SOUTH AFRICAN LAW REFORM COMMISSION

Project 124

PRIVACY AND DATA PROTECTION

REPORT

2009

TO MR E SURTY, MP, MINISTER OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT

I am honoured to submit to you in terms of section 7(1) of the South African Law Reform Commission Act 19 of 1973 (as amended) for your consideration, the Commission's report on privacy and data protection.

Y MOKGORO
CHAIRPERSON: SOUTH AFRICAN LAW REFORM COMMISSION
2009

INTRODUCTION

The South African Law Reform Commission was established by the South African Law Commission Act, 1973 (Act 19 of 1973).

The members of the Commission are -

The Honourable Madam Justice Y Mokgoro (Chairperson)
The Honourable Mr Justice W L Seriti (Vice-Chairperson)
The Honourable Mr Justice D M Davis
Adv C Albertyn
Ms T Madonsela (full-time member)
Mr T Ngcukaitobi
Adv D Ntsebeza SC
Prof PJ Schwikkard
Adv M Sello

The Commission's offices are on the 12th floor, Sanlam Centre c/o Pretorius and Schoeman Streets, Pretoria. Correspondence should be addressed to:

The Secretary
South African Law Reform Commission
Private Bag X668
PRETORIA 0001
Telephone: (012)392-9566
Fax: (012)320-0936
E-mail: analouw@justice.gov.za
Website: www.doj.gov.za/salrc/index.htm

The members of the Project Committee for this investigation are:

The Honourable Mr Justice CT Howie
Prof J Neethling
Prof I Currie
Ms C da Silva
Ms C Duval
Prof B Grant
Ms A Grobler
Mr M Heyink
Ms S Jagwanth
Ms A Tilley

The Chairperson is Mr Justice CT Howie, the Project Leader is Prof J Neethling and the researcher is Ms Ananda Louw.

SUMMARY OF RECOMMENDATIONS FOR LEGISLATIVE REFORM

Privacy is a valuable aspect of personality. Data or information protection forms an element of safeguarding a person's right to privacy. It provides for the legal protection of a person in instances where his or her personal information is being collected, stored, used or communicated by another person or institution.

In South Africa the right to privacy is protected in terms of both the common law and in sec 14 of the Constitution. The recognition and protection of the right to privacy as a fundamental human right in the Constitution provides an indication of its importance.

The constitutional right to privacy is, like its common law counterpart, not an absolute right but may be limited in terms of law of general application and has to be balanced with other rights entrenched in the Constitution.

In protecting a person's personal information consideration should, therefore, also be given to competing interests such as the administering of national social programmes, maintaining law and order, and protecting the rights, freedoms and interests of others, including the commercial interests of industry sectors such as banking, insurance, direct marketing, health care, pharmaceuticals and travel services. The task of balancing these opposing interests is a delicate one.

Concern about information protection has increased worldwide since the 1960's as a result of the expansion in the use of electronic commerce and the technological environment. The growth of centralised government and the rise of massive credit and insurance industries that manage vast computerised databases have turned the modest records of an insular society into a bazaar of information available to nearly anyone at a price.

Worldwide, the surveillance potential of powerful computer systems prompt demands for specific rules governing the collection and handling of personal information. The question is no longer whether information can be obtained, but rather whether it should be obtained and, where it has been obtained, how it should be used. A fundamental assumption underlying the answer to these questions is that if the collection of personal information is allowed by law, the fairness, integrity and effectiveness of such collection and use should also be protected.

There are now well over fifty countries that have enacted information protection statutes at national or federal level and the number of such countries is steadily growing. The investigation into the possible development of information privacy legislation for South Africa is therefore in line with international trends.

Early on, it was, however, recognised that information privacy could not simply be regarded as a domestic policy problem. The increasing ease with which personal information could be transmitted outside the borders of the country of origin produced an interesting history of

international harmonisation efforts, and a concomitant effort to regulate transborder information flows.

Two crucial international instruments evolved:

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.

These two agreements have had a profound effect on the enactment of national laws around the world, even outside the OECD member countries. They incorporate technologically neutral principles relating to the collection, retention and use of personal information.

Although the expression of information protection in various declarations and laws varies, all require that personal information be dealt with according to specific principles known as the "Principles of Information Protection" which form the basis of both legislative regulation and self-regulating control.

Some account should also be taken of the UN Guidelines, the APEC initiative, as well as the Commonwealth Law Ministers' proposed Model Laws. In all these instances countries are encouraged to enact legislation that will accord personal information an appropriate measure of protection, and also to make sure that such information is collected only for appropriate purposes and by appropriate means.

In 1995, the European Union furthermore enacted the Data Protection Directive in order to harmonise member states' laws in providing consistent levels of protection for citizens and ensuring the free flow of personal data within the European Union. It imposed its own standard of protection on any country within which personal data of European citizens might be processed. Articles 25 and 26 of the Directive stipulate that personal data should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection".

Privacy is therefore an important trade issue, as information privacy concerns can create a barrier to international trade. Considering the international trends and expectations, information privacy or data legislation will ensure South Africa's future participation in the information market, if it is regarded as providing "adequate" information protection by international standards.

A pertinent example in this regard is the importance for South Africa to ensure a successful 2010 FIFA Soccer World Cup. In order to enforce proper customs and immigration control measures through passenger surveillance and monitoring, the personal information of large numbers of international travelers, who will be making use of international airlines, will have to be facilitated by

SARS, SAPS and the Department of Home Affairs. However, the international airlines will be unable to provide the advance passenger information needed until South Africa can guarantee the adequate protection of the information.

It should be noted that the promulgation of information protection legislation in South Africa will necessarily result in amendments to other South African legislation, most notably the Promotion of Access to Information Act 2 of 2000, the Electronic Communications and Transactions Act 25 of 2002 and the National Credit Act 34 of 2005. All these Acts contain interim provisions regarding information protection in South Africa.

The recommendations of the Commission, as set out in the Bill accompanying this report as **Annexure C**, can be summarised as follows:[1]

a) Privacy and information protection will be regulated by a general information protection statute, with or without sector specific statutes, which will be supplemented by codes of conduct for the various sectors and will be applicable to both the public and private sector. Automatic and manual processing will be covered and identifiable natural and juristic persons will be protected **[Chapter 2, clauses 3-6].**

b) General principles of information protection have been developed and incorporated in the legislation. The proposed Bill gives effect to eight core information protection principles, namely accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. Provision is made for exceptions to the information protection principles **[Chapter 3, Part A, clauses 7-24]**. Exemptions are furthermore possible for specific sectors in applicable circumstances **[Chapter 4, clauses 33-34]**. Special provision has furthermore been made for the protection of special (sensitive) personal information **[Chapter 3, Part B, clauses 25-32]**.

c) A statutory regulatory agency should be established. Provision has been made for an independent Information Protection Regulator.**[Chapter 5, Part A, clauses 35-47]**. The Regulator will, inter alia, be responsible for the implementation of both the proposed Protection of Personal Information Act (see Annexure C) and the Promotion of Access to Information Act, 2000. Data subjects will be under an obligation to notify the Regulator of any processing of personal information before they undertake such processing **[Chapter 6, Part A, clauses 50-54]** and provision has also been made for prior investigations to be conducted where the information being collected warrants a stricter regime **[Chapter 6, Part B, clauses 55-56]**. Options have been provided in the text of the report **[Chapter 7, para 7.2.189(h)]**

---

[1] References in brackets are to the applicable clauses, parts and chapters in the **Protection of Personal Information Bill** set out in **Annexure C** to this Report.

for different alternatives regarding the structure of the Regulator. The basic structure set out in the Bill will be adjusted according to the options chosen.

d) Enforcement of the Bill will be through the Regulator using as a first step a system of notices where conciliation or mediation has not been successful. Failure to comply with the notices will be a criminal offence. The Regulator may furthermore assist a data subject in claiming compensation from a responsible party for any damage suffered. Obstruction of the Regulator's work is regarded in a very serious light and constitutes a criminal offence **[Chapter 10, clauses 70-94 and Chapter 11, clauses 95-100]**.

e) A flexible approach should be followed in which industries will develop their own codes of conduct (in accordance with the principles set out in the legislation) which will be overseen by the regulatory agency. Codes of conduct for individual sectors may be drawn up for specific sectors on the initiative of the specific sector or of the Regulator itself. This will include the possibility of making provision for an adjudicator to be responsible for the supervision of information protection activities in the sector. The Regulator will, however, retain oversight authority. Although the codes will accurately reflect the information protection principles as set out in the Act, it should furthermore assist in the practical application of the rules in a specific sector **[Chapter 7, clauses 57-65]**.

f) Specific provision has been made for the protection of data subjects' rights in so far as unsolicited electronic communications (spam) and automated decision making are concerned **[Chapter 8, clauses 66-68]**.

g) It is the Law Commission's objective to ensure that the legislation provides an adequate level of information protection in terms of the EU Directive. In this regard a provision has been included that prohibits the transfer of personal information to countries that do not, themselves, ensure an adequate level of information protection **[Chapter 9, clause 69]**.

The recommendations and draft legislation are the result of a very thorough consultation process. Should these recommendations be adopted by Parliament, the protection of information privacy in South Africa willl be in line with international requirements and developments.

TABLE OF CONTENTS

LIST OF ANNEXURES

LIST OF SOURCES

Ad hoc Joint Committee of South African Parliament ***Report of the Ad Hoc Joint Committee on the Open Democracy Bill*** [B67-98], 24 January 2000.

Alvarez R "On guard: Electronic Health Records and Safeguarding Patient Privacy" Presentation made at the Health Information Privacy Day in Toronto on 24 September 2007.

Australian Law Reform Commission ***Keeping Secrets: The Protection of Classified and Security Sensitive Information*** ALRC 98 June 2004 accessed at http://www.austlii.edu.au/other/alrc/publications/reports/98/index.html on 18/3/2005.

Australian Law Reform Commission ***Review of Australian Privacy*** Discussion Paper 72 September 2007.

Bainbridge D ***Data Protection*** CLT Professional Publishing Welwyn Garden City 2000.

Bennett C J "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.za/polisci/bennett.

Bennett CJ "Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada" August 1997 available at http://web.uvic.ca/~polisci/bennett/research/iso.htm accessed on 29/10/2002.

Bennett CJ "What Government Should Know About Privacy: A Foundation Paper" Presentation prepared for the Information Technology Executive Leadership Council's Privacy Conference, June,19 2001 (Revised August 2001) available at http://web.uvic.za/polisci/bennett, accessed on 29/10/2002.

Bennett CJ "The Data Protection Authority: Regulator, Ombudsman, or Campaigner?" Presentation delivered at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002.

Bennett CJ and Raab CD ***The Governance of Privacy - Policy Instruments in Global Perspective*** Ashgate Publishing Aldershot/Hamshire 2003 (reprinted in 2004).

Berkman Center for Internet & Society (Berkman Online Lectures and Discussions) Harvard Law School ***Privacy in Cyberspace 2002*** available at http://eon.law.harvard.edu/privacy/module6.html accessed on 16/7/2002.

Burchell JM ***Personality Rights and Freedom of Expression: The Modern Actio Injuriarum*** Juta Cape Town 1998.

Burchell JM "Media Freedom of Expression Scores as Strict Liability Receives the Red Card: National Media Ltd v Bogoshi" 1999 ***SALJ*** 1.

Bygrave LA "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling" ***Computer Law and Security Report*** 2001 Vol 17 17-24 accessed at http://folk.uio.no/lee/publications/ on 29/7/2005.

Bygrave LA ***Data Protection: Approaching Its Rationale, Logic and Limits*** Kluwer Law International The Hague 2002.

Calcutt Committee ***Report of the Committee on Privacy and Related Matters***, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO.

Cameron O ***Information and Systems Management: Balancing Security and Privacy*** Discussion Document for the Department of Justice and Constitutional Development to Establish Security Requirements and Frameworks 23 September 2003.

Canadian Medical Association (CMA) ***Health Information Privacy Code*** 16 September 1998 accessed at http://www.cma.ca/cma/common/displayPage on 15/11/2002.

Centre for Democracy and Technology (CDT)'s Guide to Online Privacy "Privacy Basics: Generic Principles of Fair Information Practices" available at http://www.cdt.org/privacy/guide/basic/generic.html accessed on 15/11/2002.

Centre for Democracy and Technology (CDT) "Why am I Getting All this Spam? Unsolicited Commercial E-mail Research" Six month Report March 2003.

Chadwick P "Who Me? Stimulating Privacy Awareness" Paper delivered at the Private Sector Privacy in a Changing World Conference, Vancouver, BC on 20-21 September 2007.

Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D & Woolman S (eds) ***Constitutional Law of South Africa*** Juta Kenwyn 1996 Revision Service 5 1999.

Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D & Woolman S (eds) ***Constitutional Law of South Africa*** 2ed Juta Kenwyn 2002.

Cockrell A "Private Law and the Bill of Rights: A Threshold Issue of "Horizontality" ***Bill of Rights Compendium*** Butterworths Constitutional Law Library.

Commission on Telecommunications and Information Technologies of the International Chamber of Commerce Working Party on Privacy and Data Protection "Model clauses for use in contracts involving transborder data flows"(1992).

Commission of the European Communities ***Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions*** issued by the United States Department of Commerce July 26, 2000 available at http://www.ita.doc.gov/td/ecom/Decisions_SECGEN-EN.htm.

Commonwealth Secretariat ***Draft Model Law on the Protection of Personal Information*** LMM(02)8 October 2002.

Commonwealth Secretariat ***Model Privacy Bill for Public Sector*** LMM(02)7 November 2002.

Council of Europe, the European Commission of the European Communities and the International Chamber of Commerce "Joint Study on Standard Clauses" (1992), available at http://www.coe.fr/dataprotection/Etudes_Rapports/ectype.htm.

Crombie G "Spam for Breakfast, Lunch and Dinner: What will the Unsolicited Electronic Messages do for Privacy?" Minter Ellison Rudd Watts Lawyers Spam and Privacy Issues 30 March 2006.

De Klerk A "The Right of a Patient to have Access to his Medical Records" 1991 ***SALJ*** 166.

Department of Communications ***Making IT Your Business*** Green Paper on E-Commerce November 2000.

Department of Trade and Industry (dti) "Introducing the National Credit Regulator" 2 June 2006 accessed at http://www.thedti.gov.za/article on 3 September 2008.

Devenish GE "The Limitation Clause Revisited - The Limitation of Rights in the 1996 Constitution" 1998 ***Obiter*** 256.

De Waal J, Currie I & Erasmus G ***The Bill of Rights Handbook*** 3ed Juta Kenwyn 2000.

Du Plessis W ***Die Reg op Inligting en die Openbare Belang*** LLD thesis PU for CHE 1986.

El Amam K "Anonymization and Health Research" Paper delivered at the Health Information Privacy Day, Toronto, September 24, 2007.

El Amam, K, Jonker, E, Sams, S, Neri, E, Neisa, A, Gao, T & Chowdry, S "Pan-Canadian De-Identification Guidelines for Personal Health Information" April 2007 Paper delivered at the 29th International Conference of Data Protection and Privacy Commissioners Montreal 26 September 2007.

Electronic Privacy Information Centre (EPIC) and Privacy International ***Privacy and Human Rights Report 2002 : An International Survey of Privacy Laws and Developments*** United States of America 2002.

Electronic Privacy Information Centre (EPIC) and Privacy International ***Privacy and Human Rights Report 2003 : An International Survey of Privacy Laws and Developments*** United States of America 2003.

Electronic Privacy Information Centre (EPIC) and Privacy International ***Privacy and Human Rights Report 2004 : An International Survey of Privacy Laws and Developments*** United States of America 2004 accessed at http://www.privacyinternational.org/survey/phr2004/ on 25/6/2005.

Electronic Privacy Information Centre (EPIC) and Privacy International ***Privacy and Human Rights Report 2006: An International Survey of Privacy Laws and Developments*** United States of America 2006.

European Commission "Public Sector Information: A Key Resource for Europe" Green Paper, 1998 available at http://www.echo.lu/legal/en/access.html.

European Commission "Data Protection: Commission Adopts Decisions Recognising Adequacy of Regimes in United States, Switzerland and Hungary" Press Release July 27, 2000 available at http://europa-eu.int/comm/interal-market/en/media/dataprot/news/safeharbour.htm/.

European Commission Decision 2001/497/EC on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries 15 June 2001.

European Commission Report on the practical operation of the European Union-United States Safe Harbor Agreement Staff Working Paper, February 2002, available at http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf>.

European Commission Decision 2002/16/EC on Model Clauses for Transfers from Responsible Parties in the EEA to Data Processors dated 27 December 2001.

European Commission Decision 2004/915/EC (amending Decision 2001/497/EC) as regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries 27 December 2004.

European Commission Final Report on the Electronic Evaluation of the Data Protection Directive 95/46/EC (prepared by RAMBOLL Management) May 2005.

European Union Art 29 Working Party ***Data Protection Law and the Media*** Recommendation 1/97 25 February 1997.

European Union Art 29 Working Party ***Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*** WP 12 24 July 1998.

European Union Art 29 Working Party ***Opinion No 3/99 on Public Sector Information and the Protection of Personal Data*** 3 May 1999.

European Union Article 29 Working Party ***Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act*** January 2001.

European Union Article 29 Working Party ***Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*** March 2001.

European Union Article 29 Working Party ***Working Document on Blacklists*** 3 October 2002.

European Union Article 29 Working Party ***Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*** June 2003.

European Union Article 29 Data Working Party ***Opinion 5/2004 on Unsolicited Communication for Marketing Purposes under Article 13 of Directive 2002/58/EC*** (WP90 11601/EN) 27 February 2004.

European Union Article 29 Working Party ***Declaration of the Article 29 Working Party on Enforcement*** WP 101 25 November 2004.

European Union Article 29 Working Party ***Report on the Obligation to Notify the National Supervisory Authorities, the Best Use of Exceptions and Simplification and the Role of the Data Protection Officers in the European Union*** WP 106 January 2005.

European Union Article 29 Data Protection Working Party ***Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*** November 2006.

European Union Article 29 Data Protection Working Party ***Opinion 4/2007 on the Concept of Personal Data*** 20 June 2007.

European Union Article 29 Data Protection Working Party ***Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)***18 February 2008.

Faul W ***Grondslae van die Beskerming van die Bankgeheim*** LLD thesis RAU 1991.

Federation of European Direct Marketing (FEDMA) ***European Code of Practice for the Use of Personal Data in Direct Marketing*** accessed at http://www.fedma.org/data-protection/ on 29 August 2008.

Financial Crime and Intelligence Division of the UK Financial Services Authority ***Report on Data Security in Financial Services - Firms' Controls to Prevent Data Loss by their Employees and Third-party Suppliers*** April 2008.

Flaherty D H ***Protecting Privacy in Surveillance Societies*** University of North Carolina Press 1989.

Flaherty DH "How to do a Privacy and Freedom of Information Act Site Visit" A revised version of a presentation to the Privacy Laws and Business Annual Conference, Cambridge, UK, July 1998.

Flaherty D H "Privacy Impact Assessments: An Essential Tool for Data Protection" 2000 accessed at http://aspe.hhs.gov/datacncl/flaherty.htm on 15/7/2005.

Froomkin, AM "The Death of Privacy?" ***Stanford Law Review*** Vol 52:1461 May 2000.

Gellman RM "Data Privacy Law (book review)" ***Government Information Quarterly*** Vol 14 No 2 1997 215. Review of the book by Schwartz PM and Reidenberg JR A Study of United States Data Protection Charlottesville, VA Michie 1996.

Goldman J " Health at the Heart of Files?" Brandeis Lecture delivered at the Massachusetts Health Data Consortium's Annual Meeting on April 28, 2001 and made available at the 23rd International Conference of Data Protection Commissioners, Paris 24-26 September 2001.

Global Internet Policy Initiative (GIPI) ***EU Directive on Privacy Protection in the Electronic Communications Sector*** October 2002 accessed at http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/spamstudy-en.pdf on 16 August 2007.

Global Internet Policy Initiative (GIPI) ***The International Legal Framework for Data Protection and its Transposition to Developing and Transitional Countries*** December 2004 accessed at http://www.cdt.org/ on 15/1/07.

Greenleaf G "Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners" Paper originally prepared for a workshop at the International Conference of Privacy and Data Protection Commissioners, Cardiff, UK September 2002, updated version accessed at http;//austlii.edu.au/graham/publications/2003/Reforming_reporting/ on 22/1/2005.

Guild E & Brouwer E "The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US" Centre for European Policy Studies Policy Brief No 109 July 2006.

Gundermann L "Genetics and Privacy: Biobanking- Trustees- Audits" Paper delivered at Health Information Privacy Day in Toronto 24 September 2007.

Gunning P "Central Features of Australia's Private Sector Privacy Law" ***Privacy Law and Reporter*** Volume 7 Number 10May 2001.

Gutwirth S (translation by Casert R) ***Privacy and the Information Age*** Rowman & Littlefield Publishers Lanham 2002.

Hahn R W "An Assessment of the Costs of the Proposed Online Privacy Legislation" Study commissioned by the Association for Competitive Technology (ACT) May 7, 2001.

Health Professions Council of South Africa (HPCSA) Patient Confidentiality Subcommittee of the National ICD-10 Task Team ***Patient Confidentiality*** 18 July 2007.

Hreinsson P "Projects and People (Islandic Health Sector Database)" Paper delivered at the 23rd International Conference of Data Protection Officers, Paris, September 2001.

