictionary* defines 'monitor' as 'to listen to and report on (radio broadcasts, especially from a foreign country); also to eavesdrop on (a telephone conversation)'.
[69] This section draws from various unpublished works authored by Lisa Thornton of Lisa Thornton, Inc.

4. PROHIBITION ON INTERCEPTION AND MONITORING[69]

4.1 General prohibition

Section 2(1)(b) of the IM Act provides that no person may intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any persons, body or organisation. Thus, unlike the prohibition regarding interception, the prohibition on monitoring goes beyond electronic communication and includes direct 'conversations'. For example, an employee's e-mail may be monitored:

- if the monitoring is not intentional;
- if the monitoring is for any reason other than to gather confidential information concerning any persons, body or organisation;[70] or
- if the person is a party to the communication.

The only other exception to the prohibition on interception and monitoring explicit in the IM Act is where a judge issues a direction authorising interception and monitoring.[71] The Courts have also determined that the IM Act — and therefore the prohibitions on interception and monitoring — does not apply to interception or monitoring of a party to the communication or conversation (with the exception of police, defence force and intelligence personnel).[72]

Section 2 of ROICA provides: '[s]ubject to this Act, no person may intentionally intercept or attempt to intercept or authorise or procure any other person to intercept or attempt to do so, at any place in South Africa, any communication in the course of its occurrence or transmission'. Any interception in contravention of this clause may constitute a criminal offence, which carries a maximum fine of two million rands or a maximum term of imprisonment of 10 years.[73]

No TSP may intentionally provide any real-time or archive communication-related information to any person other than its customer to whom such information relates. To do so would be an offence in terms of ROICA.[74] A TSP, however, is obliged to provide such information when addressed with a real-time communication or archived communication-related written direction or upon written authorisation given by the customer. Such authorisation must be given each time such a request is made, and may be subject to any or varied conditions determined by the customer concerned.[75]

The aforementioned procedures do not preclude the use of any other Act, for example the Criminal Procedure Act, where applicable, to obtain information. The continued use of procedures contained in existing laws may result in the provision of ROICA being circumvented, particularly as ROICA does not repeal other laws

[70] In determining whether the exception applies, one should have regard to the purpose for which the monitoring occurs. See *Protea Technology Ltd and Another v Wainer* (note 6 above). Confidential information is different from information that is intended by the communicator to be private. See also *Kidson* (note 35 above).
[71] s 2(2) of the IM Act.
[72] See *S v Dube; S v Kidson*, and *Tap Wine Trading* (note 36 above).
[73] s 49(1) of ROICA.
[74] ss 12 and 50 of ROICA.
[75] ss 13 and 14 of ROICA.
[76] s 15(1) and (2) of ROICA.
[77] s 42(1) and (3) of ROICA.

that permit the retrieval of information from a telecommunication system.[76]

A PSP, TSP or DKH, or any of their employees, may also not disclose any information that he or she obtains in the exercise of his or her powers or performance of his or her duties in terms of ROICA.[77] To do so would constitute an offence in terms of section 51(1)(a)(i) of ROICA.

4.2 Exemptions under ROICA

Similar to the IM Act, section 3(a) of ROICA allows authorised persons to intercept any communication in accordance with an interception direction issued by a judge. Other exceptions include:

- unintentional interception;[78]
- interception by a party to the communications;[79]
- interception with the written consent of one of the parties to the communications;[80]
- interception of indirect (electronic) communications in the carrying on of any business;[81]
- interception by certain law-enforcement personnel to prevent serious bodily harm;[82]
- interception by certain law-enforcement personnel to determine the location of a person in an emergency;[83]
- interception in a prison;[84]
- monitoring of signals by persons responsible for installing, operating and maintaining equipment in carrying out such duties;[85] and
- monitoring of the radio frequency spectrum by Icasa.[86]

ROICA draws distinctions between parties to a communication who are law-enforcement officers and those who are not. A number of the exemptions dealing with parties to a communication who are not law-enforcement officers, are briefly discussed below with specific reference being made to the employer-employee environment.

4.2.1 Interception of communication by a party to the communication

A party to a communication may intercept any communication, unless it is being done for purposes of committing an offence.[87] A 'party to a communication' in respect of a direct communication refers to any person who participates in such direct communication or to whom such direct communication is directed or in whose immediate presence such direct communication occurs and is audible to the person concerned, regardless of whether or not the direct communication is

[78] s 2 of ROICA.
[79] s 4 of ROICA.
[80] s 5 of ROICA.
[81] s 6 of ROICA.
[82] s 7 of ROICA.
[83] s 8 of ROICA.
[84] s 9 of ROICA.
[85] s 10 of ROICA.
[86] s 11 of ROICA.
[87] s 4(1) of ROICA; s 4(2) applies in respect of law-enforcement officers.

specifically directed at him or her. In respect of an indirect communication, the party to the communication is defined in section 1 of ROICA as:

- the sender or the recipient or intended recipient of such indirect communication;
- if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients; and
- any other person who, at the time of the occurrence of the indirect communication, is in the immediate presence of the sender or the recipient or intended recipient of that indirect communication.

4.2.2 Interception of communication with the consent of a party to the communication

A person may intercept any communication if one of the parties to the communication gives prior written consent to such interception, unless such communication is intercepted by such person for the purpose of committing an offence.[88] This provision is similar to that contained in the IM Act which provides that if a dispatcher knows that his or her communication is being intercepted or gives permission for such interception, then it is permitted.

However, unlike the IM Act, in ROICA the consent must be in writing and given prior to the interception occurring. It may be given by any one of the parties to the communication. A general consent obtained by employers as part of the terms and conditions of employment (in an employment contract, policy, practice or procedure or other relevant document in the employment environment) to intercept personal employee communications may be construed as a prior 'consent in writing' as contemplated in section 5 of ROICA. It is unlikely that the reference to 'consent in writing to such interception' in section 5 would require that consent must be obtained each time an interception is sought. However, employers who include 'a general consent for interception' as part of the conditions of employment or include such consent in an employment contract, must ensure that the scope of the consent is drafted in a manner which ensures that at the time the employee agreed to the interception the employee understands the ambit of what he or she agrees to. It is unlikely that this provision would apply in respect of police informer traps. Consent from one of the parties to the recording would not be regarded as sufficient authority to allow the interception as law-enforcement officers are compelled to procure a direction authorising such interception.[89]

4.2.3 Interception of communications in a business[90]

Interception of communication in business has broad application. It has particular application in the work environment and the employer-employee relationship in respect of the monitoring and/or accessing of employees' e-mails, monitoring of

[88] s 5(1) of ROICA; s 5(2) read with s 16(5)(a) applies in respect of law-enforcement officers.
[89] *R v Duarte* (note 40 above).
[90] s 1 of ROICA defines a 'business' as any business activity conducted by any person, including the activities of any private or public body.

websites accessed by employees, and recordings of the content of telephone calls made by employees. Its application is considered with particular reference to e-mail interception.

