SCRIPT-ed

Volume 3, Issue 4, June 2006

Watching the watcher: recent developments in privacy regulation and cyber-surveillance in South Africa

Caroline B Ncube[*]

Abstract

This article outlines developments in privacy regulation in South Africa. The first part comments on the recently issued draft bill on the protection of personal information. It pays particular attention to the provisions on transborder information flows. The second part comments on the Regulation of Interception of Communications and Provision of Communication Related Information Act (70 of 2002) which ushers in a very controversial cyber-surveillance regime.

DOI: 10.2966/scrip.030406.344

[*] Lecturer, University of Cape Town, South Africa.

1. Introduction

South Africa "is by far the best-connected to the Internet in Africa. It faces the same problems as the United States or Europe, of reconciling respect for online privacy and freedom of expression with the need to fight cyber crime and terrorism."[1] This article examines South Africa's efforts to respect privacy and to fight cyber crime. South African privacy laws have been under construction for several years. I have discussed the early efforts in another article. [2] This article will outline the latest developments in this law reform process. I will also briefly discuss South Africa's new regime of cyber-surveillance which seems to create the potential for serious inroads into the right to privacy.

2. Draft privacy legislation

The South African Law Review Commission (formerly the South African Law Commission) has been investigating privacy and information protection for several years. It published an issue paper in 2003 (SALRC Issue Paper 24 2003). After considering the feedback it received, the SALRC issued a discussion paper and draft bill in October 2005. At that time a call was made to the public for any comments to be made by 28 February 2006. There was a very good response to the discussion paper which is currently being considered by the SALRC.[3]

The draft bill proposes a general information protection statute to be known as the Protection of Personal Information Act (PPIA) which will be applicable to both the public and private sector, unlike the Promotion of Access to Information Act (PAIA) (2 of 2000) which is applicable only to the public sector. The draft bill covers both automatic and manual processing unlike the Electronic Communications and Transactions Act (ECTA) (25 of 2002) which as provided for in s50 (1) only applies to personal information that has been obtained through electronic transactions. The PAIA and ECTA will have to be amended once the draft bill becomes law. The draft bill protects identifiable natural and juristic persons. It has ninety-seven sections divided into ten chapters. The objects of the Act and an interpretation section are found in chapter 1. The application of the Act is provided for in chapter 2. Information protection principles are provided for in chapter 3 and the exemptions in chapter 4. Supervision is provided for chapters 5, 6 and 7. Enforcement, offences and sanctions are provided for in chapters 8 and 9. Miscellaneous and transitional provisions are provided for in chapter 10.

South Africa has opted for the comprehensive laws model like the European Union and the draft bill, once it becomes law, will be supplemented by codes of conduct for

---

[1] Reporters san frontieres borders "South Africa" *(http://www.rsf.org/article.php3?id_article=10728),* CB Ncube "Africa confronts cyber-crime" (2004) 2 *Speculum Juris* 312 and C Ncube "The legal regulation of identity theft in South Africa" (2005) 1 *Speculum Juris* 119.

[2] CB Ncube, "A comparative analysis of Zimbabwean and South African data protection systems', (2004) 2 *The Journal of Information, Law and Technology (JILT) (http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/ncube/)*

[3] ITWeb, "Draft privacy law receives comment" 28 April 2006 *(www.itweb.co.za)*

the various sectors. Industries will be encouraged to develop their own codes of conduct which comply with the principles set out in the legislation.

The Act and the codes of conduct will be monitored and supervised by a statutory regulatory body to be called the Information Protection Commission (the Commission) provided for in Chapter 5 of the bill. The Commission will consist of a full-time Information Commissioner and two other persons appointed by the state president. Section 35 (1) (b) provides that to be eligible for appointment to the commission, a person "must be appropriately qualified, fit and proper … for appointment on account of the tenure of a judicial office or on account of experience as an advocate or as an attorney or as a professor of law at any university, or on account of any other qualification relating to the objects of the Commission."