Hustinx PJ "Co-regulation or Self-regulation by Public and Private Bodies - The Case of Data Protection" Published in Freudendesgabe fur Alfred Bullesbach 2002 Umbruch von Regelungssystemen in der Informationgesellschaft accessed at http://www.dutchdpoa.nl/documenten/enon 11/11/07.

Information Commissioner ***Chapter 3: The Data Protection Principles of the IC's Legal Guidance*** Version 1 Nov 2001.

Information Commissioner ***Freedom of Information Act Awareness Guidance No1*** accessed at http://www.informationcommissioner.gov.uk/eventual.aspx?ide77 on 17/2/2005.

Information Commissioner ***Data Protection Act 1998: The Eighth Data Protection Principle and International Data Transfers*** 30 June 2006.

Information Commissioner ***International Transfers of Personal Information: General Advice on How to Comply with the 8th Data Protection Principle*** Data Protection Guidelines 31 August 2007.

Information Commissioner ***Credit Explained*** accessed at www.ico.gov.uk on 20 August 2008.

Internet Service Providers Association (ISPA) ***A Code for Internet Service Providers Providing E-mail Services*** Spam Code of Practice, May 2007.

Jacob J "Health at the Heart of Files" Paper presented at the 23rd International Conference of Data Protection Commissioners, Paris, September 2001.

Jones C, Rankin TM and Rowan J "A Comparative Analysis of Law and Policy on Access to Health Care Provider Data: Do Physicians have a Privacy Right over the Prescriptions they Write?" ***Canadian Journal of Administrative Law and Practice*** 2001.

Joubert WA ***Grondslae van die Persoonlikheidsreg*** Balkema Cape Town 1953.

Joubert WA "Die Persoonlikheidsreg: n Belanghebbende Ontwikkeling in die Jongste Regspraak in Duitsland" 1960 ***THRHR*** 23.

Kang J "Information Privacy in Cyberspace Transactions" 50 ***Stanford Law Review*** April 1998 1193.

King Committee on Corporate Governance ***King Report on Corporate Governance for South Africa*** 2002.

Klaaren J "Access to Information and National Security in South Africa" ***National Security and Open Government: Striking the Right Balance*** Maxwell School of Citizenship and Public Affairs Syracuse University New York 2003 195.

Korff D **Final Report: EC Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons** Commission of the European Communities (Study Contract ETD 97/B5-9500/78) accessed at http://europa.eu.int/comm/internal_market/privacy/docs/studies/legal_en.pdf on 5/4/2004.

Korff D **EC Study on Implementation of Data Protection Directive: Comparative Summary of National Laws** (Study Contract ETD 2001/B5-3001/A/49) Human Rights Centre Cambridge September 2002 accessed on 25/3/2005 at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/consultation/.

La Forest G V ***The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*** Report of the Special Advisor to the Minister of Justice 15 November 2005.

Laosebikan FO ***Privacy and Technological Development: A Comparative Analysis of South African and Nigerian Privacy and Data Protection Laws*** Ph.D Thesis University of Kwazulu-Natal 2007.

Loukidelis D "Privacy Law Enforcement: The Experience in British Columbia Canada" Paper delivered at the APEC Symposium on Data Privacy Implementation: Developing the APEC Privacy Framework, Santiago, Chile, February 2004.

Loukidelis D "Transborder data flows & privacy—an update on work in progress" 7th Annual Privacy & Security Conference Victoria BC February 10, 2006.

Lopez JMF "The Data Protection Authority: The Spanish Model" Presentation delivered at the 24th International Conference of Data Protection and Privacy Commissioners Cardiff, 9-11 September 2002.

Lowrance WW "Privacy , Confidentiality, and Identifiability in Genomic Research" Paper delivered at the 29th International Conference of Data Protection and Privacy Commissioners September 2007.

McKerron RG ***The Law of Delict*** Juta Cape Town 1971.

McKinsey and Company, South Africa ***Calling: South Africa's Global Business Process Outsourcing and Off-shoring Opportunity Headline Report*** June 2005.

McQuoid-Mason D J ***The Law of Privacy in South Africa*** Juta Johannesburg 1978.

McQuoid-Mason D J "Consumer Protection and the Right to Privacy" 1982 ***CILSA*** 135.

McQuoid-Mason D J "Invasion of Privacy: Common Law v Constitutional Delict - Does it Make a Difference?" ***Acta Juridica*** 2000 227.

Mostert F "Public figures and privacy" ***De Rebus*** November 1997.

Nadasen S "Data Protection for Companies: Privacy and More" ***Insurance and Tax*** September 2003.

National Assembly of the Parliament of the Republic of South Africa ***Report of the Ad Hoc Committee on the Review of Chapter 9 and Associated Institutions*** Cape Town South Africa 31 July 2007.

National Telecommunications and Information Administration, Department of Commerce United States of America ***Elements of Effective Self-regulation for the Protection of Privacy and Questions Related to Online Privacy*** Notice and request for public comment RIN 0660-AA13 dated 6 May 1998.

National Telecommunications and Information Administration, Department of Commerce United States of America ***Privacy Report*** Appendix A: Marketing Profiles available at http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

Neethling J ***Die Reg op Privaatheid*** LLD thesis UNISA 1976.

Neethling. J "Die Reg op Privaatheid en die Konstitusionele Hof: Die Noodsaaklikheid vir Duidelike Begripsvorming: ***Bernstein v Bester*** 1996 2 SA 751 CC; ***Case and Curtis v Minister of Safety and Security*** 1996 3 SA 617 CC"1997 60 ***THRHR*** 137.

Neethling J "Aanspreeklikheid vir "Nuwe" Risiko's: Moontlikhede en Beperkinge van die Suid-Afrikaanse Deliktereg" 2002 65 ***THRHR*** 589.

Neethling J & Potgieter JM "Herlewing van die Amende Honorable as Remedie by Laster" 2003 66 ***THRHR*** 329.

Neethling J "The Concept of Privacy in South African Law" 2005 ***SALJ*** 18.

Neethling J ***Van Heerden-Neethling Unlawful Competition*** Lexis Nexis Durban 2008.

Neethling J "Data Protection and Juristic Persons" (2008) 71 ***THRHR***.

Neethling J "The Law of Delict and Punitive Damages" 2008 **Obiter**.

Neethling J, Potgieter JM & Visser PJ ***Neethling's Law of Personality*** Butterworths Durban 2005.

Neethling J, Potgieter JM & Visser PJ ***Law of Delict*** Butterworths Durban 2006.

New Zealand Law Commission ***Public Registers: Review of the Law of Privacy Stage 2*** Report 101 January 2008.

OECD "Inventory of Privacy Enhancing Technologies(PET's)" Report developed by Hall L in co-operation with the Secretariat of the Working Party on Information Security and Privacy of the Directorate for Science, Technology and Industry of the OECD dated 7 January 2002 (DSTI/ICCP/REG (2001) 1 FINAL).

OECD "OECD Governments Launch Drive to Improve Security of Online Networks" News release dated August, 7 2002.

OECD ***Consumers in the On-line Marketplace: the OECD Guidelines Three Years Later*** Report by the Committee on Consumer Policy on the Guidelines for Consumer Protection in the Context of Electronic Commerce February 2003 (DSTI/CP (2002) FINAL).

OECD Task Force on Spam ***Spam Issues in Developing Countries*** 26 May 2005.

OECD Task Force on Spam ***Anti-spam Regulation*** 15 November 2005.

OECD ***Draft Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Against Spam*** C (2006) 57 31 March 2006.

OECD ***Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*** 12 June 2007.

Office of the Federal Privacy Commissioner of Australia ***Draft National Privacy Principles Guidelines*** A Consultation document Australia 7 May 2001 available at http://www.privacy.gov.au/publications/dnppg.html accessed on 2/4/2003.

Office of the Federal Privacy Commissioner of Australia ***The Results of Research into Community, Business and Government Attitudes Towards Privacy in Australia*** July 31 2001 available at http://www.privacy.gov.au/publications/.

Office of the Federal Privacy Commissioner of Australia ***Guidelines on Privacy Code Development*** September 2001 available at http://www.privacy.gov.au/publications/.

Office of the Press Secretary The White House ***Fact Sheet: President Bush Signs Anti-SpamLaw*** 16 December 2003.

Office of the Privacy Commissioner of Canada ***Your Privacy Responsibilities: A Guide for Business and Organizations*** December 2000 available at http://www.privcom.gc.ca/.

Office of the Privacy Commissioner of Canada ***Annual Report to Parliament 2000-2001, Part One – Report on the Privacy Act*** December 2001 available at http://www.privcom.gc.ca/.

Office of the Privacy Commissioner of Canada ***Annual Report to Parliament 2000-2001, Part Two – Report on the Personal Information Protection and Electronic Documents Act***, December 2001 available at http://www.privcom.gc.ca/.

Office of the Privacy Commissioner of Canada "Determining the Appropriate Form of Consent Under the Personal Protection and Electronic Documents Act" ***Fact Sheet*** accessed at http://www.privcom.gc.ca/fs-fi/ On 25 May 2006.

Office of the Privacy Commissioner of Canada "Best Practices for Dealing with Pre-PIPEDA Personal Information (Grandfathering)" ***Fact Sheet*** accessed at http://www.privcom.gc.ca/fc-fi/on on 21 February 2008.

Office of the Privacy Commissioner of New Zealand ***Draft Guidance Note on Codes of Practice under Part VI of the Privacy Act*** Issue No 5 dated 5 December 1994 available at http://www.privacy.org.nz/recept/.

Office of the Privacy Commissioner of New Zealand ***Privacy Act Review 1998*** Discussion Paper No 2: Information Privacy Principles available at http://www.privacy.org.nz/recept/.

Office of the Privacy Commissioner of New Zealand ***Drafting Suggestions for Departments Preparing Public Register Provisions*** Note prepared by Blair Stewart Assistant Commissioner June 2005.

Office of the Privacy Commissioner of New Zealand ***Report to the Minister of Justice in Relation to the Unsolicited Electronic Messages Bill*** 3 April 2006.

Ombudsman for Long Term Insurance ***Annual Report*** 2005.

Parliament of Australia Senate Legal and Constitutional Committee ***Privacy in the Private Sector*** Chapter 7 The Co-regulation Model 1999 accessed at http://www.aph.gov.au/senate/committee/legcon_ctte/ on 25/4/2005.

Parliament of the Republic of South Africa ***Report of the Ad hoc Committee on the Review of Chapter 9 and Associated Institutions*** A report to the National Assembly of the Parliament of South Africa Cape Town South Africa 31 July 2007.

Performance and Innovation Unit, UK Cabinet Office ***Privacy and Data-sharing: The Way Forward for the Public Services*** April 2002.

Perlman L "Protection of Minors From Age-Restricted Content" Presentation made at LHR Adult Content Round Table 29 March 2007.

Perrin S, Black H, Flaherty D & Rankin TM ***The Personal Information Protection and Electronic Documents Act: An Annotated Guide*** Toronto, 2001.

Petzer N "Opnion: Who Should Carry the Internet Banking Can? ***De Rebus*** November 2003.

Piller, C "Privacy in Peril" ***Macworld*** 10 n7 Jul 1993 124 available at

http://www.newfirstsearch.oclc.org/.

Raab, CD "Privacy Protection: The Varieties of Self-regulation" Paper delivered at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002.

Rautenbach IM "The Conduct and Interests Protected by the Right to Privacy in Section 14 of the Constitution" ***TSAR*** 2001.1, 115.

Reidenberg J "Technologies for Privacy Protection" Presentation at the 23rd International Conference of Data Protection Commissioners, Paris, 24-26 September 2001.

Roberts A "New Strategies for Enforcement of the Access to Information Act" (2002) 27 ***Queens Law Journal*** 647.

Roos A "Data Protection Provisions in the Open Democracy Bill, 1997" (1998) 61 ***THRHR*** 499.

Roos A ***The Law of Data (Privacy) Protection: A Comparative and Theoretical Study*** LLD thesis UNISA October 2003.

Roos A "Data protection: Explaining the International Backdrop and Evaluating the Current South African Position" 2007 ***SALJ*** Vol124 400.

Rotenberg, M (ed.) ***The Privacy Law Sourcebook: United States Law, International Law and Recent Developments*** EPIC 2001.

Smedinghoff T "Trends in the Law of Information Security" ***BNA International World Data Protection Report*** August 2004.

South African Law Commission ***Computer-related Crime: Preliminary Proposals for Reform in Respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects*** Discussion Paper 99 Project 108 June 2001.

South African Law Reform Commission ***Privacy and Data Protection*** Project 124 Issue Paper 24 September 2003.

South African Law Reform Commission ***Privacy and Data Protection*** Project124 Discussion Paper 109 October 2005.

South African Law Reform Commission ***Statutory Revision: Review of the Interpretation Act 33 of 1957*** Project 25 Discussion Paper 112 September 2006.

Standards Council of Canada ***National Standard of Canada*** The Model Code for the Protection of Personal Information September 1995.

Stewart B "The New Privacy Laws: Exemptions and Exceptions to Privacy" Paper prepared for The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century Sydney 19 February 1997 accessed at http://www.privacy.org.nz/media/comfin.html on 24/06/2005.

Strathclyde Law School ***LLM in Information Technology and Telecommunications Law (Distance Learning)*** Web Est. 1994 Updated October 2001 available at http://itlaw.law.strath.ac.uk/distlearn/.

Strauss SA (red) ***Huldigingsbundel vir WA Joubert*** Butterworths Durban 1988.

Swire, P "New Study Substantially Overestimates Costs of Internet Privacy Protections" 9 May 2001.

Tang R "Data Protection, Freedom of Expression and Freedom of Information - Conflicting Principles or Complimentary Rights?" Paper delivered at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002.

Task Group on Open Democracy ***Open Democracy Act for South Africa: Policy Proposals*** 1995.

Thornton L "Protecting Minors form Harmful Content via Mobile Phones" Discussion Paper for Focus Group hosted by Lawyers for Human Rights Child Rights Project, 26 March 2007.

US Department of Commerce ***Privacy and the NII: Safeguarding Telecommunications-related Personal Information*** 23 October 1995 (NTIA Privacy Report) available at **http://www.ntia.doc.gov/ntiahome/privwhitepaper.html** accessed on 23/4/2002.

US Department of Health and Human Services **"**Protecting the Privacy of Patients' 'Health Information'" ***HHS Fact Sheet*** May 9, 2001.

US Department of Justice Computer Crime and Intellectual Property Section (CCIPS) "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet" March 9, 2000 available at http://www.usdoj.gov/criminal/cybercrime/.

United States Federal Trade Commission ***Privacy Online: A Report to Congress*** June 1998.

United States Federal Trade Commission ***Privacy Online: Fair Information Practices in the Electronic Marketplace*** Report to Congress May 2000.

United States General Accounting Office (GAO) "Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk" Statement of Dacey RF November, 19 2002 (GAO-03-303T).

US Senate Republican Policy Committee **Legislative Notice** No 43 October 22, 2003.

Valeri L "Is Technology a Privacy-enhancer or Privacy Threat? Some Thoughts" Presentation delivered at the 24th International Conference of Data Protection and Privacy Commissioners Cardiff, 9-11 September 2002.

Vande Lanotte J, Sarkin J & Haeck Y (eds) ***The Principle of Equality: A South African and a Belgian Perspective*** Papers from a seminar held in Ghent Belgium 6-11 February 2000 Maklu Antwerpen 2001.

Van der Merwe NJ & Olivier PJJ ***Die Onregmatige Daad in die Suid-Afrikaanse Reg*** Van der Walt Pretoria 1989.

Victorian Law Reform Commission ***Privacy Law : Options for Reform*** Information Paper 2001 available at www.lawreform.vic.gov.au.

Visser PJ "Some Principles Regarding the "Requester" of Access to a Record and Related Issues in terms of the Promotion of Access to Information Act 2 of 2002" (2002) 65 ***THRHR*** 254.

Volman Y "Public Sector Information: A Key Resource for Europe" Presentation made at Bristol Conference 2 March 2005.

Walker C "Regulation and Guidance on the Use of Child Data" ***Data Protection Law and Policy*** Newsletter for Data Protection Professionals October 2006 Vol 3 Issue 10.

Woolman S "Coetzee: The Limitations of Justice Sachs's Concurrence" 1996 ***SAJHR*** 12.1 99.

World Medical Association ***Declaration on Ethical Considerations Regarding Health Databases*** Washington, 2002.

Wugmeister M, Retzer K, and Rich C "Codes of Conduct: The Solution for International Data Transfers?" ***Morrison & Foerster Legal Updates and News*** July 2003 (Article first published in WPDR, June 2003, accessed on 15/8/2005 at http://www.mofo.com/tools/print.asp?mofo_dev/news/updates/files/update1170.html.

Zaroukian MH "EHR's and Patient Data Privacy - Building Trust Through Effective Identity Profiling, Authentication and Authorisation" Presentation delivered at the Health Information Privacy Day Toronto September 2007.

TABLE OF CASES

SOUTH AFRICA

Financial Mail (Pty) Ltd ao v Sage Holdings Ltd ao 1993 (2) SA 451 (A).

Fose v Minister of Safety and Security 1997 (3) SA 786 (CC).

Foulds v Smith 1950 (1) SA 1 (A).

Gardener ao v Walters ao NNO (in re Ex parte Walters ao NNO) 2002 (5) SA 796 (C).

Gardener v Whitaker 1995 (2) SA 672 (E); 1994(5) BCLR 19 (E).

Gosschalk v Rossouw 1966 (2) SA 476 (C).

Government of the Republic of South Africa v Sunday Times Newspaper 1995 (2) SA 221 (T).

Grutter v Lombard ao 2007 (4) SA 89 (SCA).

Holomisa v Argus Newspapers Ltd 1996 (2) SA 588 (W).

Informa Confidential Reports (Pty) Ltd v Abro 1975 (2) SA 760 (T).

Investigating Directorate: Serious Economic Offences ao v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty) Ltd ao v Smit NO ao 2001 (1) SA 545 (CC).

Islamic Unity Convention v Independent Broadcasting Authority ao 2002 (4) SA 294 (CC); 2002 BCLR 433 (CC).

Jansen Van Vuuren ao NNO v Kruger 1993 (4) SA 842 (A).

Johncom Media Investments Limited v Mandel ao Case CCT 08/08; [2009] ZACC 5.

Jooste v National Media Ltd ea 1994 (2) SA 634 (C).

Khumalo ao v Holomisa 2002 (5) SA 401 (CC); 2002 (8) BCLR 771 (CC)***.***

Kidson ao v SA Associated Newspapers Ltd 1957 (3) SA 461 (W).

Klein v Attorney-General, Witwatersrand Local Division ao 1995 (3) SA 848 (W), 1995 (2) SACR 210(W).

Kritzinger v Perskorporasie van Suid-Afrika (Edms) Bpk ea 1981 (2) SA 373 (O).

Laugh It Off Promotions CC v SAB International Finance BV t/a Sabmark International 2006 (1) SA 144 (CC); 2005 (8) BCLR 743 (CC).

Lotus River, Ottery, Grassy Park Residents Association ao v South Peninsula Municipality 1999 (2) SA 817 (C).

Mandela v Falati 1995 (1) SA 251 (W).

Mhlongo v Bailey ao 1958 (1) SA 370 (W).

Midi Television (Pty) Ltd v Director of Public Prosecutions Western Cape 2007 (5) SA 540 (SCA); 2007(9) BCLR 958 (SCA).

Mineworkers Investment Co (Pty) Ltd v Modibane 2002 (6) SA 512 (W)**.**

Mistry v Interim Medical and Dental Council of South Africa ao 1998 (4) SA 1127 (CC) ;1998 (7) BCLR 880 (CC).

Morar v Casojee 1911 EDL 171.

Motor Industry Fund Administrators (Pty) Ltd ao v Janit ao 1994 (3) SA 56 (W);1995 (4) SA 293 (A).

Mr and Mrs "X" v Rhodesia Printing and Publishing Co Ltd 1974 (4) SA 508 (R).

Mthembi - Mahanyele v Mail and Guardian Ltd 2004 (6) SA 329 (SCA).

NM ao v Smith ao 2007(7) BCLR 751 (CC).

National Media Ltd ao v Bogoshi 1998 (4) SA 1196 (A).

National Media Ltd ao v Jooste 1996 (3) SA 262 (A).

Neethling v Du Preez: Neethling v The Weekly Mail 1994 (1) SA 708 (A).

Nell v Nell 1990 (3) SA 889 (T).

O'Keeffe v Argus Printing and Publishing Co Ltd ao 1954 (3) SA 244 (C).

Pakendorf v De Flamingh 1982 (3) SA 146 (A).

Pauw v African Guarantee and Indemnity Co Ltd 1950 (2) SA 132 (SWA).

Pharmaceutical Manufacturers Association of South Africa ao: In re Ex parte President of the Republic of South Africa ao 2000 (2) SA 674 (CC).

Pickard v SA Trade Protection Society (1905) 22 SC.

President of the Republic of South Africa ao v South African Rugby Football Union ao 1999(4) SA 147 (CC).

Prinsloo ao v SA Associated Newspapers Ltd ao 1959 (2) SA 693 (W).

R v R 1954 (2) SA 134 (N).

R v S 1955 (3) SA 313 (SWA).

R v Holliday 1927 CPD 395.

R v Umfaan 1908 TS 62**.**

Rhodesian Printing and Publishing Co Ltd v Duggan ao 1975 (1) SA 590 (RA).