4.2.3.1 Direct communications

Under the IM Act an employee's communications may be intercepted (before it is sent/received, while being sent/received and after it is being sent/received) if:[91]

- Such interception is unintentional. However, it may be argued that when an employer intercepts business-related e-mails and in the process also intercepts employees' personal e-mail, he or she does not do so intentionally and, thus, does not contravene the IM Act. However, to the extent that an employee is permitted to use the business communication system for personal e-mail, it is arguable that the employer must expect that there would be personal e-mail. As such by retrieving all e-mail on a system it would, arguably, be doing so intentionally.
- The dispatcher of the e-mail knows that his or her communications are being intercepted or gives permission for such interception. The exception applies only to the dispatcher and not to the recipient or intended recipient. As such, outgoing (ie dispatched) e-mail may be intercepted if all of those who use the e-mail system are informed accordingly, but incoming e-mail may not be intercepted unless the sender can be informed prior to sending the e-mail that it may be intercepted. This, however, is unlikely to occur.
- If you are a party to the communication. Personal e-mails remain protected and unless a company completely prohibits the use of its e-mail systems for personal use and enforces this prohibition, personal employee e-mails would not be considered e-mail of the company as the company is not 'a party to the communication'.

The general prohibition contained in section 2 of ROICA applies to the interception and monitoring of direct communications that occurs in the carrying on of a business. Thus, any interception and monitoring of direct communications by an employer can take place only if the employer is party to the communication or with the prior written consent of one of the parties to the direct communication.

4.2.3.2 The exemption relating to indirect communications

The interception and monitoring of indirect (electronic) communications in business is regulated by section 6 of ROICA. The purpose of section 6 appears specifically to provide an exception to the prohibition on interception allowed by employers inter alia to intercept the personal indirect communications of employees in certain circumstances, and where such employees have not given their prior written consent. In terms of section 6, the type of communication that may be intercepted is very wide and the conditions imposed are not very strict. Section 6 of ROICA has to some extent been modelled on the United Kingdom

[91] s 2(1) of the IM Act.
[92] s I 2000 No 2699.

Telecommunications (Lawful Business Practice) (Interception of Communications) ('the British Regulations').[92]

Section 6(1) of ROICA provides the exception and section 6(2) sets out conditions that have to be met before the exception applies. Section 6(1) states that any person may, in the course of carrying on any business, monitor, intercept or examine any indirect communications. That section limits the meaning of an indirect communication:

- to the means by which a transaction is entered into in the course of that business [section 6(1)(a)];[93]
- which otherwise relates to that business [section 6(1)(b)];[94] or
- which otherwise takes place in the course of carrying on that business [section 6(1)(c)];[95]

in the course of its transmission over a telecommunication system.[96]

Although section 6(1)(a) specifically refers to communication 'by means of which a transaction is entered into' and section 6(1)(b) specifically refers to communication that 'relates' to a business, section 6(1)(c) refers generally to communication that takes place 'in the course of carrying on of that business'. It is arguable that most (if not all) personal indirect communication of employees, where such employees make use of employers' communications systems, falls within the exception set out in section 6(1)(c) of ROICA.

Section 6(2)(b) provides that a person may intercept an indirect communication as indicated above only if –

- the interception is 'for purposes of' monitoring or keeping a record of indirect communications:[97]
- in order to establish the existence of facts [section 2(1)(b)(i)(aa)];
- for purposes of investigating or detecting the unauthorised use of the employer's telecommunication system [section 2(1)(b)(i)(bb)], or
- where it is undertaken in order to secure, or is an inherent part of the effective operation of such system [section 2(1)(b)(i)(cc)];[98] or
- monitoring indirect communications made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose. [99]

This does not place an onerous obligation on the employer, nor does it limit the exception very much. As long as an employer understands that it may intercept e-

[93] s 6(1)(a) of ROICA.
[94] s 6(1)(b) of ROICA.
[95] s 6(1)(c) of ROICA.
[96] According to s 51 of ROICA, contravention of s 6 constitutes an offence punishable by a maximum fine of two million rands or imprisonment for a period not exceeding 10 years.
[97] s 6(2)(b)(i) of ROICA.
[98] For example, detecting spam and unusual e-mail traffic, detecting hardware and software problems or errors, monitoring viruses or preventing hackers from getting into the system.
[99] s 6(2)(b)(ii) of ROICA.

mail only for one or more of the stated purposes, there should be no problem in meeting the condition.

Section 6(2)(a) provides that communication may be intercepted only by the system controller or with the express or implied consent of the system controller.[100] Section 6(2)(c) states that such interception may occur if the telecommunication system concerned is provided for use wholly or partly in connection with that business, and if the system controller has made all reasonable efforts to inform in advance all individuals using the telecommunication system that indirect communication transmitted through it may be intercepted or if such indirect communication is intercepted, it will be with the express or implied consent of the user of the system.[101] The consent of the system controller may be obtained through a general or specific letter of authority. It does not necessarily have to be obtained prior to the event or in writing. In fact, this condition would be complied with if the system controller made all reasonable efforts to inform the users of its communication systems of any interception or monitoring. Users can be informed by using, for example, e-mail signatures, employment contracts, and e-mail use policies.

Another means of ensuring that users are aware that the Internet usage is monitored and/or intercepted is by structuring employment contracts in a manner which includes an employee's consent to the monitoring of his or her e-mail, post and telephone conversations to the extent that it is a condition of employment. In addition, use can be made of an electronic agreement or so-called 'click-wrap agreements.' In terms of such agreements, an employee is deemed to have consented to the interception and monitoring of his or her Internet access when he or she clicks on the acceptance button (thereby accepting the terms of the click agreement) when logging onto the computer network of the business.[102]

Section 6 specifically deals with the interception that occurs in connection with the carrying on of a business. It may well mean that an employer is not entitled to monitor and intercept employee communications not connected with the carrying on of the business. An employer in such a case would need to obtain the employee's express written consent to be able to monitor and intercept such communications. Furthermore, section 6 does not apply once an e-mail or other message reaches its end-user as ROICA makes it clear that the interception must occur during the course of its transmission over a telecommunication system.

