

ISPA ADVISORY 10: The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002

By: Tracy Cohen

February 2003

<p>Disclaimer: This advisory is produced for informational purposes only to familiarize ISPA members with the main provisions of the above law. It is not a complete analysis of the relevant law or its implications and in no way should be interpreted as legal advice offered by ISPA. ISPA, its members, and its advisors cannot be held liable for any reliance by readers on this document, its accuracy or interpretation of the law.</p>
--

Relevance

In 1998, the South African Law Commission (SALC) began a project to review the existing 1992 law on the monitoring and interception of communication and make a number of recommendations for its reform. Various draft bills have been published since then, and following public consultation, culminated in *The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002*. (“The RIC Act”). Although signed by the President on 30 December 2002, the Act will only come into operation at a later date still to be determined. The main provisions of the Act are summarized below with attention drawn to the implications for ISPs.

Introduction and Legislative History

Surveillance and monitoring of communications (‘wiretapping’ or ‘bugging’) is conducted in nearly every country in the world by governments and private groups, for a range of reasons. The most renowned target of the wiretap is the standard fixed-line telephone system but surveillance now extends to newer technologies and applications. Since 11 September 2001, wiretap laws around the world have been amended to expand their scope and there has also been a proliferation of new laws.

The South African surveillance law was first significantly amended in 1992 to increase individual privacy protections: the *Interception and Monitoring Prohibition Act* (No. 127 of 1992) focused primarily on telephonic and postal communications. A protracted law commission project (SALC, Project 105, November 1998) reviewing old apartheid security laws decided to prioritize the investigation into interception and monitoring of

communications for crime investigation and intelligence gathering purposes, and to extend its ambit from just telephones and postal articles to include all communications networks.

(For details of the SALC Project and the 1992 Act, please refer to ISPA Advisory 2: The surveillance of electronic communications: Monitoring and interception laws in South Africa, 24 February 2000, available at <http://www.ispa.org.za>).

COE Convention on Cybercrime

The law reform process was further impacted upon by the Council of Europe Convention on Cybercrime (<http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>). SA is one of four non-member signatories to that convention and as such, is required to develop certain measures in accordance with that agreement. The RIC Act conforms to this requirement.

The COE Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The COE Convention has an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence. SA is expected to develop hate speech legislation in 2003.

A Note on Privacy

It should be noted that the right to privacy of communications is a fundamental right, protected in section 14 of the Constitution.¹ This includes the right to be free from intrusions and interference by the state and individuals. The Constitution explicitly states that the right includes not having “*the privacy of communications infringed.*” It is universally accepted however, that that no right is absolute in operation and as long as reasonable grounds exist to limit that right, and that the law is of general application to all citizens, this limitation may be constitutionally acceptable. The RIC Act is of general application, which provides for the limitation of the above right in certain circumstances.

However, ISPs and other service suppliers are still required to honour the privacy rights of consumers and subscribers, except where deviation is required by law. While there has been a move to expand the scope of surveillance legislation, there is a corresponding move within other recent legislation also to protect consumer privacy in order to enable e-commerce. While these initiatives arguably lack meaningful consumer protection, they are expected to be strengthened by a general Data Privacy Bill to be tabled in Parliament by 2004.

The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002. (“RIC Act”)

Summary of General Provisions

1. ISPs are explicitly included in the Act, under the general definition of a Telecommunications Service Provider (TSP).
2. Like its predecessor, the RIC Act continues to generally prohibit monitoring and surveillance of communications except in certain circumstances, or where authorised to under an ‘interception direction’. (Sections 2-3)
3. There is also a general prohibition against a TSP or any employee providing *real-time*² or *archived communication-related information* to anyone other than the customer of the TSP to whom the information relates, unless required to do so by law, or unless a customer explicitly agrees in writing. (Sections 12-15).
4. Sections 3-11 set out the exemptions to the general prohibition on unlawful surveillance. This means that surveillance can take place without a direction where:
 - (a) the person (including a law enforcement officer) intercepting is a party to the communication;
 - (b) a party to the communication has given prior written consent to such interception;
 - (c) the interception takes place in connection with carrying on of business; (call centre monitoring; record keeping; transactional purposes, etc.) This is discussed further below.

¹ *Constitution of the Republic of South Africa Act No. 108 of 1996*

² Defined in the Act as “any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system.