S v A ao 1971 (2) SA 293 (T).

S v Boshoff ao 1981 (1) SA 393 (T).

S v I ao 1976 (1) SA 781 (RA).

S v Bailey 1981 (4) SA 187 (N).

S v Manamela ao (Director-General of Justice Intervening) 2000 (5) BCLR 491 (CC).

S v Makwanyane ao 1995 (3) SA 391 (CC); 1995 (6) BCLR 665 (CC).

Sage Holdings Ltd ao v Financial Mail (Pty) Ltd ao 1991 (2) SA 117 (W).

Shelton v Commissioner for the SARS[11] 2000 (2) SA 106 (E).

Swanepoel v Minister van Veiligheid en Sekuriteit 1999 (4) SA 549 (T).

Tshabalala-Msimang ao v Makhanya ao Witwatersrand High Court Case Number 18656/07 30 August 2007.

[11] 2002 (2) SA 106 ECD.

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977(4) SA 376 T; 1979 (1) SA 441 (A).

Walker v Van Wezel 1940 WLD 66.

Young v Sheikh 2004 (3) SA 46 (C).

CANADA

Edmonton Journal v Alberta (Attorney-General) 1989 64 DLR 4th 577 (SCC).

UNITED KINGDOM

Campbell v MGN Limited [2002] EWCA Civ 1371; [2003]QB633 (CA).

UNITED STATES

Griswold v. Connecticut 381 U.S. 479 (1965).

Katz v. United States 389 U.S. 347 (1967).

Lake v. WalMart Stores, Inc 582 N.W.2d 231 (Minn. 1998).

Paul v. Davis 424 U.S. 714 (1976).

Union Pacific R.R Co v Botsford 141 US 251 11 S.Ct 1000, 35 L.Ed 734(1891).

Whalen v. Roe 429 U.S. 589 (1977).

SELECTED LEGISLATION

SOUTH AFRICA

Banking Act 38 of 1942.

Broadcasting Act 4 of 1999.

Companies Act 61 of 1973.

Constitution of the Republic of South Africa,1996.

Consumer Protection Act 68 of 2008.

Copyright Act 98 of 1978.

Criminal Procedure Act 51 of 1977.

Customs and Excise Act 91 of 1964.

Defence Act 42 of 2002.

Electoral Act 73 of 1998.

Electronic Communications and Transactions Act 25 of 2002.

Electronic Communications Security Pty (COMSEC) Act 68 of 2002.

Financial Advisory and Intermediary Services Act (FAIS) 37 of 2002.

Financial Intelligence Centre Act (FICA) 38 of 2001.

Human Rights Commission Act 54 of 1994.

Independent Broadcasting Authority Act 153 of 1993.

Independent Communication Authority of South Africa Amendment Act of 2000 (as amended).

Interception and Monitoring Prohibition Act 127 of 1992.

Interpretation Act 33 of 1957.

Intelligence Services Act 65 of 2002.

Intelligence Services Oversight Act 40 of 1994.

Labour Relations Act 66 of 1995.

Local Government Municipal Electoral Act 27 of 2000.

Local Government Municipal Property Act 6 of 2004.

Local Government Municipal Structures Act 117 of 1998.

Long-term Insurance Act 52 of 1998.

National Archives of South Africa Act 43 of 1996.

National Credit Act 34 of 2005.

National Credit Regulations, 2006 Published under GN R 489 in GG 28864, 31 May 2006.

National Health Act 61 of 2003.

National Key Points Act 102 of 1980.

National Strategic Intelligence Act 39 of 1994.

National Water Act 36 of 1998.

Open Democracy Bill [B67-98].

Promotion of Access to Information Act 2 of 2000.

Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000.

Protection of Information Act 84 of 1982.

Protection of Information Bill [B28-2008].

Public Audit Act 25 of 2004.

Public Finance Management Act 1of 1999.

Public Protector Act 23 of 1994.

Public Service Act,1994 (Proc. 103 of 3 June 1994).

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

Revenue Laws Second Amendment Bill [B81-2008].

SA Reserve Bank Act 90 of 1989.

Short-term Insurance Act 53 of 1998.
State Information Technology Agency Act 88 of 1998.

Statistics Act 6 of 1999.

Telecommunications Act 103 of 1996.

Telecommunications Amendment Act 103 of 1996.

ARGENTINA

Personal Data Protection Act, 2000**.**

AUSTRALIA

Commonwealth of Australia Constitution Act.

Privacy Act, 1988.

Privacy Amendment (Private Sector) Act, 2000.

Spam Act 129, 2003 (as amended).

CANADA

Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982.

Privacy Act, 1982.

Personal Information Protection and Electronic Documents Act, 2000.

Quebec Act respecting the Protection Of Personal Information in the Private Sector, 1993.

GERMANY

Germany's Federal Data Protection Act, 1990.

HONG KONG

Personal Data (Privacy) Ordinance.

NETHERLANDS

Constitution of the Kingdom of the Netherlands, 1989.

Personal Data Protection Act 2000 (Wet Bescherming Persoonsgegevens).

NEW ZEALAND

Privacy Act, 1993.

Unsolicited Electronic Messages Act, 2007.

UNITED KINGDOM

Consumer Credit Act, 1974.

Data Protection Act, 1998.

Data Protection (Processing of Sensitive Personal Data) Order 1999.

Freedom of Information Act, 2000.

Human Rights Act, 1998.

Privacy and Electronic Communications Regulations, 2003.

USA

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, 2003.

Children’s Online Privacy Protection Act (COPPA), 1988 (passed in Congress 1998).

Drivers Privacy Protection Act, 1994.

E-Government Act, 2002.

Electronic Communications Privacy Act,1986.

Fair and Accurate Credit Transactions Act, 2003.

Fair Credit Reporting Act, 15 U.S.C. 1681, 1970.

Financial Services Modernisation Act, 1999 (Gramm-Leach-Bliley Act).

Freedom of Information Act, 1966.

Homeland Security Act, 2002.

Privacy Act, 1974.

Privacy Protection Act,1980.

Telephone Consumer Protection Act, 1991.

The Right to Financial Privacy Act, 1978.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001 (USA PATRIOT Act).

Video Privacy Protection Act, 1988.

CONVENTIONS, DIRECTIVES, GUIDELINES AND DECLARATIONS

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) Regarding the Supervisory Authorities and Trans-border Data Flows, ETS No 179, open for signature 8.11.2001.

African [Banjul] Charter on Human and People's Rights adopted June 27, 1981 OAU Doc. CAB/LEG/67/3 rev.5, 21 I.L.M. 58 (1982) entered into force Oct 21, 1986.

American Convention on Human Rights, "Pact of San Jose, Costa Rica" 22 November 1969 entered into force on 18 July 1978.

American Declaration on Rights and Duties of Mankind approved by the Ninth International Conference of American States, Bogota, Columbia, 1948.

Asia-Pacific Economic Cooperation (APEC) ***Privacy Framework*** (2005).

Asia- Pacific Economic Cooperation "APEC Data Privacy Pathfinder: Proposed Work Plan" Electronic Communications Steering Group (ECSG) Meeting, Cairns, Australia, 29 June 2007.

Commission of the European Communities (authors Serge Gauthronet and Etienne Drouard) ***Unsolicited Commercial Communications and Data Protection***, January 2001.

Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005) open for signature November 4, 1950, entry into force September 3, 1950.

Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS No 108, Strasbourg, 1981,(CoE Convention) available at <http://www.coe.fr/eng/legaltxt/108e.htm>.

Council of Europe Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, 4 October 2005.

Council of European Union Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR)Data by Air Carriers to the United States Department of Homeland Security(DHS)(2007 PNR Agreement)Brussels 18 July 2007.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (EU Directive).

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector Referred to as the ISDN Directive (replaced by 2002/58/EC dated 12 July 2002).

Directive 2000/31/EC of the European Parliament and of the Council of 2000 on Electronic Commerce dated 8 June 2000.

Directive 2002/21/EC of the European Parliament and of the Council on a Common Regulatory Framework for Electronic Communications Networks and Services of 25 June 2002.

Directive 2002/58/EC on Privacy Protection in the Electronic Communications Sector dated 12 July 2002..

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the Re-use of Public Sector Information.

Directive 2004/82/EC of the European Parliament and of the Council of 29 April 2004 on the obligations of carriers to communicate passenger data.

International Covenant on Civil and Political Rights (ICCPR),adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976.

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution 45/158 of December 18, 1990.

Organisation for Economic Co-operation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981.

Organisation for Economic Co-operation and Development (OECD) "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.

United Nations Convention on Migrant Workers. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution 45/158 of December 18, 1990.

United Nations Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990.

United Nations (UN) Guidelines Concerning Computerised Personal Data Files (hereinafter termed UN Guidelines) adopted by the UN General Assembly on 14 December 1990 Doc E/CN.4/1990/72, 20.2.1990.

Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948.

CHAPTER 1: INTRODUCTION

1.1 History of the investigation

1.1.1 On 17 November 2000 the South African Law Reform Commission ("the Commission") considered and approved the inclusion in its programme of an investigation entitled "Privacy and Data protection". [1]

1.1.2 The impetus behind the decision of the Commission to include this investigation in its programme lay in the Report of the Ad Hoc Joint Committee on the Open Democracy Bill dated 24 January 2000[2] (the Open Democracy Bill was later renamed and became the Promotion of Access to Information Act).[3]

1.1.3 The report pointed out that the Open Democracy Bill (as it then was) dealt with access to personal information in the public and private sector to the extent that it included provisions regarding mandatory protection of the privacy of third parties. The report went on to say :

> The Bill only deals with the aspect of access to private information of an individual, be it access by that individual or another person, and does not regulate other aspects of the right to privacy, such as the correction of and control over personal information and so forth.

The Committee furthermore reported that foreign jurisdictions with access to information legislation have also enacted separate privacy and data protection legislation.

1.1.4 The Committee therefore requested the Minister for Justice and Constitutional Development

---

1 89th Meeting of the Commission held on 17 November 2000. The Minister confirmed the inclusion of the investigation on 8 December 2000.

2 Ad hoc Joint Committee of South African Parliament ***Report of the Ad Hoc Joint Committee on the Open Democracy Bill*** *[*B67-98], 24 January 2000, as published in the Announcements, Tablings and Committee Reports of Parliament.

3 Promotion of Access to Information Act 2 of 2002.

to introduce privacy and data protection legislation in Parliament, after thorough research of the matter, as soon as reasonably possible.[4] The Minister, in turn, approached the Commission to consider the possible inclusion of such an investigation in its programme.

1.1.5 The investigation was included in the programme of the Commission and the Minister appointed a Project Committee, at the request of the Commission, to assist the Commission in its task. The Chairperson of the Committee is The Honourable Mr Justice Craig Howie. Prof Johann Neethling was appointed as project leader and the other members are Prof Iain Currie, Ms Caroline da Silva, Ms Christiane Duval, Prof Brenda Grant, Ms Adri Grobler, Mr Mark Heyink, Ms Saras Jagwanth and Ms Allison Tilley. In March 2007 Prof PJ Schwikkard was delegated to the Project Committee to act as the representative of the newly-appointed Commission.[5]

1.2 Exposition of the problem

1.2.1 A person's right to privacy entails that such a person should have control over his or her personal information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions. [6]

1.2.2 Information protection is an aspect of safeguarding a person's right to privacy. It provides for the legal protection of a person [7] (the data subject) in instances where such a person's personal particulars (information) is being processed by another person or institution (the data user/responsible party[8]). Processing of information generally refers to the collecting, storing, using and communicating of information.

---

4 See para 4 on page 17 of the Report of the Ad Hoc Joint Committee referred to above.

5 The term of the previous Commission expired on 31 December 2006 and a new Commission was appointed as from 1 January 2007.

6 Neethling J, Potgieter JM & Visser PJ ***Neethling's Law of Personality*** Butterworths Durban 2005 (hereafter referred to as "***Neethling's Law of Personality***") 31 fn 334; **National Media Ltd ao v Jooste** 1996 (3) SA 262 (A) 271-2.

7 Although the primary concern here is with information relating to an identified or identifiable living (natural) person, information on juristic persons are also included (see Neethling J "Databeskerming : Motivering en Riglyne vir Wetgewing in Suid-Afrika" in Strauss SA (red) ***Huldigingsbundel vir WA Joubert*** Butterworths Durban 1988 (hereafter referred to as "Neethling ***Huldigingsbundel WA Joubert***") at 105 fn 2. See furthermore Chapter 3 below regarding the substantive scope of the proposed legislation.

8 See clause 2 (definition section) of the draft proposed Protection of Personal Information Bill set out in Annexure C to this report (hereafter referred to as "the Bill" or "POPIA") for a definition of "responsible party".

1.2.3 The processing of information by the responsible party threatens the personality in two ways:[9]

a) First, the compilation and distribution of personal information creates a direct threat to the individual's privacy; [10] and

b) second, the acquisition and disclosure of false or misleading information may lead to an infringement of his identity.[11]

1.2.4 The recognition of the right to privacy is deeply rooted in history. Psychological and anthropological evidence suggest that every society, even the most traditional, adopts mechanisms and structures that allow individuals to resist encroachment from other individuals or groups.[12] Privacy is embedded in very old and well-understood social conventions. The value of stressing the universality of privacy is the way it can be equated with common decency.[13]

1.2.5 The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights,[14] which also protects territorial and communications privacy. The right to privacy is also dealt with in various other international instruments.[15]

---

9 ***Neethling's Law of Personality*** at 270-1. Other personality rights, especially the right to a good name or fama, which are infringed through the communication of defamatory data (cf eg ***Pickard v SA Trade Protection Society*** (1905) 22 SC 89*;* ***Morar v Casojee*** 1911 EDL 171; ***Informa Confidential Reports (Pty) Ltd v Abro*** 1975 (2) SA 760 (T)) may obviously also be relevant.

10 ***Neethling's Law of Personality*** at 270: Privacy includes all those personal facts which a person himself determines should be excluded from the knowledge of outsiders. Privacy is infringed if outsiders become acquainted with such information. This occurs through intrusion into the private sphere or disclosure of private facts.

11 ***Neethling's Law of Personality*** at 271: The processing of incorrect or misleading personal data through the data media poses a threat to an individual's identity, since the information may be used in a manner which is not in accordance with his true personal image. Obsolete information can mislead. The problems grow when the data are wrong.

12 Westin, A ***Privacy and Freedom*** New York Antheum 1967 as referred to by Bennett CJ "What Government Should Know About Privacy: A Foundation Paper" Presentation prepared for the Information Technology Executive Leadership Council's Privacy Conference, June 19, 2001 (Revised in Aug 2001)(hereafter referred to as "Bennett ***Government Foundation Paper***"); see also Roos A ***The Law of Data (Privacy) Protection: A Comparative and Theoretical Study*** LLD Thesis UNISA October 2003 (hereafter referred to as "Roos-thesis") at 1 for examples of information collection through the ages.

13 Chadwick P "Who Me? Stimulating Privacy Awareness" Paper delivered at the Private Sector Privacy in a Changing World Conference,Vancouver, BC on 20-21 September 2007.

14 Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948.

15 The United Nations Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990; the International Covenant on Civil and Political Rights (ICCPR), adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976; and the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution

(continued...)

1.2.6 In South Africa the right to privacy is protected in terms of both our common law[16] and in section 14 of the Constitution. [17] The common law protects rights of personality under the broad umbrella of the *actio injuriarum.*[18] In terms of the common law the right to privacy is limited by the rights of others and the public interest.[19]

1.2.7 The recognition and protection of the right to privacy as a fundamental human right in the Constitution provides an indication of its importance.[20] The constitutional right to privacy is, like its common law contemporary, not an absolute right but may be limited in terms of our law of general application[21] and has to be balanced with other rights entrenched in the Constitution. [22]

---

15 (...continued)
45/158 of December 18, 1990. On a regional level, various treaties make these rights legally enforceable. See for example Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms **,**open for signature November 4, 1950, entry into force September 3,1950. The American Convention on Human Rights "Pact of San Jose,Costa Rica" 22 November 1969, entered into force on 18 July 1978 (Art 11,14) and the American Declaration on Rights and Duties of Mankind approved by the Ninth International Conference of American States,Bogota,Columbia,1948 (Article V,IX and X) contain provisions similar to those in the Universal Declaration and International Covenant; The European Convention furthermore created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been active in the enforcement of privacy rights and have consistently viewed Article 8's protections expansively and interpreted the restrictions narrowly. In trying to give the necessary focus and relevance to international law, in 1994, South Africa signed and ratified three major human rights treaties of which ICCPR was one. There has, however, not been any real strategy for reviewing international human rights instruments to determine whether and how to sign and ratify them. Sarkin J "Implemetation of Human Rights in South Africa: Constitutional and Pan-African Aspects: A South African and Belgium Perspective" in Vande Lanotte J, Sarkin J and Haeck Y (eds) ***The Principle of Equality: A South African and a Belgian Perspective*** Papers from a seminar held in Ghent, Belgium 6-11 February 2000 Maklu, Antwerpen, 2001.

16 In terms of the common law every person has personality rights such as the right to privacy, identity, dignity, good name and bodily integrity. See ***Neethling's Law of Personality*** at 51.

17 The Constitution of the Republic of South Africa, 1996 (hereafter referred to as "the Constitution") which came into operation on 4 February 1997. Section 14 of the Constitution reads as follows:

Everyone has the right to privacy, which includes the right not to have-
- a) their person or home searched;
- b) their property searched;
- c) their possessions seized; or
- d) the privacy of their communications infringed.

Section 14 (a), (b) and (c) of the Constitution seek to protect an individual from unlawful searches and seizures. Section 14(d) accommodates a broader protection of privacy approaching that covered by the common law *actio iniuriarum* in South African law.

18 See discussion in Chapter 2 below.

19 See discussion in Chapter 2 below.

20 ***Neethling's Law of Personality*** at 219-220.

21 Section 36 of the Constitution.

22 See the discussion of sections 16, 22 and 32 of the Constitution in Chapter 2 below. The law should also consider such competing interests as administering national social programmes, maintaining law and order, and protecting the rights, freedoms and interests of others, including the commercial interests of industry sectors such as banking, insurance, direct
(continued...)

1.2.8 In the drafting of legislation a proper balance has to be found between the different competing interests, namely an open and accountable society on the one hand, and the right to be left alone on the other:

a) Firstly, the Constitution recognises every person's right to choose their trade, occupation or profession freely.[23] It is clear that in order to exercise this right properly,[24] an individual may need personal information about others. [25]

b) Secondly, it is obvious that the state (and its organs) and business can only fulfil its functions properly if it also has access to sufficient personal information regarding their subjects and clients.

Future legislation will have to accommodate all these rights and interests in a balanced manner.

1.2.9 There are many reasons why individuals disclose information about themselves and allow organisations to keep personal information about them. Sometimes it is because they are required to do so or because the provision of a particular product or service is conditional upon them giving that information, such as when they are applying for a credit card or a government benefit. At other times it is because they are providing it for a particular purpose such as when they enter a competition, or visit a doctor. When people provide information in one context, they often do not realise that this information may ultimately be used for other purposes as well.[26] The most important private data users are credit bureaux, transport companies, the health and medical profession, banks and financial institutions, the insurance industry, and the retail and direct marketing industry. As far as the state is concerned, individuals are required by statute to provide certain information.

1.2.10 Interest in the right to privacy increased worldwide in the 1960s and 1970s with the advent

---

22 (...continued)
marketing, health care, pharmaceuticals and travel services. In recent years large scale gathering and sharing of personal information has become a way of life for business and government. The task of balancing these opposing interests is a delicate one. See also ***Neethling's Law of Personality*** 273.

23 See section 22 of the Constitution. See discussion in Chapter 2.

24 See also section 15(1) of the Constitution, dealing with the right to undertake scientific research.

25 See sections 16 and 32 of the Constitution. See further discussion in Chapter 2.

26 Victorian Law Reform Commission ***Privacy Law: Options for Reform*** Information Paper 2001 available at www.lawreform.vic.gov.au (hereafter referred to as "Victorian Law Reform Commission ***Privacy Law: Options for Reform***") at 21.

of information technology. [27] The surveillance potential of powerful computer systems prompted demands for specific rules [28] governing the collection and handling of personal information.[29] The question could no longer be whether the information could be obtained, but rather whether it should be obtained and, once it has been obtained, how it should be used. [30] The fundamental assumption underlying the answer to these questions is that if you can protect the information on which decisions are made about individuals, you can also protect the fairness, integrity and effectiveness of that decision-making process.[31]

1.2.11 The genesis of modern legislation in the area of information protection can be traced to the first information protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978).[32] There are now well over fifty countries which have enacted information protection statutes at national or federal level and the number of such countries is steadily growing. [33]

1.2.12 Early in the debates, it was, however, recognised that information privacy could not be regarded as simply a domestic policy problem. The increasing ease with which personal information could be transmitted outside the borders of the country of origin produced an interesting history of international harmonisation efforts, and a concomitant effort to regulate

---

27 Piller C "Privacy in Peril" ***Macworld*** 10 n7, Jul 1993 124-130 available at http://newfirstsearch.oclc.org/: The advent of telecommunications, the growth of centralised government, and the rise of massive credit and insurance industries that manage vast computerised databases have turned the modest records of an insular society into a basaar of data available to nearly anyone for a price; Neethling ***Huldigingsbundel WA Joubert*** at 105 et seq.