In light of the foregoing, it is clear that an employer may not access an employee's e-mail box without permission and unless its purpose for doing so falls within the exceptions contained in section 6. To do so otherwise would constitute an infringement of the employee's right to privacy. When permitted to do so, however, an employer, as part of its monitoring and interception, may intercept or monitor e-mail and Internet usage both in respect of the content of the communication as well as the website or e-mail address which the employee uses either for sending or retrieving information in the course of its transmission over the telecommunication system.

The British Regulations, on which section 6 was modelled, consider a

[100] A 'system controller' is defined in s 1 of ROICA. This definition differentiates between public and private entities but regards the chief executive officer, equivalent officer or a person duly authorised, as being the system controller.
[101] s 6(2)(d) of ROICA.
[102] These 'click-wrap' agreements have been legalised under the Electronic Communications and Transactions Act, 25 of 2002.

communication that serves as the means through which a transaction is entered into in the course of the business (or which otherwise relates to that business or which otherwise takes place in the course of the carrying on of that business) as a communication that is relevant to that business. The British Regulations list as a legitimate purpose the monitoring of communications in order to determine whether or not they are relevant to the employer's business. Thus, although section 6 does not condone the blanket monitoring of personal communication, without the employee's consent, it would allow for the interception of communications transmitted on the employer's communication system for the purpose of establishing whether or not a communication relates to the business of the employer.

It is evident from the British Regulations that:

- Interception and monitoring for purposes of crime prevention must be undertaken by law-enforcement officers. Private individuals and companies are not authorised to intercept communications under the guise of crime detection and prevention. Therefore, employers cannot justify interception of business-related communications on the basis that they are trying to prevent fraud and corruption.
- Although the British Regulations allow the monitoring of communications to ascertain compliance with regulatory or self-regulatory practices or procedures and to ascertain or demonstrate the standards that are achieved or ought to be achieved by persons using the system, ROICA does not make similar provision. IN TERMS OF ROICA, an employer cannot use this as a basis to justify the interception of employee communications without the employee's consent. Employers can, however, argue that interception for purposes of detecting unauthorised use of the system includes issues of non-compliance with business policies and regulatory practices and as such are permissible.[103]

The legitimate purpose provisions of ROICA are aimed at balancing employees' rights to privacy with the need for employers to prevent the misuse and abuse of telephones, e-mail and the Internet, as well as to protect their communication systems from viruses, spam, hackers and other threats. In this regard it is clear that interception of communications for purposes of detecting hardware and software problems or errors, viruses, hacking and other threats to the system would qualify as measures taken 'to secure ... the effective operation of the system' and would be regarded as a legitimate basis for intercepting and monitoring indirect communications during the course of transmission.[104] It is evident that section 6 permits the monitoring and interception of the e-mail of employees and others who use e-mail systems in a business for the purpose of detecting and eliminating viruses and the like, and for the purpose of maintaining control over company communications where it serves a legitimate business interest and is done in the course of carrying on a business by or under the approval of the system

[103] s 6(2)(b)(i) of ROICA. See T Bortz and L Louw 'The Regulation of Interception of Communications and the Provision of Communication-related Information Act 70 of 2002' *Tech Werks* (March 2003) 4-5.
[104] Bortz and Louw (note 102 above) 4.

controller.[105] Employers should inform employees, consultants and others who use their e-mail systems of the company's e-mail policy. Employees should also advise them of the circumstances under which the employer is entitled to monitor and intercept the use of its telephone, facsimile facilities, Internet and e-mail. Care should be taken to include a specific provision that informs the user that e-mail, including personal e-mail, may be monitored and intercepted by the employer. Employees should similarly be advised to inform the recipients of their e-mails that their e-mails may be monitored and intercepted. An easy method of informing users that e-mails may be monitored and intercepted is to make this information an integral part of the log-on procedures or by way of e-mail signatures informing users that the e-mail may be monitored and intercepted.

4.2.4 Interception of communications to prevent serious bodily harm

Only law-enforcement officers may intercept communications to prevent serious bodily harm. If the law-enforcement officer is of the opinion that the communication must be intercepted urgently and it is not reasonably practicable to do so pursuant to an oral or written direction, he or she may do so without such direction.[106] When faced with a request, a TSP 'must' (the provision is peremptory) route the duplicate signals of the indirect communication concerned to the designated interception centre.[107] An interception centre is established in terms of section 32(1)(a) of ROICA for purposes of interception in terms of ROICA. Interception centres fall under the control of the Minister of Justice and Constitutional Development.

4.2.5 Interception of communications for purposes of determining locations in case of an emergency

Section 8 of ROICA regulates the interception of communications for purposes of determining the location of a party to a communication in the case of an emergency. This type of interception can be done only by a law-enforcement officer, who would then request the necessary information from the relevant TSP, who can intercept the communication from the sender. This section is invoked when a law-enforcement officer is of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency. If the party to the communication is not a law-enforcement officer, he or she should inform a law-enforcement officer of the matter and cannot personally make the request to determine the location of the sender. A TSP, on receipt of such a request, must comply and provide the location, together with any other information, which, in the opinion of the TSP concerned, is likely to be of assistance in dealing with the emergency.[108] The TSP may do so in any manner that it deems appropriate.

[105] s 6(2) of ROICA.
[106] s 7(1)(b) of ROICA.
[107] s 7(2) of ROICA.
[108] s 8(3) of ROICA.
[109] Defined in s 1 of the Correctional Services Act, 111 of 1998.
[110] s 9 of ROICA.
[111] Ibid.

4.2.6 Interception of communications authorised by other legislation

Any communication may in the course of its occurrence or transmission be intercepted in any prison[109] if such interception takes place in the exercise of any power conferred in terms of any regulations under the Correctional Services Act.[110] Other exceptions to the prohibition on interception are the interception of communication in terms of other laws, for example, in terms of provisions of the Defence Act, 44 of 1957.[111]

4.2.7 Monitoring of signals and radio frequency spectrum

Any person who is lawfully engaged in duties relating to the:

- installation or connection of any equipment, facility or device used, or intended to be used, in connection with a telecommunications service;
- operation or maintenance of a telecommunication system; or
- installation, connection or maintenance of any interception device used, or intended to be used, for the interception of a communication under an interception direction,

may in the ordinary course of the performance of such duties monitor a signal relating to an indirect communication where it is reasonably necessary to do so in the performance of his or her duties.[112]

In terms of section 11 of ROICA, an inspector appointed in terms of section 98 of the Telecommunications Act may, when engaged or performing functions relating to the management of the radio frequency spectrum, monitor radio frequency spectrum relating to an indirect communication, where it is reasonably necessary to monitor that spectrum, for purposes of identifying, isolating or preventing an unauthorised or interfering use of such frequency or of a transmission.