Section 39 provides that the powers and duties of the Commission will include public education on privacy rights, monitoring compliance with the PPIA, consultation with the public and government on privacy, handling privacy related complaints, undertaking research and reporting and drafting and issuing codes of conduct. To achieve meaningful enforcement, the SALRC, in Chapter 6 of the Discussion Paper, recommends that**:**

1. there be provision for external supervision through the Commission;
2. information subjects be provided with legal remedies which they can enforce in a court of law;
3. the Commission should have investigative powers and authority to engage in legal proceedings where the information protection legislation has been violated.
4. Individuals should be able to enforce their rights independently of the Commission, such as the inherent right to approach a court or appeal to a court against a decision taken by a responsible party or the Commission.
5. Individuals who have suffered damage by reason of a contravention of the information protection legislation should also be entitled to compensation by either the responsible parties or the data processors.
6. the legislation should also provide for a number of criminal offences under the Act.

These recommendations are implemented by Chapter 8 of the draft bill. It is yet to be seen whether the government has enough resources to fully monitor and enforce the PPIA.

2.1 Transborder information flows

The South African government has not openly declared its intention to apply for "adequacy" to the EU. It has however acknowledged that data flows from the EU to South Africa are of critical importance because "Europe is the largest source of investment for South Africa and accounts for almost half of South Africa's total foreign trade…"[4] Any decrease in the flow of personal data from Europe is likely to impact significantly on South Africa's economy. Since the overthrow of apartheid and

[4] South Africa Yearbook 2003/4 *(http://www.info.gov.za/yearbook/2004/economy.htm)*

the institution of the Constitution which provides for the right to privacy, there have been concerted efforts to protect privacy. Section 94 of the bill, which provides for transborder information flows, is thus motivated both by constitutional or human rights concerns and trade considerations.

Articles 25-6 of the 1995 European Union Data Protection Directive (EU Directive)[5] provide that the personal data of European citizens can only be processed in countries that can guarantee adequate levels of protection. The European Commission (the Commission) is empowered to determine whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into. The Commission is also empowered to decide that certain standard contractual clauses offer sufficient safeguards as required by Article 26 (2) in that they provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

Data may lawfully flow from the EU to South Africa in three circumstances:

First, once South Africa is declared as a country offering adequate levels of protection. Such a declaration means that personal data can flow from EU member states and three European Economic Areas member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.[6] To date, Argentina, Guernsey, Hungary, Isle of Man, Switzerland and Canada have been declared as providing adequate levels of protection.[7]

Second, in the absence of such a declaration, if the Commission finds that the incorporation of certain standard clauses into a contract will offer sufficient safeguards.

Third, in the absence of such a declaration or a finding as to the adequacy of contractual clauses, data may be transferred in the following specific circumstances provided for by Article 26 (1):

1. The data subject has given his consent unambiguously to the proposed transfer; or
2. The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
3. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
4. The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
5. The transfer is necessary in order to protect the vital interests of the data subject; or

---

[5] *(http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm)*

[6] EUROPA EU –Internal market- Data Protection - Adequacy *(http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm)*

[7] Europa, "Commission decisions on the adequacy of the protection of personal data in third countries" *(http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm)*

6. The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

For ease of reference I will reproduce s94 of the Bill in full-

A responsible party in South Africa may transfer personal information about a data subject to someone (other than the responsible party or the data subject) who is in a foreign country only if

(a) the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Protection Principles set out in Chapter 3 of this Act; or

(b) the data subject consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is reasonably impracticable to obtain the consent of the data subject to that transfer;

(iii) if it were reasonably practicable to obtain such consent, the individual would be likely to give it.