28 Electronic Privacy Information Center (EPIC) and Privacy International ***Privacy and Human Rights Report* 2002 *An International Survey of Privacy Laws and Developments*** United States of America 2002 available at http://www.privacyinternational.org/ (hereafter referred to as "EPIC and Privacy International ***Privacy and Human Rights Report 2002***") at 8.

29 For the opposite viewpoint: The chief executive officer of Sun Microsystems, Scott McNealy told a group of reporters and analysts in 1999 that consumer privacy issues are a "red herring". He reputedly said: "You have zero privacy anyway. Get over it." Jodie Bernstein, Director of the Bureau of Consumer Protection at the Federal Trade Commission in the USA, responded that McNealy's remarks were out of line. Polly Sprenger "Sun on Privacy: Get Over IT" ***Wired News*** 26 January 1999 available at http://www.com/news/politics/.

30 See Roos thesis at 8 for examples of technological inventions such as data matching, profiling, data mining, smart cards, cookies and spam that create an increased threat to the privacy of persons.

31 Bennett ***Government Foundation Paper*** at 6.

32 An excellent analysis of these laws is found in Flaherty DH ***Protecting Privacy in Surveillance Societies*** University of North Carolina Press 1989.

33 Bygrave *LA* ***Data Protection: Approaching Its Rationale, Logic and Limits*** Kluwer Law International The Hague 2002 (hereafter referred to as "Bygrave ***Data Protection***") at 30. See also the discussion in Chapter 9 below.

transborder information flows.[34]

1.2.13 Two crucial international instruments evolved:

a) The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention);[35] and
b) the 1981 Organisation for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[36]

1.2.14 These two agreements have had a profound effect on the enactment of laws around the world. Nearly thirty countries have signed the CoE Convention. The OECD guidelines have also been widely used in national legislation, even outside the OECD member countries.

1.2.15 The OECD Guidelines incorporate eight principles relating to the collection, purpose, use, quality, security and accountability of organisations in relation to personal information. However, the OECD Guidelines do not set out requirements as to how these principles are to be enforced by member nations. As a result, OECD member countries have chosen a range of differing measures to implement the privacy principles.[37]

1.2.16 In 1995, the European Union enacted the Data Protection Directive[38] in order to harmonise member states' laws so as to provide consistent levels of protection for citizens and ensure the free flow of personal information within the European Union. The Directive arose from the conviction that European citizens were losing control over their personal information and that they had a fundamental right to privacy. It, furthermore, imposed its own standard of protection on any country within which personal information of European citizens might be processed. Articles 25 and 26 of the Directive stipulate that personal information should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection" (the so-called safe-harbour

---

34 Bennett ***Government Foundation Paper*** at 6.

35 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data ETS No. 108 Strasbourg, 1981 (hereafter referred to as "CoE Convention") available at <http://www.coe.fr/eng/legaltxt/108e.htm>.

36 Organisation for Economic Co-operation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981 (hereafter referred to as "OECD Guidelines") available at http://www.oecd.org/documentprint/.

37 See Chapter 9 below for the developments in the APEC countries.

38 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (hereafter referred to as "EU Directive").

principle).[39]

1.2.17 The Directive sets a baseline common level of privacy that not only reinforces current information protection law, but also establishes a range of new rights. The Directive contains strengthened protection over the use of sensitive personal information relating, for example, to health, sex life or religious or philosophical beliefs. The commercial and government use of such information generally requires "explicit and unambiguous" consent of the data subject. The directive applies to the processing of personal information in electronic and manual files. It provides only a basic framework which is to be developed and elaborated on in national laws.[40]

1.2.18 The Directive was adopted with member states being required to implement its provisions by October 24, 1998. This time-table has proved difficult for member states to comply with.

1.2.19 Some account should also be taken of the UN Guidelines.[41] The Guidelines are intended to encourage those UN Member States without information protection legislation in place to take steps to enact such legislation based on the Guidelines. The Guidelines are also aimed at encouraging governmental and non-governmental international organisations to process personal information in a responsible, fair and privacy-friendly manner. The Guidelines are not legally binding and seem to have had much less influence on information regimes than the other instruments.[42]

1.2.20 The Commonwealth Law Ministers furthermore proposed for consideration by Senior Officials at their meeting in November 2002 that model legislation (Model Bills) to implement the Commonwealth commitment to freedom of information should be enacted in member countries for both the public and the private sectors.

1.2.21 The intent of the proposed model legislation is to ensure that governments and private organisations accord personal information an appropriate measure of protection, and also that such information is collected only for appropriate purposes and by appropriate means. The model seeks, in accordance with general practice in member countries, only to deal with information privacy

---

39 For further discussion see Chapter 6 below.

40 As referred to in Strathclyde Law School ***LLM in Information Technology and Telecommunications Law (Distance Learning)*** Web Estr. 1994 Updated Oct 16 2001 "Notes for Information Security Theme Two: Data protection" (hereafter referred to as "Strathclyde Law School LLM") at 4 (accessed at http://itlaw.law.strath.ac.uk/distlearn/). A good example is the Directive's requirement that member states shall appoint an independent supervisory agency. The particular form of the agency is not specified.

41 The United Nations' (UN) Guidelines Concerning Computerised Personal Data Files adopted by the UN General Assembly on 14 December 1990 Doc E/CN.4/1990/72 20.2.1990 (hereafter referred to as "UN Guidelines").

42 Bygrave ***Data Protection*** at 33.

which is the most common aspect of privacy regulated by statute and which involves the establishment of rules governing the collection and handling of personal information, such as those relating to the status of credit or medical records. It also seeks to create a legal regime which can be administered by small and developing countries.[43]

1.2.22 The international instruments referred to above will form the basis of discussion throughout this paper. The reasons are that they contain clear basic principles of information protection and that they serve as influential models of national and international initiatives on information protection.[44]

1.2.23 Although the detailed mechanisms of information protection in the international instruments and laws varies, all require that personal information must be:

- obtained fairly and lawfully;
- used only for the specified purpose for which it was originally obtained;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.

These principles are known as the "Principles of Information Protection" and form the basis of both legislative regulation and self-regulating control.[45]

1.2.24 In South Africa the traditional common law principles of protecting individual privacy and identity are unable to deal effectively with the new problems in this field. Apart from the Constitution itself, there is no legislation which deals specifically and fully with information protection. In view of the extent and seriousness of the threat to the individual's personality, it is surprising to find that in the South African legal system – unlike the position in many other Western legal systems – measures for the protection of the individual (information protection) have not yet been enacted.

---

43 The Meeting considered both Model Laws. The Law Ministers commended the Model law for the public sector as a useful tool which could be adopted to meet the particular constitutional and legal positions in member countries. They decided, however, that the Model Bill on the protection of personal Information needed more reflection. The Model Laws are furthermore being examined in regional workshops conducted by the Secretariat.

44 Bygrave ***Data Protection*** at 30.

45 See discussion in Chapter 4 below.

South African commentators[46] are unanimous that the creation of such measures through legislation is a matter of great urgency.[47]

1.2.25 It should be noted that the Promotion of Access to Information Act,[48] inter alia, recognises the information protection principle that personal information should be accessible to the subject. This Act, the Electronic Communications and Transactions Act[49] and the National Credit Act[50] have interim provisions dealing, respectively, with the correction of information, the voluntary adherence to information protection principles and, in the case of the National Credit Act, a limited regulatory system for credit bureaux.[51] These sections have been regarded as interim measures until specific information privacy legislation has been finalised. See the discussion below on the proposed amendments to these Acts and other South African legislation. [52]

1.2.26 Four models aimed at the protection of personal information can be identified.[53] Depending on their application, these models can be complementary or contradictory. In most countries several are used simultaneously. In the countries that protect privacy most effectively, all the models are used together to ensure information protection. The models are as follows:[54]

a) Comprehensive laws

In many countries around the world, there is a general law that governs the collection, use and dissemination of personal information by both the public and private sectors. An

---

46 ***Neethling's Law of Personality*** at 273 and the references made in fn 65. For the opposite view see Van der Merwe (ibid).

47 The idea to develop privacy legislation for South Africa is in line with international trends worldwide. The United Kingdom (Data Protection Act 1998); Canada (Privacy Act 1982 and Personal Information Protection and Electronic Documents Act, 2000), Australia (Privacy Act, 1988 and The Privacy Amendment (Private Sector) Act 2000), New Zealand (Privacy Act 1993) and most European countries have already enacted privacy legislation.

48 Act 2 of 2000, see section 88.

49 Act 25 of 2002, see sections 45, 51 and 52.

50 Act 34 of 2005.

51 See discussion on credit reporting in para 5.3 below.

52 See discussion in Chapter 5 below. Consequential amendments may furthermore be necessary in 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.

53 Exposition as set out in EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 3-5.

54 See, however, the discussion in this regard in Chapter 7 below.

oversight body then ensures compliance. This is the preferred model for most countries adopting information protecting laws and was adopted by the European Union to ensure compliance with its information protection regime. A variation of these laws, which is described as a co-regulatory model, was adopted in Australia. Under this approach, industry develops rules for the protection of privacy that are enforced by the industry and overseen by the private agency.

b) Sectoral laws

Some countries, such as the United States, have a generic act for the public sector only. They have avoided enacting general information protection rules for the private sector in favour of specific sectoral laws governing for example, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. A major drawback with this approach is that it requires that new legislation be introduced with each new technology - protection therefore frequently lags behind. The lack of legal protection for individual privacy on the Internet in the USA is a striking example of its limitations. There is also the problem of a lack of an oversight agency. In many countries, sectoral laws are used to complement comprehensive legislation by providing more detailed protection for certain categories of information, such as telecommunications, police files or consumer credit records.

c) Self-regulation

Information protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. However, in many countries, particularly the United States, these efforts have been disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries have tended to provide only weak protection and lack enforcement. Self-regulation forms a major part of the privacy protection system for the private sector in the United States and Singapore.

d) Technology

With the recent development of commercially available technology-based systems, information protection has also moved into the hands of individual data subjects. Data

subjects using the Internet and some physical applications can employ a range of programs and systems that provide varying degrees of privacy and security of communications. These include encryption, anonymous remailers, proxy servers and digital cash.[55] However, not all tools are effective in protecting information privacy. Some are poorly designed while others may be designed to facilitate law enforcement access.

1.2.27 The Commission put forward these models and other proposals for discussion and evaluation in the Issue and Discussion Paper. It was clear that the process of establishing policy had to go beyond the level of basic statutory information protection principles to include the ways in which these principles should be enforced, eg, through supervisory authorities.

1.2.28 It has been argued[56] that governments may find that proposed measures to protect privacy could meet the staunch opposition of business interests which see such safeguards as an expense and an unjustified constraint on their right to conduct their business affairs as they wish.

1.2.29 On the other hand, business interests may be enhanced by a statutory information protection regime. Many countries, especially in Asia, have developed or are currently developing information protection laws in an effort to promote electronic commerce. These countries recognise that consumers are uneasy about the increased availability of their personal information, particularly with new means of identification and forms of transactions, and therefore that their personal information is being utilised worldwide. Information privacy laws are therefore being introduced, not from a human rights perspective, but rather as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.

1.2.30 The task of balancing these opposing interests is therefore a delicate one and the main reason why the Commission's thorough consultation process is of such great importance in this investigation. [57]

---

55 EPIC maintains a list of privacy tools at http://www.epic.org/privacy/tools.htm.

56 Victorian Law Reform Commission ***Privacy Law: Options for Reform*** at 6: The USA is also debating the merits of privacy legislation and a major part of the debate concerns the costs to business. Robert Hahn, in a study supported by the Association for Competitive Technology Hahn RW "An Assessment of the Costs of the Proposed Online Privacy Legislation" May 7, 2001 argues that costs could run into billions of dollars and may be prohibitive. This report was however criticised by Peter Swire, former White House Counsellor on Privacy in Swire P " New Study Substantially Overestimates Costs of Internet Privacy Protections", 9 May 2001.

57 See the discussion on the consultation process below. The Hon Justice Michael Kirby AC CMG in a foreword to Bygrave ***Data Protection*** states that when a completely new problem comes along, the legal mind is often paralysed for a time. Attempts are made to squeeze the problem into old familiar bottles. And when this does not work, attempts are made to create new receptacles by analogy with those that seem most suitable.....Not only is the legal mind resistant to the idea of new approaches to new problems. The institutions of lawmaking are often highly inflexible. Typically, the emerging issues are complex, beyond the easy comprehension of the elected lay people who sit in the legislatures and even the overworked

(continued...)

1.2.31 Considering international trends and expectations, information privacy or data legislation[58] will ensure South Africa's future participation in the information market, if it is regarded as providing "adequate" information protection by international standards.[59]

1.2.32 Marc Rotenberg (director of Computer Professionals for Social Responsibility) commented as follows in an online forum sponsored by the *Wall Street Journal*: [60]

> There is a close tie between privacy and pluralism... This is what I suspect is at risk in the current rush to record and exchange personal data. Global Village in theory. Surveillance State in practice.

Whichever view one holds, one thing is certain "Privacy is an issue whose time has come."[61]

1.3 Terms of reference

1.3.1 The terms of reference for this investigation have been stated as follows:

a)` To investigate all aspects regarding the protection of the right to privacy of a person in relation to the processing (collection, storage, use and communication) of his, her or its personal information by the State or another person.

b) To recommend any legislative or other steps which should be taken in this regard.

1.3.2 The Commission therefore investigated all aspects regarding the protection of the right to privacy of a person with specific reference to the processing of his or her personal information by the State or other persons. For a discussion on the scope of the investigation see Chapter 3 below.

---

57 (...continued)
officials who advise them. Sometimes powerful forces of national interests or the interests of transnational corporations see advantage in delaying an effective legal response to a demonstrated problem. If nothing is done, or if any legal response is left to "soft options", the strong and the powerful can continue to do what they want. Responses reflecting community values will then play second fiddle to the tune of unregulated power.

58 Bygrave ***Data Protection*** at 1 states that the term "data protection" is most commonly used in European jurisdictions. In other jurisdictions, such as the USA, Canada and Australia, the term "privacy protection" tends to be used in stead.

59 Roos A "Data Protection Provisions in the Open Democracy Bill, 1997" 1998 (61) **THRHR** (hereafter referred to as "Roos ***THRHR***") at 499.

60 Piller ***Macworld*** at 7.

61 Bennett ***Government Foundation Paper*** at 28.

1.4 Methodology

1.4.1 In accordance with the Commission's policy to consult as widely as possible, every effort has been made in this investigation to publicise the investigation and to elicit response from interested persons and organisations as well as from members of the public. Considerable effort has furthermore gone into obtaining the inputs from all government departments, but especially from the Department of Justice's Policy Unit.

1.4.2 In September 2003 the Commission published a comprehensive Issue Paper for information and comment.[62] The publication of this Issue Paper was the first step in the consultation process. The problems that had given rise to the investigation were explained and possible options for solving these problems were pointed out. A copy of the Issue Paper was also made available on the Commission's website.

1.4.3 Written comment was received from 34 persons and institutions.[63] Numerous follow-up discussions, meetings and presentations furthermore resulted from this publication. [64]

1.4.4 A Discussion Paper with draft legislation was subsequently published in October 2005 for general information and comment.[65] In this paper the preliminary proposals of the Commission were set out and options for reform identified. The way in which information privacy was regulated in other countries was furthermore discussed.

1.4.5 During March and April 2006 the Commission held regional workshops countrywide where members of the Project Committee were present to explain and discuss the proposed options for law reform and to note comments. The closing date for comments to the Discussion Paper was extended (on public request) from 28 February 2006 to 30 September 2006. A total of 63 written submissions were received.[66]

---

62 South African Law Reform Commission ***Privacy and Data Protection*** Project 124 Issue Paper 24 September 2003 (hereafter referred to as "Issue Paper 24") available at http://www.doj.gov.za/salrc/index.htm.

63 A list of respondents is enclosed as Annexure A.

64 See eg. meetings with the Department of Justice and Constitutional Development; Department of Trade and Industry; SAFPS; Credit Bureau Association; Trans Union; NEDLAC.

65 SA Law Reform Commission ***Privacy and Data Protection*** *Project 124* Discussion Paper 109 October 2005 (hereafter referred to as "Discussion Paper 109") available at http://www.doj.gov.za/salrc/index.htm.

66 A list of respondents to Discussion Paper 109 is enclosed as Annexure B.

1.4.6 The respondents to the Discussion Paper seemed to be overwhelmingly in favour of the proposed legislation. Comments were mostly submitted on points of detail only.[67]

1.4.7 Many submissions contained constructive criticism and helpful suggestions to improve the proposals of the Commission. The Commission duly considered each contribution and incorporated the ideas put forward in this report where appropriate. The Commission would like to take this opportunity to thank all who responded to the Issue and Discussion papers.

1.4.8 In this report the right to privacy is discussed with particular reference to the protection of personal information (Chapter 2). This is followed by an overview of the purpose and scope of the Protection of Personal Information Bill (Chapter 3), the Information Protection Principles to be incorporated in the Bill (Chapter 4) and the rights of data subjects in specific circumstances (Chapter 5). Thereafter the problems with cross-border information transfers are discussed (Chapter 6), monitoring, supervision (Chapter 7) and enforcement (Chapter 8) of the legislation are set out and a comparative study of the legal position regarding the protection of information in other jurisdictions is provided (Chapter 9). In each case the position as set out in the Discussion Paper is stated, followed by an overview and evaluation of the submissions received on the Discussion Paper and, in conclusion, the recommendations of the Commission.

67 See the discussion in this regard in Chapter 2 below.

CHAPTER 2: RIGHT TO PRIVACY

2.1 Recognition of the right to privacy

2.1.1 Privacy is a valuable and advanced aspect of personality. Sociologists and psychologists agree that a person has a fundamental need for privacy.[1] Privacy is also at the core of our democratic values.[2] An individual therefore has an interest in the protection of his or her privacy.

2.1.2 Although privacy concerns are deeply rooted in history,[3] privacy protection as a public policy question can be regarded as a comparatively modern notion. The right to privacy has, however, become one of the most important human rights of the modern age and is today recognised around the world in diverse regions and cultures.[4]

2.1.3 The modern privacy benchmark at an international level can be found in the 1948 Universal

---

1 ***Neethling's Law of Personality*** at 29.

2 Preserving privacy fosters individual autonomy, dignity, self-determination, and ultimately promotes a more robust, participatory citizenry. A watched society is a conformist society. Unwanted exposure may lead to discrimination, loss of benefits, loss of intimacy, stigma, and embarrassment: see Goldman J "Health at the Heart of Files?" Brandeis Lecture delivered at the Massachusettes Health Data Consortium's Annual Meeting and made available at the 23rd International Conference of Data Protection Commissioners in Paris in 24-26 September 2001 (hereafter referred to as "Goldman") at 2. See also the discussion in Kang J "Information Privacy in Cyberspace Transactions" 50 ***Stanford Law Review*** April 1998 1193 at 1212-20 where the counter values against control over personal information are described as commerce (better information leads to better markets) and truthfulness (privacy can be used to deceive and defraud). In so far as the second value is concerned it should however be noted that the conscious concealment of personal information does not always amount to lying: the hallowed example is the secret ballot.

3 See ***Neethling's Law of Personality*** at 42,45,46 for the position in Roman and Roman-Dutch law; EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 5 refers to the recognition of privacy in various religions: the Qur'an an-Noor (24:27-28 (Yusufali); al-Hujraat 49:11-12 (Yusufali**)** and in the sayings of Mohammed (Volume 1, Book 10, Number 509 (Sahih Bukhari); Book 020, Number 4727 (Sahih Muslim); Book 31, Number 4003 (Sunan Abu Dawud). The Bible has numerous references to privacy. Jewish law has long recognised the concept of being free from being watched. See reference to Rosen J ***The Unwanted Gaze*** Random House 2000. Privacy was also protected in Classical Greece and ancient China.

4 In many countries privacy is now protected by constitutional guarantees or general human rights legislation: Examples of countries that recognise a right to privacy in their Constitution, other than South Africa (section 14 of the Constitution**)**, are eg the Kingdom of the Netherlands (Constitution of the Kingdom of the Netherlands, 1989), Republic of the Philippines (art III, Constitution of the Republic of the Philipines, 1987), Russian Federation (art 23, Constitution of the Russian Federation,1993). While the Constitution of the United States of America does not contain an explicit right to privacy, the Courts in that country, going back as far as 1891 (***Union Pacific R.R Co v Botsford***, 141 US 251 11 S.Ct 1000, 35 L.Ed 734(1891) have interpreted the Constitution as providing a right to personal privacy. The UK has recently enacted general human rights legislation that protects the right to privacy in their Human Rights Act, 1998 (UK).

Declaration of Human Rights,[5] which specifically protects territorial and communications privacy.[6]

2.1.4 The right to privacy is also dealt with in various other international instruments,[7] such as the United Nations Convention on the Rights of the Child,[8] the International Covenant on Civil and Political Rights (ICCPR),[9] and the United Nations Convention on Migrant Workers.[10]

2.1.5 At regional level, a number of treaties make this recognition of the right to privacy legally enforceable.

a) Article 8 of the European Convention for the Protection of Human Rights and

---

5 Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948.

6 Art 12 of the United Nations Universal Declaration of Human Rights, 1948 provides:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

According to Burchell JM ***Personality Rights and Freedom of Expression: The Modern Actio Injuriarum*** Juta Cape Town 1998 (hereinafter referred to as "Burchell ***Personality Rights***") at 371, the word 'arbitrary' points towards some acceptance that certain invasions of privacy may be regarded as reasonable and others as unreasonable. In fact, the Universal Declaration recognises limits to the exercise of rights. These limits are defined as those 'determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society' (art 29).