- (d) or takes place to prevent serious bodily harm or for determining location of a person in the case of an emergency;³
 - (e) the interception takes place in a prison; or while monitoring a signal for installing or maintaining telecommunication equipment; facilities or devices or in the course managing the radio frequency spectrum.
5. No TSP can offer a telecommunication service that is not capable of being monitored. That is, all telecommunication services must be surveillance enabled or capable. (Section 30(1)(a)).
 6. All the costs of ensuring surveillance capacity must be borne by the TSP.
 7. TSP's including ISPs are required to store communication-related (traffic) data.
 8. The agencies or persons that may make applications for the surveillance of communications include, law enforcement agents, the SA Police Service (SAPS), the National Defence Force (SANDF), the Secret Service and the National Intelligence Agency (NIA) or a member of the Independent Complaints Directorate.

Communications and Directions

The Act distinguishes between '*direct communications*' (audible, oral communications between two or more people) and '*indirect communications*' (the transfer of information including messages in the form of speech; music; data; text; visual images; signals and radio frequency spectrum).

Except where interception is authorised without a Direction, the Act provides for a variety of "interception directions" that can be obtained by law enforcement, who must apply to a designated (retired) judge to obtain an interception direction, before requiring assistance from ISPs. These are:

- (a) The broad **interception direction**;
- (b) A **real-time communication related direction** (for traffic related data on an ongoing basis for no longer than three-months at a time)
- (c) an **archived communications direction** (any communication related information in the possession of and being stored by a TSP)

³ There are a number of procedural requirements after the interception has been made justifying the action. These are not detailed in this advisory, save to say that where a TSP has been requested to intercept a communication without a direction, the facts, findings of the interception and/or duplicate signals, where the

- (d) or **supplementary direction** or a combination thereof.
- (e) **entry warrants** (to rig premises and intercept postal articles)
- (f) **Decryption directions.**

Applications for Decryption Directions which may be granted for a maximum of three months at a time, require detailed information including the identity of the applicant; customer, if known, in respect of whom the decryption of encrypted information is required; and decryption key holder to whom the decryption direction must be addressed; it should also describe the encrypted information which is required to be decrypted; specify the decryption key, if known, which must be disclosed; or decryption assistance which must be provided, and the form and manner in which it must be provided.

A judge can only issue such authorization if the decryption key holder specified in the application is in possession of the encrypted information and the decryption key thereto. The Act does however go on to state that if a decryption key holder to whom a decryption direction is addressed, is not in possession of the encrypted information; or incapable, without the use of a decryption key that is not in his or her possession, to comply fully with that decryption direction, the decryption key holder concerned must endeavour to comply, to the best of his or her ability, with that decryption direction.

There are a range of very complex provisions regarding the obligations decryption key holders; the assistance they are to provide and the routing of decrypted data to monitoring centres – the essence of which is that such holders *are obligated* to disclose the decryption key, if they have it, or provide decryption assistance, if the facility for encryption was provided by the TSP concerned. Failure to do so is liable to fine and/or imprisonment on conviction.

Similarly, on receipt of any interception direction, a TSP must route the duplicate signals of indirect communications to a designated interception centre and make the necessary facilities available to do so.

communication was indirect, must be set out in an affidavit, documenting the steps that TSP has taken in complying with a request from law enforcement.

Grounds for surveillance orders

These are specified in Chapter 3 of the Act, and include criminal investigations of serious offences; gathering of information regarding actual or potential threats to public health and safety and national security or actual threats to other compelling national economic interests; gathering of information concerning property which could be which could be “an instrumentality of a serious offence” or is or could be the proceeds of unlawful activities and to assist foreign law enforcement agencies with interception regarding organised crime or terrorism under a mutual assistance agreement.

While "serious offence"⁴ is defined, there is still no definition or qualification of the national interest, or when it may be compelling. The threshold of "reasonable grounds to believe" remains the standard for a Judge to grant an order, but further grounds that need to be satisfied have been built in an attempt to enhance this weak standard.⁵

The requirement for interception capability and compensation

As stated above, all TSPs must ensure that, at their own costs, their networks are surveillance enabled. The Act provides that the Minister may elect to exempt ISPs from this requirement. However, as discussed below, this exemption may see a condition imposed requiring that ISP to contribute to a fund to centrally purchase the facilities and devices required for surveillance.

The Minister must, after consultation with other relevant Ministers, ICASA and the TSPs concerned, issue a directive determining the manner in which surveillance capability is to be effected and communication-related information, stored. This includes, security, technical and functional requirements of the facilities and devices to be acquired by the TSP. This, yet to be issued Ministerial Directive, must specify to TSPs the:

- ♣ capacity needed for interception purposes;
- ♣ technical requirements of the systems to be used;

⁴ Some examples include, high treason, terrorism, sabotage, sedition, threat of risk of life, offences related to drugs/trafficking, corruption; smuggling ammunition, firearms, explosives and unlawful possession, possession of endangered, scarce or protected game, plants, illicit dealing in precious metals or stones; offences relating to the prevention of Organised Crime Act, any offence for which 7 or 10 years imprisonment is the penalty.