5. DIRECTIONS IN ROICA

An interception direction is a written direction issued by the designated judge on request of an applicant[113] authorising the interception of communication, addressed to a PSP or TSP and executed by a law-enforcement officer. Only law-enforcement officers may intercept communications on receipt of a direction from the designated judge.[114] An interception direction may specify conditions or restrictions relating to the interception of the communications.[115]

There are essentially four kinds of direction that may be issued in terms of ROICA. These authorise:

- the interception of communications;
- the provision of communication-related information as soon as it becomes available (ie real-time communication-related information);

[112] s 10 of ROICA
[113] s 1 of ROICA defines an applicant to include certain police officers, certain members of the South African National Defence Force, certain members of the National Intelligence Agency, head of the Directorate or an Investigating Director of the National Prosecuting Authority and members of the Independent Complaints Directorate in certain circumstances.
[114] s 1 read with s 16(1) of ROICA.
[115] s 16(6)(c) of ROICA.

- the provision of communication-related information stored by a TSP (ie archived communication-related information); and
- DKHs to disclose decryption keys or to provide decryption assistance in respect of encrypted information.

5.1 Issuing of Directions

Section 1 of ROICA provides that law-enforcement officers may apply for directions. These include the police service, the defence force, the intelligence services and the Directorate of Special Operations.[116]

The issuing of an interception direction always lies within the discretion of the designated judge.[117] Strict criteria apply and the judge may issue an interception direction only if he or she is satisfied, on the facts alleged in the application concerned, that there are reasonable grounds to believe that:

- The matter involves the commission of a serious offence.[118]

(Section 16(5)(a)(i) of ROICA relates to serious offences that may be committed in the future. This provision may not withstand constitutional scrutiny on the basis that it speculates on future acts that have not yet occurred. It is comparable to the decision of the Constitutional Court in Hyundai that a search and seizure, for purposes of a preparatory investigation, would not be constitutionally justifiable in the absence of a reasonable suspicion that an offence had been committed. Search and seizures would be analogous to interception and monitoring of communication and the decision of the Court in respect of search and seizures would be equally applicable to interception and monitoring.[119])

- The information concerns an actual or potential threat to the public health or safety or national security or actual threat to compelling national economic interests of the country.[120]

(The use of the phrase 'national security' in section 16(5)(a)(ii) and (iii) of ROICA should not be interpreted so broadly that it can be used to justify any State action. If it is, it also runs the risk of being struck down by the Courts as being constitutionally overbroad.)

- The making of a request is to provide a competent authority outside South Africa with assistance in respect of organised crime or offences relating to terrorism and is in accordance with an international mutual assistance agreement or the interests of South Africa's international relations or obligations.[121]

[116] See also s 16(3) of ROICA.
[117] s 16(4) of ROICA.
[118] s 16(5)(a)(i) of ROICA. A 'serious offence' would include organised crime, conspiracies or offences that are financially lucrative for those committing them, as well as the 14 offences listed in the Schedule to ROICA. These include inter alia treason, terrorism, offences that result in a loss of life, genocide, crimes against humanity, war crimes and offences for which punishment may be imprisonment for life or for at least five years without an option of a fine.
[119] *Hyundai* (note 31 above).
[120] s 16(5)(a)(ii) and (iii) of ROICA.
[121] s 16(5)(a)(iv) of ROICA.

- The information concerns property that is or could probably be used in the commission of a serious offence or is or could probably be the proceeds of unlawful activities.[122]

(In terms of the IM Act a designated judge can issue a direction on the grounds contained in the written application if the judge is convinced that the communication sought to be intercepted or monitored involved a serious offence that cannot properly be investigated in any other manner[123] or that it was necessary to preserve the security of the country.[124] As indicated above, in terms of ROICA a designated judge would need to be 'satisfied' of the aforementioned criteria before granting a direction.[125] In practice, the distinction between the provision contained in the IM Act and ROICA may have the effect that a judge would no longer need to be assured that the direction is essential for the purpose for which it is being sought, but can take the view that on a balance of probabilities it appears to be the case.)

- In terms of ROICA the judge must be satisfied on the facts alleged in the application that there are reasonable grounds to believe that the interception of the particular communications concerning the relevant ground referred to in section 16(5)(a) of ROICA as indicated above, will be obtained by means of such interception direction.[126] In addition, the judge must be satisfied that 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 grounds referred to in section 16(5)(a) of ROICA (as set out in the application) are commonly used by the person or customer in respect of whom the application for the interception direction is made.[127]

The judge must further be satisfied, in respect of a direction being sought relating to serious offences, potential threats to the public health or safety, national security or national economic interests, requests for international mutual legal assistance relating to organised crime and terrorism, and property which is or can be used in a serious offence or is the proceeds of unlawful activity,[128] that other investigative procedures have been applied and

- have failed to produce the required evidence, or
- reasonably appear to be unlikely to succeed if used, or
- are likely to be too dangerous to use in order to obtain the required evidence.[129]

In addition, there must be reasonable grounds to believe that the offence cannot be adequately investigated or the information cannot adequately be obtained in

[122] s 16(5)(a)(v) of ROICA.
[123] s 3(6) of the IM Act. The IM Act defines a 'serious offence' with reference to Schedule 1 of the Criminal Procedure Act, 51 of 1977, ss 13(f) and 14(b) of the Drugs and Drug Trafficking Act, 140 of 1992 and offences defined in s 2 of the National Prosecuting Authority Act, 32 of 1998. It excluded specific types of murder as well as, inter alia, rape and robbery, unless these were committed on an organised basis.
[124] s 3(1)(b) read with s 3(6) of the IM Act.
[125] s 16(5) of ROICA.
[126] s 16(5)(b)(i) of ROICA.
[127] s 16(5)(b)(ii) of ROICA.
[128] s 16(5)(a)(i), (iii), (iv) and (v) of ROICA.
[129] s 16(5)(c) of ROICA.

another appropriate manner.[130] This, however, does not apply in respect of serious offences involving organised crime or property used as an instrument of a serious offence and which could be the proceeds of unlawful activities.