7 See generally Rotenberg M (ed) ***The Privacy Law Sourcebook: United States Law, International Law and Recent Developments*** EPIC 2001.

8 United Nations Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990. Art 16 of the United Nations Convention on the Rights of the Child, 1989 provides:

> 1. No child shall be subject to arbitrary or unlawful interference with his or her privacy, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
>
> 2. The child has the right to the protection of the law against such interference or attacks.

9 International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976. Art 17 provides as follows:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> (2) Everyone has the right to the protection of the law against such interference or attacks.

10 Art 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution 45/158 of December 18, 1990.

Fundamental Freedoms 1950 [11] states:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

b) The American Convention on Human Rights[12] (Art 11,14) and the American Declaration on Rights and Duties of Mankind[13] (Art V,IX and X) contain provisions similar to those in the Universal Declaration and International Covenant.

It is, however, interesting to note that the African [Banjul] Charter on Human and People's Rights[14] does not make any reference to privacy rights.[15]

2.1.6 The European Convention furthermore created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been active in the enforcement of the right to privacy and have consistently viewed Article 8's protection expansively and interpreted the restrictions narrowly.[16]

---

11 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005) open for signature November 4, 1950, entry into force September 3, 1950.

12 Pact of San Jose, Costa Rica 22 November 1969 entered into force on 18 July 1978.

13 Approved by the Ninth International Conference of American States, Bogota, Columbia, 1948.

14 Adopted June 27 1981 OAU Doc. CAB/LEG/67/3 rev.5,21 I.L.M. 58 (1982) entered into force Oct 21 1986.

15 Gutwirth S (translation by Casert R) ***Privacy and the Information Age*** Rowman & Littlefield Publishers Lanham 2002 suggests that in the African context "the solution to individual conflicts is subordinate to safeguarding the stability of the social context". The status of the individual is limited. Everyone is expected to be part of different, strictly hierarchical communities. It is with the development of industrialisation on a wide scale, that the concept of privacy develops.

16 Strossen N "Recent United States and International Judicial Protection of Individual Rights: A Comparative Legal Process Analysis and Proposed Synthesis " 41 ***Hastings Law Journal*** 805 (1990) as referred to in EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 7 and the references made therein.

2.1.7 In South Africa the right to privacy is protected by both our common law[17] and the Constitution.[18] The Constitutional Court[19] has emphasised the interdependency between the common law and constitutional right to privacy. A fundamental issue at stake, however, concerns the extent to which the Bill of Rights has application in common law disputes.

2.1.8 The Constitution is the supreme law of South Africa and any law or conduct inconsistent with it is invalid (section 2). Certain fundamental rights - to which juristic persons are also entitled to the extent required by the nature of the right and the nature of a particular juristic person(section 8(4)) - are entrenched in Chapter 2 (the Bill of Rights). The Bill is applicable to all law - therefore also the common law relating to the right to privacy - and binds not only the State (section 8(1)) but also, if applicable, natural and juristic persons (section 8(2)). This vertical and horizontal application of the Bill can take place directly or indirectly.[20]

2.1.9 Direct vertical application means that the State must respect (or may not infringe) the fundamental rights except in so far as such infringement is reasonable and justifiable in terms of the limitation clause (section 36(1)). Direct horizontal application connotes that the courts must give effect to applicable fundamental rights by applying and developing the common law to the extent that legislation fails to do so, except where it is reasonable and justifiable to develop the common law to limit the relevant right(s) in accordance with the limitation clause (sections 8(3) and 36(1)).[21]

2.1.10 The indirect application of the Bill of Rights means that all legal rules, principles or norms - including those regulating the law relating to the right to privacy - are subject to and must thus be given content in the light of the basic values of the Bill. In this regard the courts have an obligation to develop the common law in accordance with the spirit, objects and purport of the Bill of Rights

---

17 See ***Neethling's Law of Personality*** Chapter 8.

18 See discussion below.

19 ***Bernstein ao v Bester ao NNO*** 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC) at 787 ff.

20 See Neethling J, Potgieter JM & Visser PJ ***Law of Delict*** Butterworths Durban 2006 (hereafter referred to as "Neethling, Potgieter & Visser ***Delict***") at 16; ***Neethling's Law of Personailty*** at 73-74; Cockrell A "Private Law and the Bill of Rights: A Threshold Issue of "Horizontality"" ***Bill of Rights Compendium*** Butterworths Constitutional Law Library (hereafter referred to as "Cockrell ***Bill of Rights Compendium***") at paras 3A4-3A10.9.

21 A court may therefore be required to consider whether infringement of a fundamental right by a common law rule which serves to protect another right can be justified in terms of the general limitation clause (Cameron J in ***Holomisa v Argus Newspapers Ltd*** 1996 (2) SA 588 (W) at 606-607).

(section 39(2)).[22]

2.1.11 The entrenchment of fundamental rights (also the right to privacy) strengthens their protection and gives them a higher status in the sense that they are applicable to all law, and are binding on the executive, the judiciary and state organs as well as on natural and juristic persons. Any legal rule or actions by the state or a person may thus be tested with reference to an entrenched right, and any limitation of such a right may occur only if it corresponds with the limitation clause of the Bill of Rights. In the case of an infringement or threat to a fundamental right, the aggrieved or threatened person is entitled to apply to a competent court for appropriate relief, which may include a declaration of rights. For example, a statutory provision limiting the right to privacy in an unreasonable manner may be set aside or interpreted in a restrictive manner.[23]

2.1.12 In the ***Pharmaceutical Manufacturers Association*** case[24] Chaskalson P stated that

> the common law relating to the control of public power supplements the provisions of the written Constitution but derives its force from it.... There is, however, only one system of law and within that system the Constitution is the supreme law with which all other law must comply.

2.1.13 Neethling, Potgieter and Visser[25] argue that in so far as the direct application of the Constitution is concerned, a distinction should, however, be made between a constitutional

---

22 See ***Carmichele v Minister of Safety and Security ao (Centre for Applied Legal Studies Intervening)*** 2001 (4) SA 938 (CC) at 950-956. Section 39 of the Constitution reads as follows:

Interpretation of Bill of Rights

39.(1) When interpreting the Bill of Rights, a court, tribunal or forum -

(a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom;
(b) must consider international law; and
(c) may consider foreign law.

(2) When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.

(3) The Bill of Rights does not deny the existence of any other rights or freedoms that are recognised or conferred by common law, customary law or legislation, to the extent that they are consistent with the Bill.

23 Neethling, Potgieter & Visser ***Delict*** at 18; ***Neethling's Law of Personality*** at 75.

24 ***Pharmaceutical Manufacturers Association of South Africa ao : In re Ex parte President of the Republic of South Africa ao*** 2000 (2) SA 674 (CC) at 698.

25 Neethling, Potgieter & Visser ***Delict*** at 19.

infringement and a delict.[26] Constitutional remedies are concerned with the acknowledgment and enforcement of fundamental rights whereas a delict is primarily aimed at the recovery of damages. But the two may overlap. In so far as indirect application is concerned, the basic values of the Constitution will always play an important role in determining wrongfulness, causality and negligence in common law disputes. The courts will therefore retain those existing common law actions which are in harmony with the values of the Constitution.[27] Burchell[28] submits that the common law of privacy in South Africa will still provide the lion's share.

2.1.14 In ***Bernstein ao v Bester NO ao***,[29] in deciding whether sections 417 and 418 of the Companies Act[30] infringe section 13 of the interim Constitution, Ackermann J warned that caution must be exercised when attempting to project common-law principles onto the interpretation of fundamental rights and their limitation.[31] He drew a distinction between the two-stage constitutional inquiry into whether a right has been infringed and whether the infringement is justified, and the single inquiry under the common law, as to whether an unlawful infringement of a right has taken place.[32]

2.1.15 There is no South African legislation dealing specifically with the protection of the right to

---

26 McQuoid-Mason DJ "Invasion of Privacy: Common Law v Constitutional Delict - Does it Make a Difference?" ***Acta Juridica*** 2000 at 227(herefter referred to as "McQuoid-Mason ***Acta Juridica***") poses the question whether a breach of a constitutional right to privacy gives rise to a constitutional delict. He furthermore discusses the possibility of creating a new constitutional delict of invasion of privacy.

27 McQuoid-Mason DJ "Privacy" in Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D & Woolman S (eds) ***Constitutional Law of South Africa*** Juta Kenwyn 1996 Revision Service 5 1999 (hereafter referred to as "McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa***") at 18—2.

28 Burchell JM "Media Freedom of Expression Scores as Strict Liability Receives the Red Card: National Media Ltd v Bogoshi" 1999 ***SALJ*** 1 (hereafter referred to as "Burchell ***SALJ)*** at 16.

29 Supra at 790. See also McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18 —1; Burchell ***Personality Rights*** at 373.

30 Act 61 of 1973.

31 Burchell ***Personality Rights*** at 384, quoting ***Bernstein v Bester*** supra.

32 It should nevertheless be noted that, dogmatically at least, at common law a distinction is also made between a prima facie invasion of the right to privacy and the justification of such invasion (see ***Neethling's Law of Personality*** at 221ff, 240ff).

privacy.[33] It is therefore important to evaluate the right to privacy in the light of both the common law and the Constitution.[34]

2.1.16 In terms of the common law every person has personality rights such as the rights to physical integrity, freedom, reputation, dignity, identity and privacy.[35]

2.1.17 The locus classicus for the recognition of an independent right to privacy in South African law is considered to be ***O'Keeffe v Argus Printing and Publishing Co Ltd ao.***[36]

2.1.18 In this case Watermeyer AJ correctly interpreted[37] dignitas so widely as to include the whole legally protected personality except corpus (bodily integrity) and fama (reputation). As such dignitas includes not only a single right of personality, but all "those rights relating to . . . dignity". Although it was not explicitly stated by the court, the judgment leaves one in no doubt that the right to privacy is included as one of these "rights".[38]

---

33 Note, however, that the Promotion of Access to Information Act 2 of 2000 (hereafter referred to as "PAIA") provides access on request to his or her personal data to the data subject. This Act, the ECT Act and the National Credit Act also have interim provisions dealing with the correction of data and the voluntary adherence to data protection principles, respectively. These sections are being regarded as interim measures until the Protection of Personal Information Bill has been finalised. It should be noted that the promulgation of data protection legislation in South Africa will necessarily result in amendments to these and other South African legislation. Section 33 of the SA Reserve Bank Act 90 of 1989 furthermore forbids the disclosure of information about customers or shareholders unless this is required for the performance of statutory duties or in court proceedings; Section 10 of the Local Government: Municipal Structures Act 117 of 1998 prohibits a councillor from disclosing information that would violate a person's privacy. Legislative provisions of this kind are, unfortunately, uncommon.

34 The position regarding the relationship between the Constitution and the common law of privacy as set out above was in general confirmed by the respondents to Issue Paper 24. See the submissions received from the Banking Council, Eskom Legal Department, Strata, the Financial Services Board and Andrew Rens.

35 See ***Neethling's Law of Personality*** at Chapter 3; ***Grutter v Lombard*** 2007 (4) SA 89 (SCA) as to the right to identity.

36 1954 (3) SA 244 (C); McKerron RG ***The Law of Delict*** Juta Cape Town 1971 at 54 states: "The case goes further than any previous case in recognising the existence of a right to privacy in South African law." This decision was cited with approval in ***Prinsloo ao v SA Associated Newspapers Ltd ao*** 1959 (2) SA 693 (W) at 695-696; ***Gosschalk v Rossouw*** 1966 (2) SA 476 (C) at 490; ***Mr and Mrs "X" v Rhodesia Printing and Publishing Co Ltd*** 1974 (4) SA 508 (R) at 511-512 (confirmed in ***Rhodesian Printing and Publishing Co Ltd v Duggan*** 1975 (1) SA 590 (RA) at 592). For discussions of the ***O'Keeffe*** case see eg ***Neethling's Law of Personality*** at 50-1,217; Joubert WA "Die Persoonlikheidsreg: 'n Belangwekkende Ontwikkeling in die Jongste Regspraak in Duitsland" 1960 ***THRHR*** (hereafter referred to as "Joubert 1960 ***THRHR***") *at* 26-27, 39 ff; Van der Merwe NJ and Olivier PJJ ***Die Onregmatige Daad in die Suid-Afrikaanse Reg*** Van der Walt Pretoria 1989 (hereafter referred to as "Van der Merwe and Olivier") at 449; McQuoid-Mason DJ ***The Law of Privacy in South Africa*** Juta Johannesburg 1978 (hereafter referred to as "McQuoid-Mason ***Law of Privacy***") at 89-90. Here a photograph of an unmarried woman was published without her consent as part of an advertisement for rifles, pistols and ammunition. She instituted an action on the ground that the publication infringed her right to privacy.

37 Various writers agreed: ***Neethling's Law of Personality*** at 50-1,217; cf also McQuoid-Mason ***Law of Privacy*** at 124-125.

38 This conclusion was also reached in ***Gosschalk v Rossouw*** supra at 490-491. Corbett J stated with reference to ***O'Keeffe***: "The rights relating to dignity include, it would seem . . . a qualified right to privacy." Cf also ***Mr and Mrs "X" v Rhodesia Printing and Publishing Co Ltd*** supra at 512; ***Sage Holdings Ltd ao v Financial Mail (Pty) Ltd ao*** 1991 (2) SA 117(W)

2.1.19 Very important is the fact that the court, in following ***Foulds v Smith***,[39] correctly rejected the view that contumelia in the sense of "insult" is the "essence of an injuria".[40]

2.1.20 The view that privacy is an independent right was, however, not always held. In a number of early South African criminal cases regarding the protection of privacy,[41] the idea that dignitas, and consequently privacy, should be limited to dignity and accordingly that insult forms an element of this iniuria, was stated. Even private law decisions after the ***O'Keeffe*** case took a similar approach to the recognition of a right to privacy.[42]

---

at 128-131; ***S v Bailey*** 1981 (4) SA 187 (N) at 189; cf however Joubert 1960 ***THRHR*** at 40. In ***Mr and Mrs "X" v Rhodesia Printing and Publishing Co Ltd*** supra at 513, Davies J simply stated: "It is clear that there is a qualified right to privacy." In this decision (512) the definition of privacy, as deduced from para 867 of the American ***Restatement of the Law*** was accepted. Privacy is, namely, a person's "interest in not having his affairs known to others or his likeness exhibited to the public . . ."

39 1950 (1) SA 1 (A) at 11; see also ***Neethling's Law of Personality*** at 50,217.

40 ***Neethling's Law of Personality*** at 217 fn 9 however expresses criticism against the ***O'Keeffe*** decision, in that it lacks a comprehensive definition of the right to privacy. As a result, identity as a personality interest is equated with privacy. Instances of unauthorised use of indicia of identity for advertising purposes primarily involve violation of identity and not privacy (see discussion on the distinction between identity and privacybelow).

41 ***Neethling's Law of Personality*** at 218 refers in this regard to the decision in ***S v A ao*** 1971 (2) SA 293 (T) as an example. This case concerned the wrongful monitoring of a private conversation. At first glance it would also appear to recognise the independent existence of a right to privacy. Botha AJ accepted, as did the judge in the ***O'Keeffe*** case, that an iniuria is constituted by the wrongful, intentional infringement of the person, dignity or reputation of another person. Similarly, the interpretation accorded to dignity by the judge was so wide that it encompassed all those aspects of personality accorded legal protection except the person and reputation. Consequently he concluded that "the right to privacy is included in the concept of *dignitas*" and that "there can be no doubt that a person's right to privacy is one of . . . 'those real rights, those rights *in rem*, related to personality, which every free man is entitled to enjoy'". Thus, on the face of it, an unequivocal recognition of the right to privacy as an independent personality right. Unfortunately, Botha AJ muddled his approach somewhat when he came to the requirement of intent. He demanded not only the intent to infringe the plaintiff's privacy, but also the "intention to impair the complainant's dignity". He found this intent in the form of dolus eventualis: "They must have foreseen the possibility that the complainant could or would be hurt and *insulted* by their conduct, but they acted in reckless disregard of his feelings." Contrary to his view expressed above, Botha AJ hereby restricted dignitas to dignity or honour as a personality interest and negated the independent existence of a right to privacy. If privacy, as such, had been accorded protection, there is not the slightest doubt that the accused had intent in the form of dolus directus to violate privacy. See also ***R v Holliday*** 1927 CPD 395 (Van der Merwe and Olivier at 449) where the plaintiff was spied upon while she was busy undressing. Gardiner J regarded the concept of privacy as implicit in the concept of dignitas. He stated (400): "It is the violation of a man's rights of personality . . . which gives rise to an action of injury. Now among the rights of personality to which under our civilization a woman is entitled, is the right to privacy in regard to her body." The judge, however, equated dignitas with "self-respect" and consequently demanded an "intention to do the insulting act" to found a conviction. (A similar viewpoint appeared from ***R v S*** 1955 (3) SA 313 (SWA) at 315; ***R v R*** 1954 (2) SA 134 (N) at 135.) Thus the right to privacy is protected only in so far as an intention to insult is present. The above decisions probably follow ***R v Umfaan*** 1908 TS 62 where the court clearly stated that dignitas can be infringed only if an element of "degradation, insult or *contumelia*" is present.

42 Eg, in ***Kidson ao v SA Associated Newspapers Ltd*** 1957 (3) SA 461 (W) (see also ***Mhlongo v Bailey*** 1958 (1) SA 370 (W) at 372), which concerned the wrongful publication of a photograph of nurses, Kuper J, following ***Walker v Van Wezel*** 1940 WLD 66, stated clearly, with regard to the iniuria pertinens ad dignitatem, that "a remedy should be given only when the words or conduct complained of involve an element of degradation, insult or *contumelia*" (at 467).

2.1.21 It has, however, been argued[43] that the equation of privacy and dignity should be rejected and that the approach in ***O'Keeffe*** should be endorsed.[44] Many recent cases (also of the Appeal Court) have by implication followed this approach. [45] Even the Constitutional Court in ***Bernstein ao v Bester NO ao*** [46] accepted the fact that the common law recognises the right to privacy as an independent personality right which the Courts have included within the concept of dignitas.

2.1.22 The conclusion is therefore that, despite the decisions equating privacy with dignity (or honour), it can safely be accepted that nowadays the right to privacy is recognised by the common law as an independent right of personality[47] and that it has been delimited as such within the dignitas concept.[48]

2.1.23 The enactment of the Constitution,[49] with the express constitutional recognition of the right to privacy in section 14, independent of the right to dignity in section 10,[50] furthermore confirms the

---

43 See ***Neethling's Law of Personality*** at 51, 217-8; Joubert 1960 ***THRHR*** at 41.

44 Joubert already stated this in 1960: see Joubert ***op cit*** at 41-42.

45 See ***Jansen van Vuuren ao NNO v Kruger*** 1993 (4) SA 842 (A) at 849 ; ***National Media Ltd ao v Jooste*** supra at 271-272; ***Financial Mail (Pty) Ltd v Sage Holdings Ltd*** ao1993 (2) SA 451 (A); ***Motor Industry Fund Administrators (Pty) Ltd ao v Janit ao*** 1994 (3) SA 56 (W) (confirmed on appeal: 1995 (4) SA 293 (A)). These cases recognise the right to privacy of both natural and juristic persons (see ***Neethling's Law of Personality*** at 219). Andrew Rens also referred the Commission to ***Khumalo ao v Holomisa*** 2002 (5) SA 401 (CC); 2002 (8) BCLR 771 (CC) where it states:
It should also be noted that there is a close link between human dignity and privacy in our constitutional order. The right to privacy , entrenched in section 14 of the Constitution, recognises that human beings have a right to a sphere of intimacy and autonomy that should be protected from invasion. This right serves to foster human dignity. No sharp lines can be drawn between reputation, dignitas and privacy in giving effect to the value of human dignity in our Constitution. See, however, ***Neethling's Law of Personality*** 28 fn 299, 219 fn 28.

46 Supra at 789.

47 The decision in ***Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk*** 1977 (4) SA 376 (T) clearly confirmed this viewpoint. Mostert J stated (at 383-384): "Die reg op privaatheid is een van die verskyningsvorms van die breër groep persoonlikheidsregte. In ons regspraak is erkenning aan sowel persoonlikheidsregte as die reg op privaatheid as beskermde regte verleen." See again also ***Jooste v National Media Ltd ao***1994 (2) SA 634 (C); ***Financial Mail (Pty) Ltd v Sage Holdings Ltd*** supra; ***Motor Industry Fund Administrators (Pty) Ltd ao v Janit ao*** supra. Cf further the ***Tommie Meyer*** Appellate Division case 1979 (1) SA 441 (A) at 455 ff ; ***Sage Holdings Ltd ao v Financial Mail (Pty) Ltd ao*** supra at 129-131; ***Boka Enterprises (Pvt) Ltd v Manatse ao NO*** 1990 (3) SA 626 (ZH) at 632; ***Nell v Nell*** 1990 (3) SA 889 (T) at 895 896; cf nevertheless McQuoid-Mason at 125-128.

48 In ***Jansen Van Vuuren ao NNO v Kruger*** supra at 849 Harms AJA explained it thus: "The *actio iniuriarum* protects a person's *dignitas* and *dignitas* embraces privacy . . . Although the right to privacy has on occasion been referred to as a real right or *ius in rem* . . . it is better described as a right of personality."