⁵ Namely, the likelihood of success in obtaining the information; that other means of investigation have failed or are too dangerous to apply; and that the wiretap is done in respect of targeted facilities commonly used by the person concerned.

- ♣ connectivity with interception centres;
- ♣ manner of routing duplicate signals of indirect communications; real-time or archived communication-related information to designated interception centres.

It should be noted that decryption key holders, the postal and TSPs may be remunerated for providing assistance in respect of direct costs (personnel and admin) incurred in assisting with the execution of a direction.

Costs, Office for interception Centres and ISP Assistance Fund

As mentioned above, all the costs of ensuring surveillance capabilities, including investment, technical, maintenance and operating costs, must be borne by the TSP concerned.

The state will carry its own cost to establish interception centres for routed information and will be responsible for the costs of connecting to telecoms providers. The centres are provided for in Chapter 6, through the establishment of an “office for interception centres” (“OIC”) – a statutory body tasked with managing and coordinating the activities of these national surveillance centres. Chapter 6 also details its staffing, powers and functions and the requirement for clear and proper record keeping by such centres.

The OIC will also be responsible for administering an Internet Service Provider Assistance Fund which will derive its revenue primarily from contributions made by ISPs who have been exempted by the Minister from the requirement to purchase or lease the facilities needed to ensure surveillance capabilities. The precise amount of contribution is yet to be determined by the Minister.

This money will then be used to acquire – whether by purchase or lease – facilities and devices required for surveillance, which will then be made available to ‘exempted’ ISPs to execute interception directions where applicable.

Therefore, ISPs are not exempted from the requirement to monitor communications in certain circumstances; but rather, from the requirement to acquire such facilities and devices to do so.

Duties of TSPs and Customers

The Act also requires all TSPs to gather detailed personal data on individuals and companies (including photocopies of ID documents) before signing service contracts (or selling SIM cards and mobile phones for pre-paid mobile services) and obliges them to retain that data and make it available to law enforcement agencies when requested to. There is no limit specified for the length of time TSPs are required to retain personal data, and the Act obliges ISPs to keep proper records of all personal information gathered.

This means that before an ISP can conclude a service contract with a subscriber/customer, they must obtain and store the following information:

(1) If the customer is a natural person: his or her full names, identity number, residential and business or postal address, and a certified photocopy of his or her identification document on which his or her photo, full names and identity number, appear. The ISP must then retain the photocopy provided and verify the photo, full names and identity number of that person with reference to his or her identification.

(2) If the customer is a juristic person, i.e. a company: his or her full names, identity number, residential and postal address; the business name and address and, if registered as such in terms of any law, the registration number of that juristic person; a certified photocopy of his or her identification document on which his or her photo, full names and identity number, appear; and a certified photocopy of the business letterhead of, or other similar document relating to that juristic person. The ISP must then retain the photocopies obtained and verify the photo, full names and identity number, of that person with reference to his or her identification document; and name and registration number of that juristic person with reference to its business letterhead or other similar document; and may obtain from such person any other information which the TSP deems necessary for purposes of this Act.

Offences and Penalties

Offences and penalties are provided for in Chapter 9 of the Act, which has slightly augmented the list of offences under its predecessor to include:

- ♣ Unlawful interception of communication or procuring any other person to intercept or attempt to intercept unlawfully;
- ♣ Unlawful provision of real-time or archived communication-related information to any person other than the customer of TSP by a TSP or employee;
- ♣ Non-compliance with an interception direction; providing false, incorrect or misleading information with regard to an interception direction, and obstructing the execution of directions or warrants;
- ♣ the sale of, manufacture, possession, or advertising of any equipment that can be used for surveillance;
- ♣ being in possession of a stolen cell phone or SIM-card. (Possession presumes knowledge in the absence of evidence to the contrary);
- ♣ unlawfully disclosing information obtained in exercising powers or duties under this Act;
- ♣ Failure to report a SIM card stolen, lost or damaged;
- ♣ Tampering with any telecommunications hardware and software for the purposes of circumventing the Act.

Different fines and/or imprisonment are provided for different offences, but range between R2 000 000 or imprisonment for a period not exceeding ten-years. Importantly for TSPs, the Act provides for the forfeiture and destruction of listed equipment if owned illegally and for the revocation of a telecoms service licence in the case of a second or subsequent conviction of an offence.