5.2 Written and oral applications

An application for an interception direction in terms of section 16(2) of ROICA must:

- be in writing, save where ROICA allows for oral applications;
- indicate the identity of the applicant;
- contain the identity of the law-enforcement officer who will execute the interception direction, if known and appropriate;
- contain the identity of the person or customer, if known, whose communication is to be intercepted; and
- contain the identity the PSP or TSP to whom the direction is to be addressed, if applicable.[131]

An applicant who applies for an interception direction may in his or her application also apply for an entry warrant or do so at any stage after the issuing of the interception direction but before the expiry of the period for which it has been issued.[132] The application must specify the grounds on which the direction is sought and contain full particulars of all the facts and circumstances alleged by the applicant in support of the application, including:

- a description of the nature and location and facilities from which, or the place at which, the communication is to be intercepted, if known;
- the type of communication required to be intercepted; and
- the basis for believing that the evidence relating to the grounds on which the application is made will be obtained through the interception.[133]

An application for a direction must further indicate the period for which the direction is required and whether any previous application had been made in respect of the same person or customer, facility or place specified in the application and, if such previous application exists, the current status thereof.[134] In addition, the application must comply with any supplementary directives relating to applications for interception directions that may have been issued under section 58 of ROICA.[135] ROICA also makes provision for the oral application for a direction or an entry warrant:[136]

- by an applicant who would be entitled to make such an application in writing;

[130] s 16(5)(c) of ROICA.
[131] s 16(2)(a) read with s 16(6) of ROICA.
[132] s 22(1) of ROICA.
[133] s 16(2)(b)-(d) of ROICA.
[134] s 16(6)(d) of ROICA. It may be issued only for a period not exceeding three months at a time, although this period may be extended on application for a further period not exceeding three months.
[135] s 58 provides that a designated judge or, if there is more than one designated judge, all the designated judges jointly, may, after consultation with the respective Judge-Presidents of the High Courts, issue directives to supplement the procedure for making applications for the issuing of directions or entry warrants in terms of ROICA.
[136] Generally, all applications, directions and requests for entry warrants must be in writing: see s 23(5) of ROICA.

- if the applicant is of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application;[137]
- which application must contain such information as required by ROICA for the written application; and
- which application must indicate the particulars of the urgency of the case or the exceptional circumstances which, in the opinion of the applicant, justify the oral application and must comply with any supplementary directives relating to oral applications issued under section 58 of ROICA which may exist.[138]

A designated judge has a discretion whether to grant an oral application and can do so only if he or she is satisfied, on the facts alleged in the oral application, that there are reasonable grounds to believe that the direction or entry warrant applied for could be issued, that such a direction is immediately necessary on any of the grounds referred to in the relevant sections of ROICA and that it is not reasonably practicable to make a written application for the issuing of a direction or entry warrant.[139]

The applicant, however, must submit a written application to the designated judge concerned within 48 hours after the issuing of the oral direction or entry warrant.[140] In instances where a judge issues an oral direction, the judge must inform the applicant orally and, if applicable, the PSP or TSP to whom it is addressed, of such an oral direction or oral entry warrant, including the contents thereof and the period for which it has been issued, and must confirm that oral direction or oral entry warrant in writing within 12 hours after issuing it.[141]

5.3 Communication-related directions

ROICA also provides specific procedures for applying for, and issuing directions for real-time, communication-related information,[142] a combination-type application,[143] archived communication-related directions,[144] and decryption directions.[145] The procedure and the requirements to be fulfilled are essentially the same as those described above.

Decryption directions, however, are directed at persons in possession of any key, mathematical formula, code, password, algorithm or any other data which is used to allow access to encrypted information or to facilitate the putting of encrypted information into an intelligible form (decryption key) for purposes of subsequent decryption of encrypted information relating to indirect communications. Such person would be directed to disclose the decryption key or provide decryption assistance in respect of encrypted information. The designated judge must consider not only the efficacy of the interception direction without the decryption

[137] s 23(1) of ROICA.
[138] s 23(2) of ROICA.
[139] s 23(4) of ROICA.
[140] s 23(4)(b) of ROICA.
[141] s 23(10) read with s 23(7) and (8) of ROICA.
[142] s 17 of ROICA.
[143] s 18 of ROICA. There was no similar provision in the IM Act.
[144] s 19 of ROICA.
[145] s 21 of ROICA.

key or assistance, but also any adverse effect that the decryption direction may have on the business of the DKH.

5.4 Entry warrants

As already stated, an applicant for a direction may in the same application apply for an entry warrant or apply at any stage after the interception direction has been issued but before the expiry of the period or extended period for which the direction has been issued. Such applications for entry warrants must be writing, unless done orally under the circumstances explained above.[146] The application must indicate:

- the identity of the applicant;
- the premises in respect of which the entry warrant is required to be issued; and
- the specific purpose for which the application is made.

If the application is made only after an interception direction has been issued, then proof of the interception direction must be provided. This should be done by way of an affidavit setting forth the results obtained from the interception direction from the date of its issuance up to the date on which the application for the entry warrant is made. Alternatively, a reasonable explanation for the failure to obtain the aforementioned results must be provided.[147]

The applicant must also indicate whether a previous application for an entry warrant for the same purpose, or in respect of the premises specified in the application, has been issued, and the status thereof. The applicant also has to comply with any supplementary directives relating to applications for entry warrants that may have been issued.[148]

A designated judge has a discretion whether or not to issue an entry warrant, and will do so only if he or she is satisfied, on the facts alleged in the application, that entry onto the premises concerned is necessary for the purpose of intercepting a postal article or a communication or for the purpose of installing, maintaining or removing an interception device on or from any premises. The judge must also be satisfied that there are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception direction concerned otherwise than by the use of an interception device installed on the premises.[149]

5.5 Execution of directions

Only a law-enforcement officer may execute a direction issued in terms of ROICA,150 and must do so in the circumstances prescribed by ROICA. An applicant for a direction may authorise any number of authorised persons[151] deemed necessary to assist with the execution of the direction.[152] The direction may

[146] s 22(1) of ROICA.
[147] s 22(2)(b)(ii) of ROICA.
[148] s 22(2) of ROICA.
[149] s 22(3) and (4) of ROICA.
[150] s 26(1) of ROICA.
[151] An 'authorised person' is defined in s 1 of the ROICA as any '(a) law-enforcement officer who may in terms of s 26(1)(a)(i) execute a direction, or (b) law-enforcement officer or other person who may, in terms of s 26(1)(a)(ii), assist with the execution of a direction.'
[152] s 26(2) of ROICA.

be executed at any place in South Africa and in respect of any communication in the course of its occurrence or transmission to which the direction applies.[153] ROICA also regulates how postal articles taken into possession in the execution of a direction are to be dealt with.[154] In terms of ROICA, non-compliance with an interception direction is a criminal offence. This is not the case under the IM Act.