49 Section 2 of the Constitution states that the Constitution is the supreme law of the Republic, that any law or conduct inconsistent with it is invalid, and that the obligations imposed by it must be fulfilled.

50 Section 10 of the Constitution states:
Everyone has inherent dignity and the right to have their dignity respected and protected.

independent existence of the right to privacy.[51] It hopefully finally lays to rest the possible equation of, and thus confusion between, these two personality rights.[52] Because the South African Constitution protects the right to privacy as a separate right, the conduct and interests so protected may furthermore be distinguished more effectively than in systems where the right is inferred from other rights.[53]

2.1.24 The right to privacy should, furthermore, be distinguished from the right to identity. Identity as an interest of personality can be defined as a person's uniqueness or individuality which identifies or individualises him as a particular person and thus distinguishes him from others.

2.1.25 Identity is manifested in various characteristics by which that particular person can be recognised; in other words, facets of his personality which are unique to him, such as his life history, his character, his name, his creditworthiness, his voice, his handwriting, his appearance (physical image), etcetera.

2.126 A person has a definite interest in the uniqueness of his being and conduct being respected by outsiders. Therefore, a person's identity is infringed if any of these characteristics are used without authorisation in ways which cannot be reconciled with his true image.[54] Seen in this light, the processing of incorrect or misleading personal information poses a threat to an individual's identity because the information is used in a manner which is not in accordance with his true personality image.[55]

2.1.27 In ***Grutter ao v Lombard***[56] Nugent JA referred to the above description of identity with approval and recognised the right to identity as a separate personality right. The protection of the right to identity is, however, not unlimited. The wrongfulness of an infringement of identity must be

---

51 As indicated (supra fn 40), the right to privacy is protected in South African law with reference to natural persons as well as to juristic persons.

52 See ***Neethling's Law of Personality*** at 219 fn 28.

53 Rautenbach IM "The Conduct and Interests Protected by the Right to Privacy in Section 14 of the Constitution" **TSAR** 2001.1,115 (hereafter referred to as "Rautenbach 2001 ***TSAR***") at 122.

54 See ***Neethling's Law of Personality*** at 36.

55 See idem 271.

56 Supra at 93,95.

assessed with reference to the basic test for wrongfulness, namely that the factual infringement of identity (that is, where the use of a characteristic of identity is contrary to the true image of the victim) must be in conflict with the legal convictions of the community (contra bonos mores). It stands to reason that the processing (collection, storage, use and disclosure) of false or misleading information is contra bonos mores and therefore constitutes a wrongful violation of identity.[57] Although considerations of legal policy may justify an infringement of identity,[58] it is highly unlikely that the processing of false or misleading information will ever be justified.[59]

2.1.28 There will, therefore, be instances where the right to identity will also be protected in terms of the Bill. However, it should be noted that privacy is also threatened by the processing of true personal information and not only by the processing of false or misleading data as is the case when identity is endangered. [60]

2.1.29 It could even be argued that the entrenchment of the right to privacy in section 14 now compels the Government to initiate steps to protect neglected aspects of the right to privacy in South Africa, such as data privacy or the protection of personal information. Section 7(2) of the Constitution provides that the state must respect, protect, promote and fulfil the rights in the Bill of Rights.[61]

2.2 Nature and scope of the right to privacy

2.2.1 Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define.[62] Definitions of privacy vary widely according to context and environment.[63] In ***Bernstein***

---

57 See ***Neethling's Law of Personality*** at 258, 275.

58 ***Grutter ao v Lombard*** supra at 96.

59 See ***Neethling's Law of Personality*** at 275.

60 Neethling J "The Concept of Privacy in South African Law" 2005 ***SALJ*** 18 at 24.

61 See ***Neethling's Law of Personality*** at 271-272; Neethling J "Aanspreeklikheid vir 'Nuwe' Risikos: Moontlikhede en Beperkinge van die Suid-Afrikaanse Deliktereg" 2002 65 ***THRHR*** (hereafter referred to as "Neethling 2002 ***THRHR***") at 589.

62 EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 2: The Calcutt Committee in the United Kingdom said that "nowhere have we found a wholly satisfactory statutory definition of privacy". But the Committee was satisfied that it would be possible to define it legally and adopted this definition in its first report on privacy: "The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication

ao v Bester NO ao [64] Ackermann J stated:

> The concept of privacy is an amorphous and elusive one which has been the subject of much scholarly debate.

2.2.2 The lack of a single definition should, however, not imply that the issue lacks importance. The need to understand the nature of the right to privacy in order to have legal certainty and protection has always been emphasised. Gross[65] warns that a lack of understanding could have the following effect:

> [O]ur ability to articulate and apply principles of legal protection diminishes, for we become uncertain what it is that compels us towards protective measures and wherein it [privacy] differs from what has already been recognised or refused recognition under established legal theory.

2.2.3 In 1996 Harms JA accepted the following definition of privacy (as proposed by Neethling[66]) in ***National Media Ltd ao v Jooste***[67]

> Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private[68] (translation from the Afrikaans).

The Constitutional Court has referred with approval to Neethling's definition on two occasions in

---

of information" ***Report of the Committee on Privacy and Related Matters*** Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO at 7.

63 EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 2: In the 1890s, future United states Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone". Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution (Samuel Warren and Louis Brandeis "The Right to Privacy" 4 ***Harvard Law Review*** at 193-220 (1890).

64 Supra at 787-788.

65 "The Concept of Privacy" 1967 ***NYULR*** at 34 as referred to by Neethling J "Die Reg op Privaatheid en die Konstitusionele Hof: Die Noodsaaklikheid vir Duidelike Begripsvorming" 1997 60 ***THRHR*** at 137.

66 See Neethling J ***Die Reg op Privaatheid*** LLD thesis UNISA 1976 (hereafter referred to as "Neethling ***Privaatheid***") at 287; ***Neethling's Law of Personality*** at 32.

67 Supra at 271.

68 This definition was also accepted in ***Jooste v National Media Ltd*** supra at 645; ***Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk*** supra at 384; ***Swanepoel v Minister van Veiligheid en Sekuriteit*** 1999 (4) SA 549 (T) at 553; see also ***Motor Industry Fund Administrators (Pty) Ltd ao v Janit ao*** supra at 60; ***Financial Mail (Pty) Ltd ao v Sage Holdings Ltd ao*** supra at 462.

Bernstein ao v Bester NO ao[69] in 1996 and in ***NM ao v Smith ao***[70] in 2007.

2.2.4 Important to note is that, in accordance with this definition a legal subject personally determines the private nature of facts. In addition, he must exhibit the will or desire that facts should be kept private.[71] If such a will for privacy is absent, then a person usually has no interest in the legal protection of his privacy.[72]

2.2.5 As stated above the right to privacy has also now been entrenched in Section 14 of the Bill of Rights in the Constitution. Section 14 reads:

> Everyone has the right to privacy, which includes the right not to have –
> (a) their person or home searched;
> (b) their property searched;
> (c) their possessions seized; or
> (d) the privacy of their communications infringed.

2.2.6 Section 14 has two parts. The first guarantees a general right to privacy. The second protects against specific infringements of privacy, namely searches and seizures and infringements of the privacy of communications.[73]

2.2.7 In ***Mistry v Interim Medical and Dental Council of South Africa ao***[74] the court assumed that even though breach of informational privacy was not expressly mentioned in section 13 of the interim Constitution (the forerunner of section 14 of the current Constitution), it would be covered

---

69 Supra at 789.

70 2007(7) BCLR 751 (CC) at para [34].

71 ***Neethling's Law of Personality*** at 31. See also the discussion by Rautenbach 2001***TSAR*** at 116: This definition need not necessarily be determinative of the constitutional meaning of the concept of privacy. The context in which it was formulated may turn out to be different from that of a bill of rights and such difference may require adjustments.

72 See ***National Media Ltd ao v Jooste*** supra at 271. Rautenbach 2001***TSAR*** at 118 states that there should be a subjective expectation of privacy which must be objectively reasonable, which means that the right is delimited by the "rights of the community as a whole (including its members)". He argues that it may be better to determine the protective ambit of the right to privacy objectively and to accommodate the subjective intentions of those who do not care about their privacy in terms of a waiver of the right.

73 De Waal J, Currie I & Erasmus G ***The Bill of Rights Handbook*** 3ed Juta Kenwyn 2000 (hereinafter referred to as "De Waal et al ***Bill of Rights Handbook*** 2000") at 267: Usually the two parts are dealt with in separate sections of bills of rights. In South Africa, however, the specific areas of protection form part of the general right to privacy.

74 1998 (4) SA 1127(CC); 1998 (7) BCLR 880 (CC) at para 14.

by the broad protection of the right to privacy guaranteed by section 13.

2.2.8 The list mentioned in section 14 is therefore not exhaustive. It extends to any other unlawful method of obtaining information or making unauthorised disclosures (eg the unlawful restoration of computer information which has been erased by its owner, and handing it over to the state for use in a criminal prosecution).[75]

2.2.9 Section 14 will, however, not only have an impact on the development of the common law action for invasion of privacy. It may also create a new constitutional right to privacy. In giving content to the general substantive right to privacy, courts will, in the first instance, be guided by common law precedents. Secondly, they will be influenced by international and foreign jurisprudence.

2.2.10 Recognition of new areas of the right to privacy may also give rise to new actions for invasion of privacy which will include not only the interests protected by the common law but also a number of important personal interests as against the state.

2.2.11 For convenience the constitutional right to privacy can be divided into three[76] groups:[77]

(a) protecting privacy against intrusions and interferences with private life;
(b) protecting privacy against disclosures of private facts; and
(c) protecting privacy against infringement of autonomy.

---

75 In ***Klein v Attorney-General, Witwatersrand Local Division*** *ao*1995 (3) SA 848 (W) at 865; 1995 (2) SACR 210 (W) this conduct was held to be a violation of the applicant's right to privacy comprehended by section 13 of the interim Constitution.

76 See also De Waal et al ***Bill of Rights Handbook*** at 270 who identify three related concerns which the right to privacy seeks to protect namely:
a) the right to be left alone;
b) the right to development of the individual personality; and
c) informational privacy.

77 McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18---8. In ***Financial Mail (Pty) Ltd ao v Sage Holdings Ltd ao*** supra at 462 and ***Motor Industry Fund Administrators (Pty) Ltd ao v Janit ao*** supra at 60 the court held that an invasion of the right to privacy may take two forms: (i) the unlawful intrusion upon the privacy of another; and (ii) the unlawful publication of private facts about a person. See also ***Bernstein ao v Bester NO ao*** supra at 789; ***Neethling's Law of Personality*** at 32-33; McQuoid-Mason ***Law of Privacy*** at 99, McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18—1, 18—8. See further ***Case ao v Minister of Safety and Security ao; Curtis v Minister of Safety and Security ao*** 1996 (3) SA 617 (CC); 1996 (5) BCLR 609 (CC) at 656 as regards protection of autonomy (***Neethling's Law of Personality*** at 34-35, 220).

2.2.12 All three groups are of importance in this investigation, but it is the first and second groups, especially information privacy, that warrant special attention.

2.2.13 The protection of information privacy generally limits the ability of people to gain, publish, disclose or use information about others without their consent.[78] Individuals therefore have control not only over who communicates with them but also who has access to the flow of information about them.[79]

2.2.14 It should, however, be remembered that the rights entrenched in the Bill of Rights are formulated in general and abstract terms. The meaning of these provisions will therefore depend on the context in which they are used, and their application to particular situations will necessarily be a matter of argument and controversy.[80]

2.2.15 In terms of section 39 of the Constitution,[81] when interpreting the Bill of Rights, the values which underlie an open and democratic society based on human dignity, freedom and equality, should be promoted. This means that an exercise is required analogous to that of ascertaining the

---

78 McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18---11 and the references made therein. During the apartheid era in South Africa there was widespread abuse of rights protecting information. Most of the offensive legislation has been repealed.

79 McQuoid-Mason ***Law of Privacy*** at 99. Neethling, Potgieter & Visser ***Delict*** at 332: "Accordingly, privacy may only be infringed by unauthorized acquaintance by outsiders with the individual or his personal affairs." See also ***Neethling's Law of Personality*** at 33.

80 De Waal et al ***Bill of Rights Handbook*** at 117. In the post-constitutional era the South African Constitutional Court has delivered a number of judgments on the right to privacy relating to the possession of indecent or obscene photographs (***Case and Curtis v Minister of Safety and Security*** supra, the scope of privacy in society (***Bernstein v Bester*** supra); and searches and information privacy (***Mistry v Interim Medical and Dental Council of South Africa*** supra). All the judgments were delivered under the provisions of the interim Constitution as the causes of action arose prior to the enactment of the final Constitution. However, as there is no substantive difference between the privacy provisions in the interim and final Constitutions, the principles remain authoritative for future application.

81 Section 39 of the Constitution reads as follows:

Interpretation of Bill of Rights

39. (1) When interpreting the Bill of Rights, a court, tribunal or forum -

(a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom;
(b) must consider international law; and
(c) may consider foreign law.

(2) When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.

(3) The Bill of Rights does not deny the existence of any other rights or freedoms that are recognised or conferred by common law, customary law or legislation, to the extent that they are consistent with the Bill.

boni mores or legal convictions of the community in the law of delict.[82]

2.2.16 Of importance is Ackermann J 's dictum in ***Bernstein ao v Bester NO ao*** [83] where he stated:

> The nature of privacy implicated by the "right to privacy" relates only to the most personal aspects of a person's existence, and not to every aspect within his or her personal knowledge and experience.

2.2.17 Earlier he explained it as follows:[84]

> In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment which is shielded from erosion by conflicting rights of the community.... Privacy is acknowledged in the truly personal realm.

2.2.18 Neethling[85] criticises this meaning of privacy as too "restrictive", especially in regard to data protection where individual bits of information viewed in isolation may not be private, but where the sum total is of such a nature that an individual may want to protect it.[86] Thus in principle compiling the data record and obtaining knowledge thereof constitutes an intrusion into the private sphere.[87]

2.2.19 His criticism was validated by Langa DP in ***Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty)***

---

82 The section furthermore requires reference for purposes of interpretation to international human rights law in general. This is not confined to instruments that are binding on South Africa. A person may also rely on rights conferred by legislation, the common law or customary law. Such rights may not, however, be inconsistent with the Bill of Rights. Although section 39 provides a starting-point when trying to interpret the Bill of Rights, it requires interpretation itself. The Constitutional Court has therefore laid down guidelines as to how the Constitution in general and the Bill of Rights in particular should be interpreted (see De Waal et al ***Bill of Rights Handbook*** 2000 at 131 ff). It should be interpreted by first of all determining the literal meaning of the text itself and identifying the purpose or underlying values of the right. A generous interpretation should furthermore be given to the text, and the history of South Africa and the desire not to repeat it should be taken into account. Finally, the context of a constitutional provision should be considered, since the Constitution is to be read as a whole and not as if it consists of a series of individual provisions to be read in isolation.

83 Supra at 789.

84 At 788-789; see also ***NM ao v Smith ao*** supra at 261.

85 See Neethling 1997 ***THRHR*** at 140; Neethling J "The Concept of Privacy in South African Law" 2005 ***SALJ*** 18 at 20.

86 See on this ***Neethling's Law of Personality*** at 270, ***Privaatheid*** at 358-359; Neethling ***Huldigingsbundel WA Joubert*** at 112-113; Du Plessis W ***Die Reg op Inligting en die Openbare Belang*** LLD thesis PU for CHE 1986 (hereafter referred to as "Du Plessis thesis") at 392.

87 This view also appears by implication from the decision in ***S v Bailey*** supra at 189-190. Here the court held that the compulsory furnishing of information to the state in terms of the repealed Statistics Act 66 of 1976 does amount to a factual infringement of privacy, but that such an infringement is lawful because it is permitted by a statutory provision.

Ltd v Smit NO ao,[88] where the court held that the statements in ***Bernstein ao v Bester NO ao*** characterises the right to privacy as lying along a continuum, where the more a person inter-relates with the world, the more the right to privacy becomes attenuated.

2.2.20 Having said that, Langa DP further held that the right to privacy should not be understood to mean that persons no longer retain such a right in the social capacities in which they 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.[89]

2.2.21 The right to privacy is not absolute. As a common law right of personality it is necessarily limited by the legitimate interests of others and the public interest.[90] As a fundamental right it can be limited in accordance with the limitation clause of the Bill of Rights (section 36), that is, by a law of general application which includes other fundamental rights.[91] In each case a careful weighing up of the right to privacy and the opposing interests or rights will have to take place.

2.2.22 Any information privacy legislation will therefore have to find a balance between the data subject's fundamental right to privacy as set out in section 14 of the Constitution on the one hand, and on the other hand, other persons' legitimate needs to obtain information about the data subject. These needs may be based on the person or institution's fundamental right to choose their trade, occupation or profession freely,[92] their fundamental right to access to information,[93] their

---

88 2001 (1) SA 545 (CC).

89 Para 16 at 557.

90 See ***Neethling's Law of Personality*** at 240 ff.

91 See Neethling, Potgieter and Visser ***Delict*** at 16.

92 As set out in section 22 of the Constitution, which states:
Every citizen has the right to choose their trade, occupation or profession freely. The practice of a trade, occupation or profession may be regulated by law.

93 As set out in section 32 of the Constitution which states:
(1) Everyone has the right of access to –
(a) any information held by the state, and;
(b) any information that is held by another person and that is required for the exercise or protection of any rights;
(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

fundamental right to freedom of expression,[94] as well as other legitimate interests or rights.

2.2.23 In this investigation it is the delicate balance between the right to privacy and these opposing rights and interests that has to be determined.

2.3 Infringement of the right to privacy

2.3.1 The elements of liability for an action based on an infringement of a person's privacy are in principle the same as any other injury to the personality, namely an unlawful and intentional interference with a legally protected personality interest - here the right to privacy.

2.3.2 The jurisprudence on the application of standards of reasonableness in the common law and jurisprudence in terms of the limitation clause under section 36 of the Constitution inform each other.[95]

2.3.3 Although it is possible that a new constitutional delict may emerge in future,[96] the courts seem (in accordance with their obligation in terms of section 39(2) of the Constitution) to be developing the common law by infusing it with the spirit of the Constitution. It is therefore a hybrid action based on a mixture of the common law and constitutional imperatives.[97] The discussion that follows will therefore focus on the common law elements while at the same time trying to

---

It should be noted that section 239(b)(ii) of the final Constitution expressly excludes from the ambit of "organ of state" courts and judicial officers. The right to privacy is furthermore likely to constitute an acceptable limitation on section 32 in certain cases. See also PAIA.

94 As set out in section 16 of the Constitution which states:

(1) Everyone has the right to freedom of expression, which includes -
- a) freedom of the press and other media;
- b) freedom to receive or impart information or ideas;
- c) freedom of artistic creativity; and
- d) academic freedom and freedom of scientific research.

(2) The right in subsection (1) does not extend to -
- a) propaganda for war;
- b) incitement of imminent violence; or
- c) advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.

95 See discussion above.

96 See discussion above.

97 McQuoid-Mason ***Acta Juridica*** 2000 at 261.

accommodate the constitutional principles.

a) Essentials for liability

2.3.4 For a common-law action for invasion of privacy based on the *actio iniuriarium* to succeed, the plaintiff must prove the following essential elements: (i) impairment of the plaintiff's privacy, (ii) wrongfulness and (iii) intention (animus iniuriandi).[98] Negligence is as a rule, therefore, insufficient to render the wrongdoer liable. [99]

2.3.5 As shown above, the Constitutional Court has pointed out[100] that whereas at common law the test as to whether there has been an unlawful infringement of privacy is a single inquiry, under the Constitution a twofold inquiry is required. In the case of a constitutional invasion of privacy the following questions need to be answered: (a) Has the invasive law or conduct infringed the right to privacy in the Constitution?[101] [102] (b) If so, is such an infringement justifiable in terms of the requirements laid down in the limitation clause (section 36) of the Constitution?[103] For this reason the Constitutional Court has cautioned against simply using common law principles to interpret fundamental rights and their limitations.[104]

2.3.6 Rights cannot be overridden simply on the basis that the general welfare will be served by the restriction. The reasons for limiting a right need to be strong, as opposed to concerns that are

---

98 See McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18—2 and the references there.

99 ***NM ao v Smith ao*** supra at 764**.**

100 ***Bernstein ao v Bester NO ao*** supra at 790.

101 Woolman S "Coetzee: The Limitations of Justice Sach's Concurrence" 1996 ***SAJHR*** 12.1 99; ***S v Makwanyane ao***1995 (3) SA 391 (CC); 1995 BCLR 665 (CC) at para 100.

102 Section 36(2) states that only laws conforming to the test for valid limitations in section 36(1) can legitimately restrict rights. However, the subsection adds that rights can be justifiably limited in terms of "any other provision of the Constitution". In general, however, the courts will be reluctant to assume that provisions in the Constitution are contradictory and will, if possible, construe apparently conflicting provisions in such a way as to harmonise them with one another.

103 ***S v Makwanyane*** supra at para 102.