A responsible party is defined in s1 as "the the natural person, juristic person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal information." Section 94(a) refers to the information protection principles set out in Chapter 3. These are processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, individual participation and accountability. These principles are equivalent to the principles contained in Article 6 of the EU Directive. Section 94 (b) is identical to Article (Art) 26 (1) (a). S94(c) and (d) are couched very similarly to Arts 26 (1) (b) and (c) respectively. Section 94(e) is similar to Art 26 (1) (e) but seems to go further as it requires in addition to the data transfer being for the benefit of the data subject that it be reasonably impracticable to obtain their consent but that it be likely that were it sought, such consent would be given. Section 94 therefore meets the minimum standards set by Arts 25-6.

It is unfortunate that the draft bill does not specifically address data transfer *via* the internet and provide separately for its unique traits. It is important to regulate data

transfer *via* advanced technologies. [8] The EU has begun tackling such issues as shown by the 2002 Directive on Privacy and Electronic Communications 2002/58/EC[9] which addresses the use of surreptitious means like spyware. The European Court of Justice has held in *Lindqvist*[10] that loading data onto a webpage that can be accessed by persons in a third country does not amount to data transfer to that country. The court noted that there was a lack of criteria in the EU Directive that would apply to the internet. South Africa would have done well to provide for such criteria.

3. Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA)[11]

South Africa promulgated RICA in 2002 and it commenced on 30 September 2005 except for ss 40 and 62(6).[12] These sections which are the crux of the cyber-surveillance regime were to commence on 30 June 2006.[13] However due to representations by interested parties the commencement has been postponed indefinitely.[14] RICA raises serious privacy concerns because it permits interception of certain communications. Communication is defined as direct communication and indirect communication, which are in turn shrouded in lengthy and complex language. The following constitute communication:

(a) conversations between people without the use of any technology;

(b) letters, postcards, books, parcels and packets;

(c) landline telephone conversations;

(d) cellular telephone conversations;

(e) SMS messages;

(f) answering machine or services messages;

(g) email;

(h) instant messaging;

(i) VOIP communications (audio and video);

(j) FTP downloads and uploads (audio, video, text);

(k) streaming media such as podcasts;

---

[8] R Wong "The shape of things to come: Swedish developments on the protection of privacy" (2005) 2:1 *SCRIPT-ed107* at 118*;* E de Kock "Data protection in South Africa" (2005) Dec *Derebus (www.derebus.org.za)*

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L201/37 31.7.2002 (*http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf)*

[10] C-101/01 [2004] 1 C.M.L.R. 20.

[11] Act 70 of 2002.

[12] Government Gazette (GG) 28075.

[13] Proclamation (Proc) R67 GG 28282 of 29 Nov 2005.

[14] Proc R25 GG 28973 of 27 June 2006.

(l) two way radio communications;

(m) all communications in prisons;

(n) website requests; chat room postings; blog postings and search engine requests and results.

Interception is permitted where:

1. it is done by one of the parties to the communication is a party to the communication (s4)
2. one of the parties to the communication gives prior written consent (s5)
3. one of the parties to the communication has been informed that it may be recorded (s6)
4. an interception directive has been granted by a court to the police, defence force, national intelligence agency, national prosecuting authority, post office, postnet or courier services (s3)
5. a law enforcement agent needs to intercept communication to prevent serious bodily harm (s7)
6. any person needs to locate another person in an emergency (s8)
7. it is done in terms of another act such as the Correctional Services Act (s9)
8. it is necessary to enable the installation, monitoring, maintenance and testing of communication services or devices (ss 10-11)

RICA has been succinctly summarised as a set of prohibitions, duties and exceptions.[15] It prohibits intentional interceptions or attempts to intercept communications (s2), the intentional provision of real-time or archived communication related information by telecommunications service providers and their employees (s12), the provision of a telecommunications service that is not interceptable by telecommunications service providers, the disclosure of information obtained while acting under RICA (s42) and dealing in equipment that could be used for interception (s44-5). The exceptions to these prohibitions have been listed above (1-9).