5.6 Fair procedures

Similar to the IM Act,[155] an application for a direction must be considered and an interception direction is likely to be issued without any notice to the person or customer to whom the application applies. Such person or customer is also not given a prior hearing in respect of such application.[156] The lack of a prior hearing is an invariable consequence of interception and monitoring in instances where it remains the only feasible and appropriate means to investigate crimes. Circumstances may well arise where an affected person is afforded a hearing subsequent to the issuance of a direction. This may occur where it would not defeat the objectives of the direction and when the affected person seeks to challenge the procedural validity of the direction granted. A hearing might also deal with the return of postal articles or recordings or transcripts or the use to be made of them. The exclusion of a right to be heard in all circumstances may constitute an infringement of the right to fair administrative action[157] or the right of access to Court or another tribunal, as the case may be,[158] as well as an infringement of the rights to privacy and freedom of expression.

In terms of section 16(10)(a) of ROICA, a TSP to whom an interception direction relating to an indirect communication is addressed may in writing apply to a designated judge for an amendment or a cancellation of an interception direction on the basis that his or her assistance with respect to the interception thereof cannot be performed in a timely or reasonable fashion. The judge must then inform the applicant of the request and consider and give a decision in respect of such request.[159] ROICA does not contemplate the applicant being given a hearing prior to the judge making such a decision.

6. OBLIGATIONS ON THE INDUSTRY

6.1 Generally

A TSP is defined in ROICA as:

- a person who provides a telecommunication service under and in accordance with a telecommunication service licence issued to such person under chapter V of the Telecommunications Act, and includes any person who provides:
- a local access telecommunication service, public payphone service, Vans or PTN as defined in the Telecommunications Act, or

[153] s 26(3) of ROICA.
[154] s 26(4) of ROICA.
[155] s 3(a) and (b) of the IM Act.
[156] s 16(7) of ROICA.
[157] s 33 of the final Constitution read with the provisions of the Promotion of Administrative Justice Act, 3 of 2000.
[158] s 34 of the final Constitution.
[159] s 16(10) of ROICA.

- any other telecommunication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Telecommunications Act, and
- Internet service providers (ISPs).[160]

In terms of the IM Act, the supplier of a postal or telecommunications service is obliged to follow directions and hand over the intercepted information to the person authorised to execute the direction. The industry also has to make available the necessary facilities and devices to enable the interception and monitoring of the conversations or communications to which the direction applies.[161] However, the industry is reimbursed for any costs incurred as a result of any action taken in terms of the IM Act either on an agreed basis or, if there is no agreement, a reasonable remuneration has to be determined by the Minister of Communications with the concurrence of the Minister of State Expenditure, or his successor-in-law.[162]

ROICA imposes certain obligations on TSPs to facilitate interception and to monitor communications, including the obligation to 'store communication-related information' and to ensure that they have the capability to intercept and monitor communications.[163] The obligations placed on the industry by ROICA are more onerous and do not contemplate reimbursement of costs as is contemplated in the IM Act.[164]

In practical terms, these obligations involve a number of TSP licensees being forced to install data capturing devices at each place where customer lines terminate in order to comply with the provisions of ROICA. This is an onerous burden to place, in particular, on smaller ISPs such as universities and Internet cafés and smaller companies — all of which would have to comply with the obligations imposed on TSPs.

Under ROICA, the Minister of Communications, in consultation with the Minister of Justice and Constitutional Development and other relevant Ministers, and after consultation with Icasa and the TSP or category of TSPs concerned, must, on the date of the issuing of a telecommunication service licence, under the Telecommunications Act, issue a directive to the TSPs concerned determining -

- the manner in which telecommunications services, that are capable of being intercepted, are to be provided, and the manner in which communication-related information is to be stored;
- the security, technical and functional requirements of the facilities and devices to be acquired by the TSP to enable the interception of indirect communications in terms of ROICA, and the storing of communication-related information in terms of section 30(1)(b) of ROICA;
- the type of communication-related information that must be stored in terms of section 30(1)(b) of ROICA and the period for which such information

[160] s 1 of ROICA defines an ISP as any person who provides access to, or any other service related to the Internet to another person whether or not such access or service is provided under and in accordance with a telecommunication service licence issued in terms of the Telecommunications Act.
[161] s 5(1) of the IM Act.
[162] s 5(2) and (3) of the IM Act.
[163] s 30(1) of ROICA.
[164] Chapters 5 and 7 of ROICA.

must be stored, which period may, subject to section 30(8) of ROICA, not be less than three years and not more than five years from the date of the transmission of the indirect communication to which that communication-related information relates.[165]

In addition, the storage period for such information — that may not be less than three months and not more than six months from the date on which a directive referred to in section 30(2)(a) of ROICA is issued — must be determined and recorded in the directive concerned.[166] It is evident from section 30(7) of ROICA that the aforementioned provisions would apply equally to existing licence holders. In this regard the Minister of Communications must, within two months after the date of the commencement of ROICA, and in consultation with the Minister of Justice and Constitutional Development and other relevant Ministers, and after consultation with Icasa and a TSP or category of TSPs to whom a telecommunications service licence has been issued under the Telecommunications Act, prior to the commencement date issue a directive:

- determining the manner in which the TSP would provide a telecommunication service that has the capability to be intercepted and is able to store communication-related information;
- indicating the security, technical and functional requirements of the facilities and devices to be acquired by the TSP, to enable the interception of indirect communications in terms of ROICA and the storing of communication-related information;
- indicating the type of communication-related information that must be stored and the period for which such information must be stored; and
- determining a period (which may not be less than three months and not more than six months from the date on which the directive is issued) for compliance with such a directive, and the period so determined must be mentioned in the directive concerned.[167]

6.2 Costs

The implementation of ROICA has far more onerous cost implications for the telecommunication industry than that of the IM Act. The set up costs for purposes of intercepting and monitoring communications and retaining information relating to communication as contemplated in ROICA have not been calculated, but they are likely to be exorbitant for the telecommunications industry as a whole. This is particularly so as TSPs have to carry the investment, technical, maintenance and operating costs of complying with ROICA.[168] Notwithstanding any other law, agreement or licence, a TSP must, unless granted an exemption,[169] at own cost

