



THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 4 | Number 4


Article 2

2009

A Synopsis of Proposed Data Protection Legislation in SA

Francis S. Cronjé
KPMG Services (Proprietary) Limited

Follow this and additional works at: <http://commons.erau.edu/jdfsl>

 Part of the [Computer Law Commons](#), and the [Information Security Commons](#)

Recommended Citation

Cronjé, Francis S. (2009) "A Synopsis of Proposed Data Protection Legislation in SA," *Journal of Digital Forensics, Security and Law*: Vol. 4 : No. 4 , Article 2.

DOI: <https://doi.org/10.15394/jdfsl.2009.1065>

Available at: <http://commons.erau.edu/jdfsl/vol4/iss4/2>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



A Synopsis of Proposed Data Protection Legislation in SA

Cover Page Footnote

1. Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, medical privacy, and freedom of information and expression. Available at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-65428](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65428) (17 August 2007). 2. a) The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and b) the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. 3. Nedbank (one of the big five banks in South Africa) has accordingly been forced, in the absence of such legislation locally which would have facilitated the bank processing information within South Africa, at great extra cost, to set up processing centres in Europe, in order to meet European information protection legislative requirements. This has resulted in the effective cost to market of the bank's outsourcing service being driven up and could very well be the reason for preventing the bank from obtaining further business processing outsourcing deals within Europe on the basis of not being cost competitive enough. (Comments on SALRC draft proposal) 4. Art 25(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. Also refer to Art 29 Working Party's Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data. (Annex to the Annual Report 1998 (XV D/5047/98) of the working party established by Article 29 of Directive 95/46/EC.) 5. Act No. 54 of 2002. View www.info.gov.za/gazette/acts/2002/a54-02.pdf (12 August 2007) 6. Art 50(2) ECT Act. 7. SALRC Discussion papers available at <http://www.doj.gov.za/salrc/dpapers.htm> (07 August 2007) 8. These countries include Angola, Botswana, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Kingdom of Swaziland, Tanzania, Zambia and Zimbabwe. For further information, see <http://www.sadc.int/home.php> (24 August 2007) 9. See <http://www.export.gov/safeharbor/> (24 August 2007) for a detailed discussion on the safe harbour agreement. 10. Ibid note 85. 11. The objectives of SADC as stated in Article 5 of the Treaty are to: Achieve development and economic growth, alleviate poverty, enhance the standard and quality of life of the people of Southern Africa and support the socially disadvantaged through regional integration; Evolve common political values, systems and institutions; Promote and defend peace and security; Promote self-sustaining development on the basis of collective self-reliance, and the interdependence of Member States; Achieve complementarity between national and regional strategies and programmes; Promote and maximise productive employment and utilisation of resources of the Region; Achieve sustainable utilisation of natural resources and effective protection of the environment; Strengthen and consolidate the long-standing historical, social and cultural affinities and links among the people of the Region. 12. Their article titled "Data Protection: Safeguarding Privacy in a New Age of Technology" can be viewed at: <http://www.heritage.org/Research/HomelandSecurity/lm16.cfm> (26 August 2007) 13. Lessig, Lawrence in "Code and other Laws of Cyberspace", Reidenberg, Joel R. in "Lex Informatica: The Formulation of Information Policy Rules Through Technology", Texas Law Review, University of Texas at Austin School of Law Publications, 76 (3) 1998 pp. 553-584, Rotenberg, Marc in "Fair Information Practices and the Architecture of Privacy" (What Larry Doesn't Get), Stanford Technology Law Review, Cite as: 2001 Stan. Tech. L. Rev. 1 http://stlr.stanford.edu/STLR/Articles/01_STLR_1 (22 August 2007) 14. Bennett CJ "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association" Prepared for the "Voluntary Codes Project" of the Office of Consumer Affairs

Industry, Canada and Regulatory Affairs Treasury Board, March 1997 available at <http://web.uvic.ca/polisci/bennett/> 15. See Part VI of the New Zealand Privacy Act. 16. Comments on SALRC draft proposal by Michalsons. 17. A good example of a code of conduct that incorporates all the information protection principles was the 1996 Canadian Bankers Association Privacy Model Code. See discussion at <http://web.uvic.ca/~polisci/bennett/research/cba.htm>. (06 August 2007) 18. A further example of a code of conduct that set out obligations that, overall, are the equivalent of all the obligations set out in those principles is the Netherlands Code of Conduct for the Processing of Personal Data by Financial Institutions. 19. Project 124, October 2005, Privacy and Data Protection. 20. See Part IIIA of the Australian Privacy Act 1988 as amended. 21. See for instance *Unitas v Van Wyk & Naude* case nr 231/2005. Sec 50 – meaning of “required” for exercise or protection of right – when available to compel pre-action production. The threshold of “required” was set very high due to uncertainty on whether to use the Promotion to Access of Information Act (PAIA). PAIA was not the appropriate remedy. Discovery would probably have been successful in this delictual action.