RICA requires cell-phone owners to report lost, stolen or destroyed SIM (Subscriber Identity Module) cards to the police (s41). It also places duties on telecommunications service providers (TSPs) who are defined in section 1 as any—

(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—

(i) a local access telecommunication service, public pay-telephone service, value-added network service or private telecommunication network as defined in the Telecommunications Act; or

(ii) any other telecommunication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Telecommunications Act; and

---

[15] R Buys " Complete guide to the regulation of Communications Act 70 of 2002" *(www.buys.co.za)*

(b) Internet service provider.

Internet service providers (ISPs) are in turn defined 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 to the first-mentioned person under Chapter V of the Telecommunications Act.*

Section 30 requires all TSPs to automatically continuously store communications related information in respect of every single communication and to provide or disclose these details as required by an interception directive. A Directive has been published to provide for the practical details on the information to be stored.[16] It provides that communication-related information, whether real-time or archived, must be stored for a cumulative period of three (3) years from the date on which the indirect communication to which the communication-related information relates, is recorded.

Section 40 imposes the most hotly contested duty on persons who sell SIM-cards. This duty is a blanket duty that will apply to any person selling a SIM-card. It will largely affect cellular telephone network operators. It requires persons who sell SIM-cards to obtain, verify and store the full names, identity number, residential and business or postal address of natural persons who are their clients or representing juristic persons who are their clients. They must also obtain, verify and store details pertaining to juristic persons such as their registration numbers and places of business. Such information in relation to existing customers has to be collected within 12 months from the date of commencement of the section. Failure to do so would result in punitive fines. The date of commencement was previously set as the 30 June 2006 but TSPs successfully argued that they would be unable to meet this deadline as they had millions of clients and would have to register at least 8000 persons per hour for the entire twelve months to meet the deadline. They also argued that a large majority of their clients simply did not have identity numbers and proper residential addresses as they lived in informal settlements. Such people's telecommunications services would have to be suspended and this would adversely affect them.[17] The date of commencement was then indefinitely postponed.

In addition to the initial capturing of information, persons who sell SIM-cards are required to ensure that proper records are kept of the information they have obtained and if notified of changes must update this information. Section 40 is currently being debated, as the Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill B9 of 2006 which seeks to amend it is before Parliament. The main aim of the Bill is to amend ss 40 and 62(6) to more clearly state specifically what information has to be recorded and stored.

---

[16] General Notice No. 1325 *GG* 28271 of 28 Nov 2005.

[17] P Vecchiatto "Operators seek RICA deadline extension" *ITWeb* 30 May 2006 *(www.itweb.co.za),* A Knott-Craig (CEO Vodacom) "RICA will wreak havoc on SA's poor," *Business Day*, 1 June 2006 *(www.businessday.co.za)*

Section 40 is vulnerable to a constitutional challenge because it treats persons selling SIM-cards differently from other TSPs who are governed by section 39. This arguably violates the other TSPs' right to equal treatment under the law.

Sections 16-23 of RICA provide for interception directions, which are defined as an authority given by a judge to intercept, route or decrypt a communication or disclose communications-related information. The South African regime is quite strong compared to jurisdictions such as the UK and US, as judicial approval is always required, which is not the case in the UK and US. There are five types of directions, namely: an Interception direction (s16); a Real-time CRI direction (s17); an Archived CRI direction (s19); a Decryption direction (s21); and a Combined direction (s18). An application for a direction may be accompanied by an application for an entry warrant is under s22. Section 1 defines an entry warrant as

> *a warrant which authorises entry upon any premises for purposes of (a) intercepting a postal article or communication on the premises; or (b) installing and maintaining an interception device on, and removing an interception device from, the premises, and includes an oral entry warrant issued under section 23 (7).*

Only certain persons may apply for directions and entry warrants, these are:

(a) an officer referred to in section 33 of the South African Police Service Act, if the officer concerned obtained in writing the approval in advance of another officer in the Police Service with at least the rank of assistant-commissioner and who has been authorised in writing by the National Commissioner to grant such approval;

(b) an officer as defined in section 1 of the Defence Act, if the officer concerned obtained in writing the approval in advance of another officer in the Defence Force with at least the rank of major-general and who has been authorised in writing by the Chief of the Defence Force to grant such approval;

(c) a member as defined in section 1 of the Intelligence Services Act, if the member concerned obtained in writing the approval in advance of another member of the Agency or the Service, as the case may be, holding a post of at least general manager;

(d) the head of the Directorate or an Investigating Director authorised thereto in writing by the head of the Directorate;

(e) a member of a component referred to in paragraph (e) of the definition of "law enforcement agency", authorised thereto in writing by the National Director; or

(f) a member of the Independent Complaints Directorate, if the member concerned obtained in writing the approval in advance of the Executive Director.