[165] s 30(2)(a) of ROICA.
[166] s 30(2) of ROICA.
[167] s 30(7) of ROICA.
[168] s 30(5) of ROICA.
[169] In terms of s 46(1)(a) of ROICA the Minister of Justice and Constitutional Development may, upon application and in consultation with the relevant Ministers, exempt ISPs from complying with s 30(4) in respect of the facilities and devices as referred to in s 30(2)(a)(ii) for such period and on such conditions as the Minister determines. Such a condition may include that an ISP to whom an exemption has been granted must pay an annual contribution to the Internet Service Providers Assistance Fund established in terms of s 38(1) of ROICA.

acquire, whether by purchasing or leasing, the facilities and devices which it requires in order to provide the interception capability and storage capacity which it is directed to have in place in terms of ROICA and/or a telecommunications licence.[170] The forms of assistance and applicable tariffs of compensation are still to be determined. Compensation payable to a PSP, TSP or DKH for providing the prescribed forms of assistance in the execution of a direction will only be in respect of direct costs incurred in respect of personnel and administration required for providing any forms of assistance.[171] The compensation due is likely to be negligible in comparison to the total costs to be incurred.

In the course of executing an interception direction TSPs will be required to route any call information and/or signals of conversations or communications to a designated interception centre.[172] It is not clear whether this means that TSPs would have to pay for a circuit to the central facility, and whether the TSP would be responsible for decoding packet information into a recognisable format as well, or both. It is, however, contemplated that the State will pay for connections between the telecommunications systems and interception centres.[173]

The cost obligations contained in ROICA were vigorously opposed during the SALC public process and in ensuing public debates leading up to the promulgation of ROICA. The SALC took note of the opposing views of ROICA. The cellular service providers (Mobile Telephone Networks (MTN) and Vodacom) and Telkom were of the view that they pay their taxes and that the revenue derived from these taxes should be appropriately directed to the implementation of ROICA. This, they contended, was so, particularly as law-enforcement, for which the interception and monitoring is a primary focus, is quintessentially a function of the State. It emerged from the SALC public consultative process that the SALC approach was premised on the view that TSPs are in possession of a very productive and lucrative resource and that it is therefore appropriate in the circumstances that they should bear particular obligations in respect of the implementation of ROICA. This appears to be the rationale underlying the SALC's view that it is entirely appropriate that TSPs should bear the costs of interception and monitoring as provided for in ROICA.[174]

It is clear from the foregoing that it is anticipated that an overwhelming amount of the costs of implementing ROICA and creating the regime for interception and monitoring will be borne by the industry. It is evident from the definition of a TSP that it includes companies that provide Internet access to employees, universities that provide Internet access to students, and Internet cafés. Accordingly, any and every supplier of telecommunications services is obliged to ensure that their supplied services have the appropriate mechanisms in place to allow for the interception and monitoring of communications.

The SALC report concluded that the obligations placed on TSPs to some extent accord with the obligations placed on TSPs in France, Belgium, Germany, the Netherlands, Australia and the United States in that the foreign TSPs also bear the responsibility of providing telecommunication systems capable of being monitored and able to store communication-related information and to do so for

[170] s 30(4) read with s 30(2)(a) of ROICA.
[171] s 31(3) of ROICA.
[172] s 28(1)(b)(i) of ROICA.
[173] Established in terms of ss 32 and 33 of ROICA. X Kritsos '*New Legislation Regulating the Interception of Communications in South Africa*' in vol 3, issue 1 (January 2003) *World Data Protection Report* 12.
[174] SALC Report (note 5 above) paras 12.2.9.16-12.2.9.19.

at least three years in most instances. Clearly the approach adopted is not novel, but is in line with the international trend of placing the cost burden for creating the capability to intercept and monitor on a TSP.[175] Although the SALC does not offer a justification for recommending that such costs be borne by the industry, it stands to reason that if it is the industry that imposes technological advancements in telecommunications, such advancements would have to be consistent with national legislation and as such be capable of interception and monitoring and be able to store information. In doing so, the State would not have to bear the responsibility and cost of creating the means to ensure that every newly developed telecommunication system can be intercepted.

The reality of these provisions is that the costs incurred will simply be passed from the industry to the consumer and will result in increased costs of telecommunications. Estimates reported for companies to implement the new monitoring and interception requirements contained in ROICA have been as high as R500 000.[176] Failure on the part of TSPs to comply with the provisions of ROICA could result in excessive fines and/or a licence being revoked.[177]

International experience has shown that the transfer of the liability of costs to the private sector is likely to have severe consequences, in particular, for smaller services providers. In the Netherlands, for example, the Telecommunications Act, 1998 imposes a similar burden on TSPs as ROICA does, and the costs for creating the interception capability are also not compensated for by the government. Certain costs were borne by the State, for example costs relating to security investigations, the costs of the installation of monitoring rooms and the rental of the communications lines to the monitoring centres, and the administrative and personnel costs relating to specific monitoring or requests for call-related information.[178] However, in imposing such costs on the industry, the government did not assess the probable costs and it was particularly difficult for ISPs to implement, as there was little experience in creating such capabilities in their networks. This led to an increase in the price of Internet access in the Netherlands and a mass closure of small ISPs. After much lobbying, the deadline for lawful interception implementation was delayed for ISPs.[179] In Australia, carriers are also obliged to develop and implement, at their own expense, an interception capability. The costs and burden upon the operators have proven more difficult and expensive than anticipated. As a result, the carriers were given both a waiver from the requirement for several years and were subsidised in respect of the costs of creating systems capable of being intercepted.[180]

ROICA may very well have the same effect in South Africa. However, the burdens and obligations placed on the telecommunications industry can be assessed fully only once the Minister of Communications has issued the directives contemplated by ROICA. On 30 October 2003, a notice was published in the Government Gazette inviting all TSPs to participate in the process of drafting

[175] SALC Report (note 5 above) para 11.4.
[176] Telkom, in its submissions to the Justice and Constitutional Development Portfolio Committee on the draft ROICA Bill, indicated that the costs of attempted compliance were estimated at R500 000 and that the final cost could be much higher, depending on ministerial directives.
[177] s 51 of ROICA.
[178] SALC Report (note 5 above) paras 4.7 and 4.8.
[179] Privacy International's submissions to the Justice and Constitutional Development Portfolio Committee on the Interception Bill dated 13 August 2001, 7-8.
[180] Privacy International's submissions (note 181 above).

directives anticipated by section 30 of ROICA.[181] Draft directives were attached and TSPs were invited to comment on or before 30 November 2003. It is contemplated that the draft directives will be the subject of public debate. As at July 2004, this process was still ongoing.