104 McQuoid- Mason ***Acta Juridica*** 2000 at 246. See however supra fn 32.

trivial.[105] They should also be in harmony with the intrinsic values set out in the Constitution.[106] In determining the current modes of thought and values of the community, the *boni mores* or convictions of the community regarding what is constitutionally right or wrong are of particular importance. This is a test analogous to that of the delictual unlawfulness inquiry under the common-law actio iniuriarum.[107]

(i) Invasion of privacy

2.3.7 The concept of privacy was defined earlier and applies to both common law and constitutional infringements of the right to privacy.[108] In terms of the common law the courts in South Africa have regarded invasion of privacy as an impairment of dignitas under the actio iniuriarum.[109]

2.3.8 In order to establish an infringement of the constitutional right to privacy the plaintiff will have to show that he or she had a subjective expectation of privacy which was objectively reasonable.[110] An individual's expectation of privacy must be weighed against the conflicting rights of the community. Such expectations may also be tempered by countervailing fundamental rights, such as freedom of expression or the right to access to information.[111]

---

105 ***Edmonton Journal v Alberta (Attorney General)*** 1989 64 DLR 4th 577 (SCC) at 612.

106 Devenish GE "The Limitation Clause Revisited - The Limitation of Rights in the 1996 Constitution" 1998 ***Obiter*** 256 at 263.

107 See ***Neethling's Law of Personality*** at 54-56; Burchell ***Personality Rights*** at 416.

108 McQuoid-Mason ***Acta Juridica*** at 247.

109 See discussion above regarding the recognition of privacy as a separate right.

110 This is analogous to the common law understanding of a wrongful infringement of the right to privacy, namely a factual infringement of privacy (acquaintance with private facts contrary to a person's determination and will), which is in conflict with the legal norm of boni mores and therefore unreasonable (see ***Neethling's Law of Personality*** at 221).

111 McQuoid-Mason ***Acta Juridica*** at 247. To determine whether the constitutional right to privacy has been infringed by a search, in ***Mistry v Interim Medical and Dental Council of South Africa*** supra at para 4, the Constitutional Court took the following factors into account:
- the substance of the communication was merely that a complaint had been made and that an inspection was planned;
- the information had not been obtained in an intrusive manner but had been volunteered by a member of the public;
- it was not about intimate aspects of the applicant's personal life but about how he conducted his medical practice;
- it did not involve data provided by the applicant himself for one purpose and used for another;
- it was information which led to a search, not information derived from a search; and
- it was not disseminated to the press or the general public or persons from whom the applicant could reasonably expect such private information would be withheld, but was communicated only to a person who had statutory responsibilities for carrying out regulatory inspections for the purpose of protecting the public health, and who was himself the subject to the requirements of confidentiality.

2.3.9 Invasions of privacy have been broadly divided into intrusions into (including acquisition of information) or interferences with private life, and disclosures or revelations of private information. These infringements of the right to privacy are sometimes referred to as substantive and informational privacy rights respectively.[112]

2.3.10 The question whether the processing of information of an individual infringes the right to privacy of that individual is factual and will be determined in each case separately. The privacy of the individual may be infringed by the collection and storing of personal information (which amount to an intrusion into privacy), as well as by the use and communication of personal information (which amount to a disclosure of privacy).

(ii) Wrongfulness

2.3.11 In order to found delictual liability in terms of the common law for the infringement of privacy, the conduct in question must be wrongful, and this is determined using the criterion of reasonableness or the norm of boni mores. Thus before it can be said that the practices of the data industry constitute a wrongful invasion of privacy or identity, it must appear not only that these interests were violated in fact,[113] but also that such violation was contra bonos mores or unreasonable.[114]

2.3.12 The acquaintance with private facts should therefore not only be contrary to the subjective determination and will of the prejudiced party, but at the same time, viewed objectively, also contra bonos mores. In the field of the protection of privacy, the boni mores or convictions of the community regarding what is delictually right and wrong is of particular importance in all countries

---

112 McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18---4. See also the reference above fn 72 to infringement of autonomy.

113 In other words, that there was unauthorised acquaintance with private facts.

114 See ***Neethling's Law of Personality*** at 221, 273-274.

as a criterion for wrongfulness.[115] This view is also apparent in South African case law.[116]

2.3.13 It has been pointed out, however, that "legal protection of private facts is extended to ordinary or reasonable sensibilities and not to hypersensitiveness."[117] Therefore the courts will not protect facts whose disclosure will not "cause mental distress and injury to anyone possessed of ordinary feelings and intelligence".[118]

2.3.14 This subjective-objective approach is similar to that of the Constitutional Court, which has held that a person's subjective expectation of privacy will only have been wrongfully violated if the court is satisfied that such expectation was objectively reasonable.[119]

2.3.15 In determining the current modes of thought and values of any community the courts may be influenced by its statute law. It is also clear that the Constitution - and its spirit, purpose and objects - will play a major role in determining the "new" boni mores of South African society.[120] Thus, it can be argued that the Bill of Rights "crystallizes" the boni mores of society by providing that an impairment of the right to privacy in the Constitution is prima facie unlawful. However, the Constitutional Court has pointed out that whereas the test for whether an invasion of privacy is unlawful at common law is a single inquiry, under the Constitution a two-fold inquiry is required, and has cautioned against simply using common law principles to interpret fundamental rights and their

---

115 Joubert WA ***Grondslae van die Persoonlikheidsreg*** Balkema Cape Town 1953 at 136 says: "Daar is min gebiede van die persoonlikheidsreg waar die opvattings van die gemeenskap so 'n groot rol speel by die bepaling van die omvang van die reg as in die geval van die reg op privaatheid." See also idem at 143-144; Van der Merwe and Olivier ***Onregmatige Daad in Suid Afrikaanse Reg*** at 449; McQuoid-Mason ***Law of Privacy*** at 118-122.

116 See eg ***S v A ao*** supra at 299 where Botha AJ set the limits of the right to privacy according to the "prevailing *boni mores* in accordance with public opinion". In ***Financial Mail (Pty) Ltd ao v Sage Holdings Ltd ao*** supra at 463 the Appelate Division held that "in demarcating the boundary between lawfulness and unlawfulness in the field, the Court must have regard to the particular facts of the case and judge them in the light of contemporary boni mores and the general sense of justice of the community as perceived by the Court"; see also ***O'Keeffe v Argus Printing and Publishing Co Ltd ao*** supra at 248; ***Jansen van Vuuren ao NNO v Kruger*** supra at 850; ***Jooste v National Media Ltd*** supra at 645-655; ***Motor Industry Fund Administrators (Pty) Ltd ao v Janit ao*** supra at 60; ***Sage Holdings Ltd ao v Financial Mail (Pty) Ltd ao*** supra at 130; ***S v I ao*** 1976 (1) SA 781 (RA) at 788-789; ***Rhodesian Printing and Publishing Co Ltd v Duggan ao*** at 594-595; see in general ***Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk*** supra at 387. See further ***Gosschalk v Rossouw*** supra at 492 where Corbett J applied the reasonableness criterion in this regard.

117 ***National Media Ltd ao v Jooste*** supra at 271.

118 ***National Media Ltd ao v Jooste*** supra at 270; ***Financial Mail (Pty) Ltd ao v Sage Holdings Ltd ao*** supra at 462.

119 McQuoid-Mason ***Acta Juridica*** at 232 and the references therein***; Neethling's Law of Personality*** at 221; See also supra fn 96.

120 McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18---3; ***Neethling's Law of Personality*** at 55-56.

limitations.

2.3.16 As indicated above, the common law accepts that privacy can be infringed only by an acquaintance with personal facts by outsiders contrary to the determination and will of the person whose right is infringed, and that such acquaintance can take place in two ways only, namely through intrusion (or acquaintance with private facts) and disclosure (or revelation of private facts). However, the Constitutional Court has also added autonomy as an interest protected under the constitutional right to privacy.[121]

2.3.17 It is necessary to examine the question of the unlawfulness of both intrusion into and disclosure of privacy in greater detail.

Intrusion

2.3.18 A violation of privacy by means of an act of intrusion[122] takes place where an outsider himself acquires knowledge of private and personal facts relating to the plaintiff, contrary to the plaintiff's determination and wishes.[123] This is also applicable to the collection and storage of personal information. When information relating to a person is collected, the total picture represented by the record of the facts is usually of such a nature that the person in question would like to restrict others from having knowledge thereof despite the fact that some of the information, viewed in isolation, is not “private” in the above sense. Thus in principle the compiling of an information record and obtaining knowledge thereof constitutes an intrusion into privacy.[124]

---

121 See the discussion supra.

122 See ***Neethling's Law of Personality*** at 222 ff.

123 For the sake of convenience two types of intrusion can be distinguished, namely acquaintance with private facts (i) where such acquaintance is totally excluded or is limited to specific persons, and (ii) where the acquaintance is permissible to an indeterminate but limited number of persons.The following guidelines may be used to facilitate determining whether an act of intrusion should be regarded as wrongful. In the first group the acquaintance is in principle wrongful unless such acquaintance takes place in accordance with the dictates of human nature and the composition of modern society. On the other hand, in the second group the acquaintance is in principle not wrongful, unless the acquisition is contrary to the dictates of human nature and the composition of modern society. Each case must be judged in its context. See ***Neethling's Law of Personality*** at 225-226.

124 See ***Neethling's Law of Personality*** at 270-271.

2.3.19 Generally speaking no person has to tolerate information concerning him being collected.[125] This would mean that, as a starting-point, the unauthorised collection or storage of personal information should be considered to be in principle contra bonos mores and thus prima facie wrongful.[126]

2.3.20 Similarly, and this stands to reason, the collection and storage of incorrect or misleading personal information is contra bonos mores and therefore wrongful, being an infringement of the right to identity.[127]

Disclosure or revelation

2.3.21 The infringement of privacy through an act of disclosure arises where, contrary to the determination and will of the plaintiff, an outsider reveals to third parties personal facts regarding the plaintiff, which, although known to the outsider, nonetheless remain private.[128]

2.3.22 It is important to note that the question of an infringement of privacy arises only if the plaintiff is identified with the disclosed facts.[129] If this element of identification is lacking, the disclosure does not relate to a specific person in his state of privacy.

2.3.23 A distinction can be made between the disclosure of private facts which have been obtained through an unlawful act of intrusion into privacy; disclosure of private facts in breach of a confidential relationship; and the mass publication of private facts.[130]

---

125 This view is comparable to – and is thus supported by – the principle that the continuous "shadowing" of a person by a private detective or extensive espionage on someone's activities infringes his right to privacy (see on this ***Neethling 's Law of Personality*** at 225); Neethling, Potgieter and Visser ***Delict*** 323.

126 See ***Neethling's Law of Personality*** at 274.

127 See ***Neethling's Law of Personality*** at 258,275.

128 See Neethling ***'s Law of Personality*** at 41, 274 ff; see also in general Giesker H ***Das Recht der Privaten an der eigenen Geheimsphäre*** 1905 (hereafter referred to as "Giesker") at 120 ff. See further the categories of publication of private facts identified by Prosser as referred to by McQuoid-Mason at 170: (i) the contents of private correspondence; (ii) debts; (iii) physical deformities and health; (iv) life-style; (v) childhood background; (vi) family life; (vii) past activities; (viii) embarrassing facts; (ix) confidential information; and (x) information stored in data banks.

129 Giesker at 122; see also Neethling ***Privaatheid*** at 47, 57, 92-93 on the application of the reasonable man test to determine whether a defamatory publication can be connected to the plaintiff.

130 See ***Neethling's Law of Personality*** at 226 ff.

2.3.24 As far as the first is concerned, if the storage of information is in principle wrongful, then it goes without saying – in view of the continuous nature of the wrongful conduct – that the communication thereof to third parties[131] should also be regarded as unlawful, in principle.[132]

2.3.25 Secondly, disclosure of private facts in breach of a confidential relationship is in principle wrongful. But it must be certain that such a relationship exists. Our law recognises, for example, the relationships between doctor and patient, banker and client, legal representative and client and spiritual advisor and congregant.[133] These examples mentioned should, however, not be regarded as a numerus clausus.[134] Whether a specific relationship deserves protection will depend entirely on the surrounding circumstances. Giesker[135] can be supported in this regard. He suggests that the more necessary it is for a person to impart the private facts to the outsider, the more pressing the protection against the disclosure of those facts to third parties by the outsider. Apart from these instances, a confidential relationship may also arise where there is an agreement between the parties that the private facts disclosed will be confidential or secret (Geheimhaltungsvertrag).[136] In such instances disclosure of the private facts will, besides breach of contract, also constitute an infringement of the right to privacy.[137]

---

131 Which amounts to a disclosure of private facts (see ***Neethling's Law of Personality*** at 274).

132 This view is supported by the rule that, eg, the disclosure of the contents of stolen private documents is wrongful in principle (see ***Neethling's Law of Personality*** at 226).

133 See ***Neethling's Law of Personality*** at 227ff.

134 Other examples which can be mentioned here are those between husband and wife, employer and employee, and teacher and pupil: see Neethling ***Privaatheid*** at 204.

135 At 131. For Maass HH ***Information und Geheimnis in Zivilrecht*** 1970 at 55 a legal duty to keep private facts secret also exists where someone is necessarily dependent upon taking another person into his/her confidence. See ***Neethling's Law of Personality*** at 228.

136 See Giesker at 129 ff; ***Neethling's Law of Personality*** at 228. It is obvious that the agreement must be valid (Giesker at 142).

137 Apart from confidential relationships, a duty not to disclose private facts in the present cirucumstances – ie where an outsider acquired authorised knowledge of the facts involved – may also arise in certain circumstances of authorised fixation or embodiment of the facts (by eg photography or tape-recording). Unauthorised disclosure of the embodied facts (eg the photograph) may then nevertheless be wrongful. An example can be found in ***Culverwell v Beira*** 1992 (4) SA 490 (W) where the alleged threatened disclosure of photographs of a naked woman taken by her lover was at stake. The court held that the woman had no legal basis to claim from her lover delivery of the photographs and negatives, or to prevent him from making copies from the negatives, since he was the owner thereof. She could not succeed merely because of the intimate and private nature of the photographs. However, the court by implication found that a disclosure of the photographs would be wrongful unless justified (see ***Neethling's Law of Personality*** at 228 fn 95). This decision can be supported, since the violation of privacy by disclosure of embodied private facts is often – as was the case in casu – of a much more serious nature than the mere disclosure of knowledge about such facts).

2.3.26 Thirdly, the mass publication of private facts is in principle wrongful.[138] [139]

2.3.27 It stands to reason that the use and disclosure of false or misleading information should also be wrongful – that such conduct is contra bonos mores requires no argument.[140]

iii) Intention

2.3.28 Apart from the wrongfulness of the infringement of privacy, the general rule is that intent or animus iniuriandi is also required by the common law before liability can be established.[141] This means that the perpetrator must have directed his will to violating the privacy of the prejudiced party (direction of the will), knowing that such violation would (possibly) be wrongful (consciousness of wrongfulness). In the absence of any of these elements, there is no question of intent.[142] Where, for example, a person bona fide but incorrectly believes that she is entering her own hotel room, the intent to infringe privacy is certainly lacking[143] and she should go free.[144]

---

138 See ***Neethling's Law of Personality*** at 231 ff.

139 The following guidelines may be used to facilitate the determination of whether an act of disclosure should be regarded in principle as wrongful. First, the disclosure of private facts acquired through a wrongful act of intrusion is in principle always wrongful. Similarly, the mass publication of private facts will always infringe the right to privacy. On the other hand, the disclosure of private facts to individuals or to small group of persons does not infringe the right to privacy unless there exists a specific confidential relationship. Such a relationship does not emerge solely from the necessity of disclosure of private facts to another person, but also from an agreement to secrecy. In either event the act should be judged in context, taking into account all the surrounding circumstances (see ***Neethling's Law of Personality*** at 236). The question of the protectability of the so-called letter secret should also be assessed according to the above principles. Therefore, apart from intrusion and mass publication, the letter secret should be protected against disclosure only if a special confidential relationship came into being between sender and receiver.

140 See supra fn 122 as to violation of identity (see also ***Neethling's Law of Personality*** at 275).

141 See ***Jansen van Vuuren ao NNO v Kruger*** supra at 849 (see also at 856-857) where Harms AJA opined that as a general rule, and irrespective of onus, a plaintiff who relies on the actio iniuriarum must allege animus iniuriandi. See ***S v A ao*** supra at 297 where it was held that the accused had intention in the form of dolus eventualis. See also ***Kidson ao v SA Associated Newspapers Ltd*** supra at 468 where Kuper J stated that "the reference in the article was intentional and in my view the existence of animus iniuriandi must be presumed". See further McQuoid-Mason ***Law of Privacy*** at 100 ff; Neethling ***Privaatheid*** at 256-257.

142 See ***Neethling's Law of Personality*** at 57-59,252-253.

143 See also McQuoid-Mason ***Law of Privacy*** at 236 ff; cf ***Littlejohn v Kingswell*** (1903) 13 CTR 154 at 159; ***S v Boshoff ao*** 1981 (1) SA 393 (T) at 396-397. Cf further ***Jansen van Vuuren ao NNO v Kruger*** supra at 856-857 where absence of consciousness of wrongfulness was also raised (unsuccessfully).

144 In this regard the decision in **S v I *ao*** supra deserves closer scrutiny. Beadle CJ required (at 787) for the lawfulness of spying on the activities of a spouse by the other spouse in order to protect his or her interest in obtaining evidential material regarding suspected adultery, inter alia that the spying had to take place in the belief, which had to be based on reasonable grounds, that the privacy of the guilty party only is violated. It is submitted that this requirement has no role to play in establishing the wrongfulness of the violating conduct. If it is clear that if one spouse was definitely involved in an adulterous relationship and the violation of privacy was reasonable, such violation is lawful irrespective of whether it occurred in the belief on reasonable

2.3.29 Animus iniuriandi is presumed as soon as wrongful infringement of privacy has been proved.[145] The defendant may then rebut the presumption.[146]

2.3.30 However, for policy reasons the courts have tended not to require the element of "consciousness of wrongfulness" as an element of animus injuriandi in wrongs touching on the liberty of the subject, such as wrongful arrest or detention, or wrongful attachment of goods. In such cases it is not open to defendants to argue that they were ignorant of the wrongfulness of their acts, and strict liability is imposed.

2.3.31 A possible effect of the Constitution on the concept of animus iniuriandi might be to regard certain of the aspects of the right to privacy mentioned in section 14 as so fundamental and important to South Africa's new democratic society that strict liability should be imposed in the same way as has been done for unlawful arrest, detention and attachment under the common law.[147] The result would be that in such cases it would not be open to defendants to show that they did not know that they were acting unlawfully by infringing a constitutional right. It has been argued that this modification of animus iniuriandi in cases involving breaches of constitutionally protected rights would accord with the "spirit, purport and objects" of the Bill of Rights.[148]

2.3.32 Neethling[149] is indeed of the opinion that the collection and use of personal information (especially by electronic databases) create such an enormous threat to the personality of the individual that it would be fair to hold the data industry accountable even without having to prove

---

grounds that the privacy of the guilty party only is violated. The presence of such a belief, whether reasonable or not, is relevant to the intent requirement of the offence concerned. Therefore, where the spouse believes that she infringes the privacy of the guilty party only – in other words, that she is acting lawfully – and the act of violation is indeed wrongful, consciousness of wrongfulness and accordingly intent is lacking.

145 See ***Kidson ao v SA Associated Newspapers Ltd*** supra at 468.

146 As far as liability of the mass media for the infringement of privacy is concerned, see ***Neethling's Law of Personality*** at 166-168; Neethling, Potgieter and Visser ***Delict*** at 306 fn 107, 317 fn 225 for an evaluation of the present negligence liability of the press for defamation in the light of the constitutional right to freedom of expression. What is said there applies mutatis mutandis to the protection of privacy.

147 In terms of the Constitution fault is not a requirement for an action based on the infringement of the constitutional right to privacy. Thus strict liability may be imposed upon a defendant who breaches the constitutional right to privacy. In some areas dealt with by section 14 the constitutional position will be the same as the common law position (McQuoid-Mason ***Acta Juridica*** at 255). Replacing the traditional fault requirement of the common law action with strict liability will therefore make little difference. However, in respect of other invasions of privacy the imposition of no-fault liability will mean a major departure from the basic principles of the actio injuriarium (McQuoid-Mason ***Acta Juridica*** at 261).

148 McQuoid-Mason ***Acta Juridica*** at 234. In ***NM ao v Smith ao*** supra at 767 Judge Madala indicated that it would not necessarily be impossible to develop the common law so as to impose negligence as an element of liability in respect of the actio iniuriarum. However, his opinion was that it would not be appropriate in the present case.

149 See ***Neethling's Law of Personality*** at 278, 2002 ***THRHR*** at 584; infra Chapter 5 para 3.2.

intent in each case. However, as an alternative to strict liability, he proposes that negligence based liability should also be considered.[150]

b) Defences/Justification

2.3.33 Defences to a common law action for invasion of privacy are similar to those for other actions under the actio iniuriarium.[151] These defences will be available but will still have to be examined in the light of the Constitution in order to determine whether they are consistent with the provisions of the limitation clause in section 36.[152]

2.3.34 In terms of the Constitution, if the plaintiff establishes that his or her right to privacy has been impaired, the defendant's conduct may not be wrongful if the latter can show that the invasion of privacy was reasonable and justifiable in terms of section 36(1).[153]

2.3.35 According to section 36(1) of the Constitution the rights in the Bill of Rights may be limited only in terms of law of general application which includes the common law. The onus of proving that the infringement is reasonable and justifiable in terms of section 36 rests on the person alleging it and should be discharged on a balance of probabilities.[154]

2.3.36. Section 36 of the Constitution [155] is a general limitation clause and sets out specific criteria

---

150 See Neethling 2002 ***THRHR*** at 583-584.

151 McQuoid-Mason ***Acta Juridica*** at 233 referring to Burchell ***Personality Rights*** at 388. A common law justification, usually, but not necessarily, arises when the defendant raises a defence. Under the Constitution the enquiry regarding whether the conduct of the defendant was reasonable and justifiable is usually part of the policy-based enquiry concerning unlawfulness. Consequently it has been suggested that the judgment in ***National Media Ltd ao v Bogoshi*** 1998 (4) SA 1196 (A) has begun to blur the distinction between constitutional and common law justifications by introducing the concept of reasonableness during the policy-based inquiry into unlawfulness in cases of publication by the press.