All applications for a direction must be written and be detailed enough to allow the judge to whom the application is made to properly consider its merits (s16 (6)). The circumstances in which a direction should be issued are fully enunciated in the Act in respect of applications for each kind of direction. For example s16 (5) (a) provides that an interception direction may only be issued if the judge to whom application is made, is satisfied that there are reasonable grounds to believe that:

(i) a serious offence has been or is being or will probably be committed;

(ii) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(iii) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(iv) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in—

(*aa*) accordance with an international mutual assistance agreement; or

(*bb*) the interests of the Republic's international relations or obligations; or

(v) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary;

A direction issued by a judge must be in writing, contain certain information and be limited to periods of three months (s16(6)).

Privacy concerns about RICA centre around the fear that the state may abuse the exceptions at the expense of the privacy of citizens who will have to rely on the state's integrity.[18] This is a reasonable fear considering the state's illegal surveillance in the past.[19] The cyber-surveillance regime will be orchestrated by the Office for Interception Centres (OIC) which is part of the National Intelligence Agency (NIA). All interception requests have to be sent to the OIC which will send these to a designated judge for the issuance of an interception directive. Once the direction is issued, the OIC will inform the relevant telecommunications service providers who will then send the required information to an interception centre linked to the OIC. Privacy will be secured by the prior requirement of judicial approval (ss16-23), progress reports submitted to the judge (s24), review of the OIC's activities by the Inspector-General of Intelligence and the duty of the OIC to report annually to parliament's joint standing committee on intelligence (s37). Citizens will also have to actively monitor the situation and defend their privacy rights. The media has a major role to play as a provider of information to the public. The new cyber-surveillance regime is yet to be tested as it is not yet in operation. There is ongoing debate among

---

[18] P Honey "Spooks go cyber" *Financial Times* 28 April 2006 (*http://free.financialmail.co.za/06/0428/cover/coverstory.htm),* P De Wet "Who watches the watcher?" *ITWeb* 15 Aug 2001 (www.itweb.co.za)

[19] "Newspaper uncovers 'unlawful' tapping by intelligence units," *The Star*, 21 Feb 1996, "Democratic party outraged by bugging of its offices," *Africa News*, 23 Nov 1999, "South Africa admits to spying on German embassy," *Reuters*, 6 Feb 6, 2000 all cited in Privacy International's 2003 Report on South Africa (*http://www.privacyinternational.org/survey/phr2003/countries/southafrica.htm*) and "The rise and fall of spy chief Billy Masetlha" *The Star* 24 March 2006.

academics and lawyers on the privacy concerns raised by RICA which will require close watching to ensure that the right to privacy is upheld.[20]

4. Conclusion

South Africa is making considerable progress towards enacting privacy legislation and is currently ushering in a new regime of cyber-surveillance. The fact that surveillance laws have been finalised before privacy legislation is an indication that the state values its powers to monitor its citizens more than the right to privacy.

---

[20] Examples of academic papers include A Meinesz "How private are your telephone calls and can they be recorded without your knowledge?" (2006) May *Derebus*; News "LSSA says ambit of new Communications Act too wide" (2003) March *Derebus;* J Van Rensburg "Intercepting communications and providing communication-related information" (2003) 11(2) *Juta's Business Law (JBL) 90.* G Lumb & E Kingdom "Are e-mails private: communications act" 2004 *Accountancy SA* 15.