The importance of obtaining the proper authority to monitor or intercept with strict adherence to procedure has been stressed in our courts and the validity of the directive can be **automatically vitiated** if not lawfully issued. This would not only constitute a criminal offence in terms of the Act, but also constitute an infringement of the right to privacy, which includes the right not to be subject to “the violation of private communications”, as set out above.⁶

⁶ See *S v Naidoo* 1998 (1) BCLR 46 (D) at 72 E-F and *Protea Technology Ltd and Another v Wainer and Others* 1997 (9) BCLR 1225 (W).

Implications for ISPs

Until the Act is fully operational and all the Ministerial Directions to be issued have been gazetted, it is difficult to do a full audit of all the implications the Act presents for ISPs, outside of the obvious financial implications. What follows is a cursory outline of some of the issues.

Application

The Act unequivocally applies to all ISPs, whether licensed or not. As such, ISPs need to ensure that they have the necessary processes in place to comply with the requirements of the Act, if called upon to do so. However, no ISP should engage in surveillance activity without the presentation of an interception direction, unless it is for the purposes of interceptions that are listed above which do not require a direction. Where justification after the fact is required, ISPs will need to document all facts findings etc of the surveillance and should ensure that systems are in place to record this thoroughly, as failure to do so is an offence.

Surveillance with implied consent

Chapter 2 provides for situations in which surveillance may occur without an interception direction or without consent. One such circumstance is in the course of the carrying on of any business. The Act allows a company to intercept any indirect communication (message, etc) in the course of its transmission over a telecommunication system, by means of which a transaction is entered into in the course of that business; which relates to that business; or which otherwise takes place in the course of the carrying on of that business.

This section is poorly drafted and the interplay between subsections presents possibilities for confusion. Nonetheless, it is suggested for the purposes of this Act, as well as for good consumer practice, that all ISP clients and prospective clients are informed in written dealings with the ISP that indirect communications may be intercepted with the express or implied consent of the person who uses that telecommunication system.

We also suggest that you make reasonable efforts to inform clients that calls made to call-centres might be monitored for customer care purposes.

Similarly, this section does not preclude the monitoring of employee e-mails, with or without explicit consent. In such a circumstance, the law requires companies to “make all reasonable efforts” to inform employees in advance of this possibility. Again, in terms of good practice and to respect the privacy rights of employees, it is advisable that employee’s attention is drawn to the possibility/likelihood of the surveillance of workplace communications either in employment contracts, or through company policy on the matter, or both.

These notifications should be dealt with in your company’s privacy policy, and reasonable efforts should be made by ISPs to draw customer’s attention to the existence and contents of such policies.

Network accessibility and costs

The costs for ensuring surveillance capability, including the acquisition of facilities and devices to do so, are to be borne by TSPs/ISPs. While the terms and precise manner of application for exemption are not yet clear, if your operation is small or medium sized one, you may wish to consider applying for exemption from this requirement. Be aware however that the Minister may require an annual contribution from you, on exemption, for the ISP Assistance Fund. The annual contribution amount has not yet been determined.

License Revocation

It is worth noting that the Act stipulates that TSPs who fail to comply with the provisions of this Act, after conviction and a fine, may have their telecommunication service licence revoked by the Minister for repeated failure to comply.

Decryption Assistance

The requirement to assist with decryption directions has been controversial and it has been suggested that it is not implementable. You are urged to seek legal assistance and advice if required to assist in a manner that you are not technologically capable of doing. The requirements may also have implications for various security products advertised and offered by ISPs.

Privacy

Notwithstanding a number of constitutional privacy concerns inherent in surveillance, monitoring and interception of communications, it is likely that given the current crime rates in the country and the criminal uses to which certain telecommunications equipment is being put to, a law of this nature will likely withstand constitutional scrutiny. The issue however remains to dilute the privacy invasions as much as possible and to protect the privacy rights of the users, customers and subscribers on the networks. Please take care to ensure that all ISP employees receive sufficient training and briefing on the privacy rights of subscribers. It is also an offence to disclose any information obtained in the performance of duties under this Act or in executing a direction or rendering assistance in executing a direction.

Whilst ISPs have to indemnify themselves against this type of liability for failure to comply, it is imperative that these provisions be scrutinized for what is and is not considered constitutionally acceptable. No ISP should make information of this nature available without having all the proper documentation and applications presented by law enforcement officials. Complete adherence to procedure is absolutely imperative in order to avoid a claim of privacy infringement. For those who still have not, it may be useful for ISPs to develop ‘privacy policies’ (also required by the Electronic Commerce and Transactions Act) that make it clear to customers when their informational privacy rights will be violated in the case of criminal investigation or matters of a like nature, providing the necessary documentation and procedures are complied with.