A Synopsis of Proposed Data Protection Legislation in SA

Francis S Cronjé
KPMG Services (Proprietary) Limited
Parktown, South Africa
francis@cybersmart.co.za

Privacy International¹ made the following statement regarding South Africa's financial sector in its 2005 world survey:

“South Africa has a well-developed financial system and banking infrastructure. Despite the sophistication of the financial sector, the privacy of financial information is weakly regulated by a code of conduct for banks issued by the Banking Council.”

This extract highlights some of the problems South Africa are experiencing with its current status on privacy as viewed from an International perspective. In recent years the International society has stepped up its efforts in creating a global village wherein the individual could be assured of having his/her privacy protected. Various conventions and guidelines² have previously laid the foundation for privacy but it was not until the European Union's (EU) launch of its Directive on Data Protection in 1995 that we have seen a real coerced shift in the focus of such protection. Cross border data transfers from the EU became something of the past unless third countries (those countries outside the EU) could prove the existence of adequate data protection provisions. It seemed to a big extend that international trade would be hampered and some of its biggest trading partners, such as the US, suddenly felt the impact due to its lagging protection measures. In order to curtail such inadequacies, a Safe Harbor Agreement was entered into between the EU and US whereby cross border data flow would be allowed under certain prerequisites. This Agreement however, does not cover Financial Institutions.

Concomitantly, South Africa, having the EU as its biggest trading partner also felt the grunt and some SA organizations had to take its processing to within the

¹ Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, medical privacy, and freedom of information and expression. Available at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-65428](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65428) (17 August 2007).

² a) The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and
b) the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.

borders of the EU.³ By implication it was then assumed that South Africa lacked the adequacy criteria as laid down by the EU Directive on Data Protection.⁴ The South African Law Reform Commission (hereinafter referred to as SALRC) instructed a project committee to work on a draft Bill on Protection of Personal Information (hereinafter referred to as POPIA).

Some of the reasons why, can best be explained as Prof Iain Currie reflects in his summary of the proposed POPIA:

“South Africa has general privacy protection in the Bill of Rights [s 14]. The right is protected by a private law action to interdict current or anticipated privacy infringements or to recover damages for infringements that have already occurred. Though information privacy is encompassed in the constitutional protection of privacy, there is no specific legislative regulatory regime for this aspect of privacy. The Promotion of Access to Information Act⁵ protects personal information from disclosure in response to a request made in terms of the Act, but has no application outside the context of such a request. It is this absence of legislation that the SALRC draft Bill intends to remedy.”

Although there is current legislation in place, none are specifically formulated to address data protection. For instance, The Electronic and Communication Transaction (ECT) Act of 2002⁶ also addresses the collection of personal information in its chapter 8 but subscription to such principles is voluntary. The Regulation of Interception of Communications (RIC) Act prohibits the interception of communications while one Act that has recently been enacted, The National Credit Act, makes specific provision for the regulation of personal information, although such regulation is restricted to the financial sector.

Should the POPIA be enacted, consequential amendments may be necessary in

³ Nedbank (one of the big five banks in South Africa) has accordingly been forced, in the absence of such legislation locally which would have facilitated the bank processing information within South Africa, at great extra cost, to set up processing centres in Europe, in order to meet European information protection legislative requirements. This has resulted in the effective cost to market of the bank's outsourcing service being driven up and could very well be the reason for preventing the bank from obtaining further business processing outsourcing deals within Europe on the basis of not being cost competitive enough. (Comments on SALRC draft proposal)

⁴ Art 25(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. Also refer to Art 29 Working Party's Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data. (Annex to the Annual Report 1998 (XV D/5047/98) of the working party established by Article 29 of Directive 95/46/EC.)

⁵ Act No. 54 of 2002. View www.info.gov.za/gazette/acts/2002/a54-02.pdf (12 August 2007)

⁶ Art 50(2) ECT Act.

respect of the following acts: Banking Act 38 of 1942, Broadcasting Act 4 of 1999, Copyright Act 98 of 1978, Electoral Act 73 of 1998, Financial Advisory and Intermediary Services Act (FAIS) 37 of 2002, Financial Intelligence Centre Act (FICA) 38 of 2001, Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002, Short-term Insurance Act 53 of 1998, Long-term Insurance Act 52 of 1998 and Telecommunications Act 103 of 1996.⁷ Subsequently, the Electronic Communications Act of 2005 might also be subject to amendments.