Clearly, in light of the foregoing the costs of installing the requisite equipment to implement interception and monitoring as contained in ROICA are high. This is likely to have a negative effect on the telecommunications industry and its efforts to increase access to communication in South Africa.

6.3 Data retention

ROICA provides for the retention of data by the TSP for a period as specified in a directive (which will be between three and five years from the date of transmission of an indirect communication).[182] There is concern that the retention of data that serves no business purpose imposes serious and ongoing costs on TSPs, in addition to the capital expenditure required to obtain the equipment to facilitate the interception and storage of communications. The period required for data retention by ROICA (three to five years) is considerably longer than the periods required for data retention in a number of other jurisdictions (eg the United Kingdom (six to twelve months) and the Netherlands (three months)). Also, a number of other jurisdictions, including Australia, Canada and the United States, favour targeted data preservation (the storage of a subset of data pursuant to a specific official request for such data), as opposed to the wholesale data retention required by ROICA. This is less costly and less damaging to the public confidence in communications networks whilst at the same time it adequately provides for law-enforcement goals to be met.[183]

The Austrian Federal Constitutional Court held that the Austrian law that compels telecommunication companies and ISPs to implement data retention measures at their own expense is unconstitutional.[184] As far as can be ascertained, this appears to be the only decision of this notice internationally.

Problems encountered by small ISPs attempting to comply with interception capability or storage requirements may be averted by an ISP applying for an exemption in terms of section 46(1)(a)(i) of ROICA. However, such exemptions are not available to small TSPs which are not ISPs. A condition to the granting of such an exemption is that the ISP would be expected to pay an annual contribution to the Internet Service Providers Assistance Fund established in terms of section 38 of ROICA. It is specifically contemplated that such exemptions will be granted to ISPs carrying on small businesses, in which case even though the ISP will still be subject to all the other provisions of ROICA, the law-enforcement agency that makes an application for the issuing of a direction to such ISP must make available the necessary facilities and devices to execute that direction.[185]

[181] GN 3159/2003 GG 25653 dated 30 October 2003; GN 2611/2003 GG 25597 dated 16 October 2003.
[182] s 30(2)(a)(iii) of ROICA.
[183] Kritsos *New Legislation Regulating the Interception of Communications in South Africa* (note 166 above) 12.
[184] Available on Quicklinks issue 268 (April 2003); available at http://www.qlinks.net/quicklinks/ecoutes.htm.
[185] s 46(2)(a) read with s 46(7) of ROICA.

6.4 Cellular phones and SIM-cards

ROICA also contains burdensome provisions relating to cellular phones and subscriber identity module (SIM) cards. It compels every cellular TSP and person who sells cellular phones and SIM-cards to obtain and retain information on persons to whom it contracts to provide a telecommunications service, cellular phone or SIM-card. The information required to be obtained includes the full names, identity number and addresses of the customer or the person representing a customer that is a juristic person, and the business name, address and registration number of a customer that is a juristic person. In addition, the provider of the cellular service, cellular phone or SIM-card must obtain and retain a certified copy of the identity document of the customer or person representing a customer that is a juristic person, as well as a certified copy of the business letterhead (or similar document) of a customer that is a juristic person.[186] Many current business practices relating to the sale of pre-paid cellular services would be inconsistent with the provisions of ROICA.

Cellular service providers must also keep records of the information described above as well as the telephone number or any other number allocated to the person concerned, and any other information that the cellular service provider may require to identify that person. Persons who sell cellular phones or SIM-cards must also retain the number of the cellular phone. TSPs who receive a request in writing to provide the information requested in terms of ROICA must comply immediately with such a request - failure to do so is a criminal offence.[187]

Transitional provisions contained in ROICA provide that any person who, at the time ROICA comes into force, is the owner of a cellular phone or SIM-card must provide the information described above to the person who provided the cellular phone or SIM-card to him or her. The timeframes for the provision of this information are still to be prescribed by the Minister of Justice and Constitutional Development. Given the growth of the cellular industry and the number of persons who have pre-paid cellular telecommunication services, especially in rural areas, it is not likely that compliance with this provision will be possible. This obligation would have to be widely publicised in order to have any effect and to ensure comprehensive compliance. However, non-compliance with this provision does not constitute an offence in terms of ROICA. MTN, in its written submissions to the Parliamentary Justice and Constitutional Development Portfolio Committee, indicated that there were approximately five million pre-paid users who do not have identities attached to them. Moreover, as a number of the distribution outlets in South Africa are informal suppliers (street vendors, spaza shops), it is not feasible for identities to be attached to buyers of cellular phones and cellular phone-related products. Presumably, the purpose sought to be achieved by this provision is to curb the theft of cellular phones and to be able to trace those cellular phones that are used in crime-related activities.

[186] s 39(1) of ROICA.
[187] s 39(3) and (4) read with s 51(3) of ROICA.

Conclusion

ROICA extensively regulates interception and monitoring of direct and indirect communication and provides the conditions that must be met in order for such interception and monitoring to occur. Although ROICA prohibits the blanket interception and monitoring of communications, it sets out in great detail the circumstances that would have to be met in order for such interception and monitoring to occur and the mechanisms that have to be invoked.

ROICA is not yet in force. Given that this process had commenced in 1995, the delay in bringing this legislation into force has been not only inordinate, but may well be an indication of the difficulties surrounding the enforcement and compliance therewith. The directives contemplated in ROICA are in the process of being drafted and have been for some time. The set up costs for enforcement on the part of government to implement ROICA may very well be a further reason for delaying its implementation. Furthermore, at the hearings before the Portfolio Committee on Justice and Constitutional Development, it was submitted on behalf of the National Director of Public Prosecutions that they had resorted to using the IM Act on only a handful of occasions. As this is the law-enforcement agency most likely to invoke ROICA for purposes of combating crime, it may be that South Africa has developed sophisticated legislation, on par with international standards, that may be excessive given its ostensible objective: crime control, and by having done is placing unnecessarily onerous burdens on a fledging and yet rapidly growing industry.

Finally, although there is currently no data protection legislation in South Africa, such legislation is in the pipeline. Once legislation is promulgated in respect thereof, ROICA and the exceptions to the prohibition on interception will have to be read together with that legislation. It may well be appropriate for both legislation to come into force simultaneously.