A survey of access to information laws and practices in 14 countries was done by the Open Society Initiative and published in its Justice in Action Series, titled, Transparency and Silence. They had the following to say about South Africa:

“South Africa, the only monitored country in Africa with a freedom of information law in place, demonstrated greater compliance with the right to information than the other four African countries. However, only 19 percent of the requests submitted in South Africa yielded a compliant outcome and only 13 percent yielded information. This is by far the lowest score of the seven monitored countries with freedom of information laws. Justice Initiative monitoring exercises in both 2003 and 2004 highlighted serious problems with the implementation of South Africa’s Promotion to Access of Information Act (Act No. 2 of 2 February 2000), and these problems resulted in high levels of mute refusals in response to requests. Although the law is strong on paper, it has proved complex to implement in practise, and there have not been sufficient efforts to make its implementation a priority. Better implementation might yet make it a model for the region.”

Clearly this is the last sort of comment that South Africa needs on the implementation of its proposed POPIA. Currently, as the draft stands, it is however not unforeseeable that such comment might well be read into its implementation, since some of its provisions might also prove too complex to implement in practise, especially seen from the banking industry’s perspective.

Some of the issues are for instance the cross border data transfer problems related to payment orders. Other problems are those concerning fraud, Basel II and the legally non-binding codes of conduct that is currently laying the guidelines for banking practices with regards to its consumers.

The question would be whether there is a golden one rule solution. I sincerely doubt this. It is my contention that an array of various factors must play a role in seeing the proposed POPIA through to its successful implementation. Such factors would include safe harbour agreements, technological solutions, and

⁷ SALRC Discussion papers available at <http://www.doi.gov.za/salrc/dpapers.htm> (07 August 2007)

sector specific regulations in the form of privacy code of conducts.

For South African banks for instance to operate successfully in Africa, specifically in the SADC region (SADC stands for ‘Southern African Development and Economic Community’ and refers to 14 African nations⁸ in Southern Africa, who have signed a mutual trade and co-operation agreement) it is my suggestion that South Africa sign a safe harbour agreement⁹ with the other members of SADEC, similar to that as between the USA and the EU, but with the exception that it also makes provision for financial institutions,. None of these countries¹⁰ currently make provision for data protection in its laws. Without such an agreement, banks for instance might be strained along in subjecting themselves to unnecessarily high costs in it’s strive to comply with the proposed POPIA. In signing such an agreement however, time limits must be set on these countries to implement similar legislation, encouraging them to step up its own democratic values in ensuring sufficient privacy measures and achieving the objectives and vision as set by SADC.¹¹ This would then set a standard for the rest of Africa and hopefully spirit them on to reach similar goals.

It is also suggested that similar safe harbour agreements must be concluded between South Africa and some of its other trading partners. Some of these major trading partners include the United Kingdom, the United States, Germany, Italy, Belgium, and Japan, although it would only be foreseen that such an agreement be reached between South Africa and the United States, since the other five do make provision for adequate measures.

Technological advances also have a role to play. Paul Rosenzweig and Alane Kochems¹² explain that technology is both a problem and a solution for the issues posed by enhanced information collection systems. It can facilitate access to and the accumulation of large amounts of data; however, if that access is not properly

⁸ These countries include Angola, Botswana, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Kingdom of Swaziland, Tanzania, Zambia and Zimbabwe. For further information, see <http://www.sadc.int/home.php> (24 August 2007)

⁹ See <http://www.export.gov/safeharbor/> (24 August 2007) for a detailed discussion on the safe harbour agreement.

¹⁰ Ibid note 85.

¹¹ The objectives of SADC as stated in Article 5 of the Treaty are to: Achieve development and economic growth, alleviate poverty, enhance the standard and quality of life of the people of Southern Africa and support the socially disadvantaged through regional integration; Evolve common political values, systems and institutions; Promote and defend peace and security; Promote self-sustaining development on the basis of collective self-reliance, and the interdependence of Member States; Achieve complementarity between national and regional strategies and programmes; Promote and maximise productive employment and utilisation of resources of the Region; Achieve sustainable utilisation of natural resources and effective protection of the environment; Strengthen and consolidate the long-standing historical, social and cultural affinities and links among the people of the Region.

¹² Their article titled “Data Protection: Safeguarding Privacy in a New Age of Technology” can be viewed at: <http://www.heritage.org/Research/HomelandSecurity/lm16.cfm> (26 August 2007)

managed, the information can be misused. When designed with proper procedures and protections and combined with oversight, technology can provide a reasonable balance between security and privacy. They continue by stating that in properly determining how best to enhance both liberty and security, it is useful to have some basic principles for assessing data protection technologies. They contend that such a list might include the following:

- The data protection technology should allow for clear audit tracks to prevent data alteration or identify when data have been changed.
- The technology should have a means to provide graduated levels of access to the data.
- The technology should have protocols for enforcing the confidentiality and security of the data.

There are multiple approaches to securing data. One means is following one of the many published information security standards; another is to protect the most sensitive data through encryption. They conclude by stating that controlling access to data and making sure that entities only have the appropriate level of access is critical if privacy interests are to be protected. Various software companies have adapted its data collection programs to make provision for legislation. A number of academic writers¹³ are also of the point of view that the solution would be in the code and that *lex informatica* could be a useful policy device. But this is a discussion in its own right. The fact that technology would and in fact must play a role is unmistakable and its contributory role in the banking industry could provide solutions to successful implementation of the proposed POPIA.

The last and probably most crucial factor is the facilitation of sector based codes of conduct. Codes offer flexibility and can be adapted to the specific economic, technological and regulatory contexts of different sectors. With or without legislation, codes will continue to be significant instruments by which organisational responsibilities are defined, employee obligations are communicated and citizen rights are established.¹⁴

In New Zealand, the approach is that codes of practice under its Privacy Act have the force of law. A breach of a ratified code of practice is as serious as a breach of

¹³ Lessig, Lawrence in "Code and other Laws of Cyberspace", Reidenberg, Joel R. in "Lex Informatica: The Formulation of Information Policy Rules Through Technology", Texas Law Review, University of Texas at Austin School of Law Publications, 76 (3) 1998 pp. 553-584, Rotenberg, Marc in "Fair Information Practices and the Architecture of Privacy" (What Larry Doesn't Get), Stanford Technology Law Review, Cite as: 2001 Stan. Tech. L. Rev. 1 http://stlr.stanford.edu/STLR/Articles/01_STLR_1 (22 August 2007)

¹⁴ Bennett CJ "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association" Prepared for the "Voluntary Codes Project" of the Office of Consumer Affairs Industry, Canada and Regulatory Affairs Treasury Board, March 1997 available at <http://web.uvic.ca/polisci/bennett/>

the information privacy principles expressed in the law, which would then trigger the complaints and enforcement procedures in the legislation.¹⁵ Although the Dutch system is similar in most respects to that in New Zealand, the codes are not formally binding on the courts. The proposed POPIA makes provision for codes in its section 62 to be legally binding.

In Australia an organisation or industry registering a Privacy Code under the Australian Privacy Act, must prove and be legally accountable for the Code providing at least the same level of protection that the ten National Privacy Principles of the Australian Privacy Act require – preferably more.¹⁶

If the proposed POPIA is to follow a co-regulatory scheme as is proposed by the SALRC, then the question has to be asked whether the current industry codes of practice will suffice.

In terms of Section 54(2) (a) of the proposed POPIA, a code of conduct must incorporate all the information protection principles¹⁷ or set out obligations that, overall, are the equivalent of all the obligations set out in those principles¹⁸.

It is generally recognised that five kinds of privacy code can be identified according to their scope of application: organisational code, the sector code, the functional code, the professional code and the technological code.¹⁹

The approach envisaged by the proposed POPIA seems to be on par with the co-regulatory scheme of Australia where any business or profession may develop a Code of Practice. The code must then be submitted to the Privacy Commissioner for approval. If the Code is deemed to be acceptable then the Commissioner may issue it.²⁰

The solution does not necessarily arrive with the issuing of the codes themselves, but rather through a pre-emptive strike and pro-active based effort on behalf of the specific sectors to submit such codes to the Commissioner. If industries sit back and wait for the Commissioner to issue these codes, problems might arise as to the interim position on the implementation and interpretation of the proposed POPIA. Having regard to the specific related problems that might arise from an industry's perspective, courts could create precedents²¹, which in the absence of

¹⁵ See Part VI of the New Zealand Privacy Act.

¹⁶ Comments on SALRC draft proposal by Michalsons.

¹⁷ A good example of a code of conduct that incorporates all the information protection principles was the 1996 Canadian Bankers Association Privacy Model Code. See discussion at <http://web.uvic.ca/~polisci/bennett/research/cba.htm>. (06 August 2007)

¹⁸ A further example of a code of conduct that set out obligations that, overall, are the equivalent of all the obligations set out in those principles is the Netherlands Code of Conduct for the Processing of Personal Data by Financial Institutions.

¹⁹ Project 124, October 2005, Privacy and Data Protection.

²⁰ See Part IIIA of the Australian Privacy Act 1988 as amended.

²¹ See for instance *Unitas v Van Wyk & Naude* case nr 231/2005. Sec 50 – meaning of “required” for exercise or protection of right – when available to compel pre-action production. The threshold of “required” was set very high due to uncertainty on whether to use the Promotion to Access of

such co-regulatory structures, could be detrimental to the industry as a whole. With its sector based knowledge, it is therefore suggested that the various industries, make sure that they have these codes of conduct or privacy codes ready for submission when the proposed POPIA becomes enacted, thereby annihilating any room for an uncertain interim period that might be subject to scrutiny.

Information Act (PAIA). PAIA was not the appropriate remedy. Discovery would probably have been successful in this delictual action.