152 See discussion above.

153 McQuoid-Mason ***Acta Juridica*** at 254.

154 McQuoid -Mason ***Acta Juridica*** at 254 and the references made therein.

155 Section 36 of the Constitution provides:

Limitation of rights

36. (1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account relevant factors, including -

(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose; and

for the limitation of the fundamental rights in the Bill of Rights.[156]

2.3.37 The limitation of constitutional rights for a purpose that is reasonable and justifiable in a democratic society involves the weighing up of competing values, and ultimately an assessment on proportionality. There is no absolute standard that can be laid down for determining reasonableness and justifiability. Whether the purpose of the limitation is reasonable and justifiable will depend on the circumstances in a case-by-case application.[157]

2.3.38 The following five factors are identified in section 36(1) as making up the proportionality enquiry:

(a) nature of the right
(b) the importance of the purpose of the limitation
(c) the nature and extent of the limitation
(d) the relation between the limitation and its purpose; and
(e) less restrictive means to achieve the purpose.

2.3.39 The factors mentioned in section 36(1) are, however, not exhaustive. They are key considerations, to be used in conjunction with any other relevant factors, in the overall determination whether a limitation is justifiable.[158] Once a court has examined each of the factors, it must then weigh up what the factors have revealed about the purpose, effects and importance of the infringing law on the one hand; and on the other, the nature and effect of the infringement caused by the action or law (a proportionality test) to determine its constitutionality. The court must engage in a balancing exercise and arrive at a global judgment on proportionality, and not adhere mechanically

---

(e) less restrictive means to achieve the purpose.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.

156 Section 36 is a codification of the approach set out in ***S v Makwanyane ao*** supra. The judge held as follows:

In the balancing process, the relevant considerations will include the nature of the right that is limited, and its importance to an open and democratic society based on freedom and equality; the purpose for which the right is limited and the importance of that purpose to such a society; the extent of the limitation, its efficacy, and particularly where the limitation has to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question.

157 ***S v Makwanyane*** supra at 708.

158 ***S v Manamela ao (Director-General of Justice Intervening)*** 2000 (5) BCLR 491 (CC) at 508 and section 36(1) of the Constitution.

to a sequential check-list.[159]

2.3.40 The High Court has explained that the criteria should be applied as follows:[160]

> There must be a reason which is justified in an open democratic society based on human dignity, equality and freedom for the infringement of a constitutional right. Further the limitation must be shown to serve a justifiable purpose.

2.3.41 A court is further empowered, horizontally between persons, to develop rules of the common law so as to limit the right in accordance with section 36(1) (section 8(3)). This will not necessarily require a complete rewriting of the South African private law. It may, however, have an impact on the style of judicial reasoning. That is, the rules of private law will no longer justify themselves, but must now be justified in terms of our new-found commitment to substantive constitutional values.[161]

2.3.42 The common law defences can be divided into those excluding wrongfulness and those excluding fault.

i) Defences excluding wrongfulness

2.3.43 Examples of traditional grounds of justification that may be relevant to the right to privacy are consent to injury, necessity, private defence, impossibility, public interest and performance in a statutory or official capacity. However, these grounds of justification do not constitute a *numerus clausus* as new grounds may emerge when weighing up the conflicting interests of persons in society.[162]

Consent

2.3.44 Consent to infringement of privacy is a unilateral act. Therefore it may be revoked at any time

---

159 ***S v Makwanyane*** supra at para 104; ***S v Manamela ao (Director-General of Justice Intervening)*** supra at 508.

160 ***Lotus River, Ottery, Grassy Park Residents Association ao v South Peninsula Municipality*** 1999 (2) SA 817 (C) per Davis J as referred to by McQuoid-Mason ***Acta Juridica*** 2000 at 253.

161 Cockrell ***Bill of Rights Compendium*** at 3A10.

162 See ***Neethling 's Law of Personality*** at 56.

preceding the defendant's injurious conduct.[163] Consent can be given expressly or tacitly.[164]

2.3.45 In order to be valid, consent must meet certain requirements. Regarding the violation of privacy, it is particularly important that the consent must be voluntary.[165] In addition, the consent must not be contrary to public policy or contra bonos mores. For this reason an irrevocable consent to violation of privacy is regarded as invalid.[166]

2.3.46 Where a person has given valid consent to the processing of information regarding himself, there can be no question of wrongfulness. Of course, the consent must satisfy all the requirements for valid consent. For example, it may possibly be argued that consent for the processing of information is invalid if it is set as a condition of employment, or of the continuance of a contract of employment, by an employer.[167] It is a question of fact whether consent was given in a particular instance.[168] These principles naturally also apply to the processing of personal information.

Necessity [169]

2.3.47 Necessity is present when the defendant by vis major is put into such a position that he can

---

163 See ***Jooste v National Media Ltd*** supra at 647. This principle applies as a rule irrespective of an agreement between the parties. In **Jooste** at 647 Olivier J explained it as follows: "Dit is relevant dat die onderhawige toestemming in die vorm van 'n ooreenkoms gegee is. Hierdie feit kan in gepaste gevalle meebring dat die toestemming nie teruggetrek mag word nie . . . Maar waar die reg waarom dit gaan van hoogs persoonlike aard is, soos die persoonlikheidsregte, geld 'n ander benadering. In daardie gevalle, meen ek, kan die toestemming herroep word mits dit tydig is. Die teenparty se remedie is om skadevergoeding weens kontrakbreuk te verhaal."

164 See ***Neethling's Law of Personality*** at 250-1.

165 Nevertheless there are many cases of violation of privacy where consent is indeed given, but it can seldom be considered voluntary as a result of some form of coercion. This is the case, for example, where a prospective employee, as a prerequisite for employment, is compelled to undergo polygraph or personality tests. Because of such coercion the consent should be invalid and consequently the violation of privacy wrongful. See Neethling ***Privaatheid*** at 207 on the position in the USA.

166 See Neethling ***Privaatheid*** at 103-104 on the position in German law.

167 See ***Neethling 's Law of Personality*** at 251.

168 See ***Neethling 's Law of Personality*** at 251.

169 See ***Neethling 's Law of Personality*** at 241-2. It is important to note that either legitimate or lawful interests of individuals or institutions or the public interest may justify the processing of data. However, it should be pointed out that such grounds of justification for the activities of the data industry are relevant only in connection with infringements of privacy. It is unthinkable that an infringement of identity may be justified. Thus the collection and disclosure of false or misleading personal data is always summarily wrongful (see ***Neethling 's Law of Personality*** at 275).

protect his legitimate interests (or those of others) only by infringing another's legal interests (in this particular case, another's privacy). If there was a reasonable alternative available to the defendant, the violating act would not be justified.[170]

2.3.48 In order to protect, further or maintain a certain interest (for example, a business interest), it is often necessary for individuals or institutions (such as potential employers, insurers, sellers, lessors and financiers) to obtain reasonably sufficient information regarding particular individuals.[171] The need to process information which infringes the privacy of "innocent" data subjects demonstrates a particular application of necessity[172] as a ground of justification; or, if one does not want to classify it as necessity, as an example of the maintenance of legitimate private interests.[173]

2.3.49 For the processing of information to be deemed lawful under the present circumstances, the following requirements must be satisfied:[174]

(i) First it must be certain that the interest which is protected is indeed a legitimate one, in other words, an interest recognised and protected by law. If this is not the case, the processing will be wrongful.[175] The same notion also forms the basis of the view[176] that information may be processed only for one or more specified lawful purposes. Information processing can have a lawful purpose only if the object is to further or protect a legitimate interest;[177] and in order that the interest(s) involved may be identified and defined, the purpose must clearly disclose which interests are at stake. For this reason the purpose must be circumscribed. Without such circumscription or definition it will be very difficult to judge whether or not the processing of information is lawful – in other words, whether a legitimate interest is protected.

---

170 See ***Neethling 's Law of Personality*** at 241; see also McQuoid-Mason ***Law of Privacy*** at 233.

171 However, since in many instances it is impracticable for these individuals or institutions to gather such information themselves, the task is performed by institutions (such as credit bureaux) which possess the necessary means and efficiency to process complete data records on a permanent basis. The latter institutions then make the information in their possession available to interested parties (see ***Neethling 's Law of Personality*** at 275).

172 See ***Neethling 's Law of Personality*** at 241-2, 275.

173 Apart from business interests, other private interests, such as scientific interests, may also justify the processing of data (see ***Neethling 's Law of Personality*** at 250).

174 See generally Neethling ***Privaatheid*** at 361-363, ***Neethling's Law of Personality*** at 275-277; see also McQuoid-Mason ***Law of Privacy*** 197-200. As will be seen infra (Chapter 6), these requirements also appear in foreign statutes and bills on data protection (see Neethling ***Huldigingsbundel WA Joubert*** at 118-120).

175 The collection and use may of course be lawful for other reasons – eg where valid consent was given.

176 See the comparative law discussion infra (Chapter 4) with regard to "purpose specification" as data protection principle.

177 Which includes the public interest: see the discussion infra.

(ii) From the foregoing it follows that the information may be used or communicated only for the protection of the legitimate interest(s) involved,[178] and that the use of information in a manner incompatible with this purpose is thus wrongful. Accordingly, there should be a duty of confidentiality on a data controller in so far as the processing of information is not in accordance with the defined purpose.[179]

(iii) Even if it is certain that the processing is for the protection of a legitimate interest, it must still be exercised in a reasonable manner.[180] A requirement which plays an important role in this regard is that the type and extent of the compiled information must be reasonably necessary for,[181] and consequently also connected with (or relevant to), the protection of the interest – in other words, no more information than is necessary for this purpose should be processed.[182] The defined or specified purpose thus also circumscribes the limits of information processing. The activities of credit bureaux may serve as an example. The purpose of these institutions is to process information for the protection of business interests in creditworthiness; thus only information reasonably linked to creditworthiness should be gathered and communicated. Any other personal facts, such as drinking habits, physical or mental health, extra-marital affairs, political views and religious affiliation are usually unnecessary for the specified purpose and therefore should not be processed.[183] If

---

178 See the comparative law discussion infra (Chapter 4) with regard to "limitation" as data protection principle. The ground of justification priviledged occasion may also be applicable here (see ***Neethling's Law of Personality*** at 275 fn 98, 251-2; see also McQuid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18-12 with regard to justification of breach of constitutional privacy). The constitutional right of access to information held by private persons (section 32(1)(b) of the Constitution) should not adversely affect the present principle since access may only be granted to persons for the excercise or protection of a right (see ***Neethling's Law of Personality*** at 275 fn 98).

179 A further principle flowing from this is that unauthorised access to processed data by a third party should in principle also constitute a wrongful intrusion into the privacy of the individual involved, even though such outsider may have a legitimate interest in the data. See Neethling ***Huldigingsbundel WA Joubert*** at 118 fn 90 91, ***Neethling's Law of Personality*** at 276 fn 101.

180 The unreasonable protection of an interest is in principle unlawful (cf Neethling J ***Van Heerden-Neethling Unlawful Competition*** Lexis Nexis Durban 2008 at 134; Neethling, Potgieter and Visser ***Delict*** at 112 ff; Van der Merwe and Olivier ***Onregmatige Daad in Suid Afrikaanse Reg*** at 64 ff); cf also the discussion of ***Gosschalk v Rossouw*** supra at 490-492 in ***Neethling's Law of Personality*** at 244 fn 222; infra fn 175.

181 Cf again the discussion of ***Gosschalk v Rossouw*** supra at 490-492 (see previous fn). The comment there applies mutatis mutandis here.

182 See the comparative law discussion infra (Chapter 4) with regard to "minimality" as a data protection principle.

183 See also McQuoid-Mason DJ "Consumer Protection and the Right to Privacy" 1982 ***CILSA*** 135 at 139. Such sensitive personal facts should also not be processed on a permanent basis unless it is clear that such processing is essential for the protection of a legitimate interest (see the comparative law discussion infra (Chapter 4) with regard to "sensitivity" as data protection principle). In many instances the acquisition and communication of such data (eg facts of an extra-marital relationship) to an interested party by a private detective agency should be sufficient on a single occasion basis to protect the interests involved (here the interest of a client in collecting and safeguarding evidential material concerning adultery) (cf ***Neethling's Law of Personality*** at 276 fn 105).

information which is unnecessary for the protection of a legitimate interest is acquired and communicated the bounds of justification are exceeded, and such conduct is unreasonable and wrongful. Whether information is reasonably necessary is a factual question which must be determined with reference to all the relevant circumstances of a particular case.

(iv) An important application of the previous requirement is that obsolete information is generally not reasonably necessary for the protection of a legitimate interest. Therefore information may not be stored or used for longer than is reasonably necessary for the specified purpose.[184]

(v) The bounds of reasonableness in relation to protecting a legitimate interest are also exceeded if information which has been obtained in an unlawful manner (such as by reading private documents, illegal wire-tapping or shadowing a person) is processed.[185] Put differently, on account of the continuing wrongfulness in these instances, such information may not be processed because the processing is inseparably linked to the original wrongfulness. If the collection and use of this type of information are regarded as lawful, the data industry will be tempted to employ illegal methods of obtaining information – a practice which cannot be accepted.

Public interest

2.3.50 The state generally protects or maintains the public interest when, by virtue of its greater power, it lays down conditions restricting the rights and freedoms of its subordinates in the public interest. These instances of restriction of the right to privacy fall within the ground of justification of statutory or official capacity.[186]

2.3.51 This ground of justification is especially appropriate in the upholding of law and order, the prevention of crime and disorder, state security, public health, morality and welfare.[187] Obviously,

---

184 See the comparative law discussion infra (Chapter 4) with regard to "minimality" as data protection principle. Many foreign statutes lay down periods after which data is regarded as obsolete. It is usually stipulated that data which is older than seven years may not be collected (see also Neethling ***Huldigingsbundel WA Joubert*** at 119 fn 97; McQuoid-Mason ***Law of Privacy*** at 84 fn 88).

185 See the comparative law discussion infra (Chapter 4) with regard to "fairness and lawfulness" as data protection principle. See also the discussion supra.

186 See ***Neethling's Law of Personality*** at 243-4, 277-8.

187 In terms of the Interception and Monitoring Prohibition Act 127 of 1992 (which will be replaced by the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002) a judge may, under certain conditions, direct that postal articles or communications transmitted by telephone or in any other manner over a telecommunications line be intercepted, or certain conversations be monitored. Cf also section 27 (articles other than letters may be opened for examination), section 35 (articles addressed to persons conducting a lottery or sports pool or dealing in indecent or obscene matter may be opened) and especially section 118 (detention of postal articles and telegrams suspected

the lawfulness or unlawfulness of a violation of privacy by exercising these capacities must be determined with reference to the relevant permissive statute or common law rule. The right to privacy is violated when the defendant transgresses his capacity.[188] A factor which plays an important role in the question whether or not the particular capacity has been transgressed, is whether the extent of the conduct concerned was reasonably necessary.[189]

2.3.52 The processing of personal information to protect the public interest is almost exclusively within the jurisdiction of the state and its organs.

2.3.53 In order for the collection and processing of information to be lawful, certain general requirements must be met. Most of these requirements are analogous to those that apply in the case of the maintenance of legitimate private interests.[190]

(i) First, the state must be expressly authorised by a valid statutory provision to process

---

of being concerned with offences and action to be taken in connection therewith) of the repealed Post Office Act 44 of 1958. The state is also empowered by statute to gather and use personal information (see eg ***S v Bailey*** supra at 189-190 on the powers in terms of the repealed Statistics Act 66 of 1976 in this regard - see also ***Neethling's Law of Personality*** at 244 fn 219) and (in terms of the Criminal Procedure Act 51 of 1977) to search persons and homes (see on this McQuoid-Mason ***Law of Privacy*** at 136-141). For further examples of statutory powers justifying a violation of privacy, see in general McQuoid-Mason ***Law of Privacy*** at 141ff, 145-147, 158 ff, 160 ff, 164 ff, 235. However, it should be noted that the above-mentioned statutory provisions may be in conflict with the Constitution. Statutory limitations of the right to privacy (which is specifically protected in section 14 of the Constitution), like the ones mentioned above, will have to meet the requirements of section 36 (the limitation clause) of the Constitution.

188 Cf ***Neethling's Law of Personality*** at 243-4.

189 A important case in this regard is ***Gosschalk v Rossouw*** supra. There the court recognised that police questioning may violate a person's right to privacy (at 490-492). However, Corbett J stated very clearly that this right does not apply absolutely, but is restricted especially by statutory capacities (at 491). The judge stated: "The right of the citizen to enjoy these immunties *vis-à-vis* the State, or the Executive, constitute what are often termed 'civil liberties' or 'the liberty of the individual or the subject'. In some countries these rights are enshrined in the Constitution or in a Bill of Rights. This is not so in this country. Here they are enshrined in the common law. At the same time the Parliament of this country may make any legislative encroachment it chooses upon the life, liberty or property of its citizens and it is the function of the courts to enforce Parliament's will." (See also ***S v Bailey*** supra at 189-190. Of course, this statement is no longer correct as the Constitution now protects fundamental rights in Chapter 2, and section 2 of the Constitution provides that the Constitution "is the supreme law of the Republic", and that "law or conduct inconsistent with is invalid".) On the other hand, the statutory capacity of the police to interrogate people is also not unlimited (***Gosschalk*** at 491-492). Consequently the individual interest in privacy and the interest of the state in upholding law and order in this regard must, where these interests are in conflict, be reconciled according to the reasonableness criterion. The court formulated its viewpoint thus (at 492): "I consider that police interrogation should be limited to that which is necessary for the investigation of the offence or alleged offence in question and that, in extent, it should not exceed what is reasonable in all the circumstances of the case. In determining what is reasonable in a particular case the Court must seek to reconcile two competing interests, viz (i) that of the individual to be protected from illegal or irregular invasions of his liberties by the authorities, and (ii) the interest of the State to secure information and evidence relating to crimes which have been committed so that justice may be properly administered . . . Neither of these two interests should be allowed to wholly displace the other. It is the duty of the Court to ensure that a fair balance between them is maintained and the basic criterion must be the test of reasonableness as applied to the particular facts of the case". Seeing that the limitation clause (section 36) of the Constitution also makes use of a reasonableness criterion, the position in terms of the Constitution should be basically the same as in the common law in this regard.

190 See generally Neethling ***Privaatheid*** at 362-363, ***Huldigingsbundel WA Joubert*** at 120-121; **Neethling'*s Law of Personality*** at 277-8.

information.[191] As said, in view of the constitutional protection afforded the right to privacy,[192] any such legislation must be reasonable and justifiable in an open and democratic society based on freedom, human dignity and equality.[193]

(ii) Second, the information may be used or communicated only for the purposes recognised by the statutory authorisation.

(iii) Third, the protection of the public interest must take place in a reasonable manner, which means that the information must be reasonably necessary for and related to the statutory purpose.[194]

(iv) Fourth, the information may not be processed for longer than is necessary for the statutory purpose.

(v) Fifth, information acquired in an unlawful manner may not be processed. Where the state or its organs exceed their statutory authority, their conduct is wrongful and they will not be allowed to make use of the fruits of such illegality.

2.3.54 If the private or public data controller[195] acts wrongfully in terms of the abovementioned information protection principles, the ordinary delictual remedies,[196] namely the interdict, the actio iniuriarum for obtaining personal satisfaction and the actio legis Aquiliae for recovering patrimonial damages, should be available to the prejudiced person.[197] The actio iniuriarum is an action by which a person claims an amount of money for injured feelings whereas the actio legis Aquiliae is an

---

191 It is generally accepted that without an express statutory authorisation, data processing by the state should be regarded as unlawful unless the consent of the individual has been obtained (see Neethling ***Huldigingsbundel WA Joubert*** at 120 fn 104). This principle is further supported by the fact that the constitutionally entrenched right to privacy may only be limited by a statutory rule which is in conformity with the limitation clause of the Constitution (section 36).

192 See the previous fn.

193 See section 36 of the Constitution. State demands for information which is reasonably required for official statistical, census and income tax purposes are likely to be regarded as reasonable and justifiable. Likewise statutory reporting requirements concerning information about child abuse and mental patients who are dangerous to others are likely to be declared constitutional (see McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18---12).

194 Cf the application of the criterion of reasonableness in ***Gosschalk v Rossouw*** supra at 490-492 (see on this supra fn 182).

195 If any institution (private or public) collects and communicates personal information for statistical purposes, it should take steps to ensure anonymity: in other words, that statistics cannot be identified with a particular individual. If this requirement is not met, the data controller acts unlawfully for the reason that the processing is not reconcilable with the specified purpose (impersonal statistics) (cf the discussion supra).

196 See ***Neethling's Law of Personality*** at 278; also Faul W ***Grondslae van die Beskerming van die Bankgeheim*** LLD thesis RAU 1991 at 536-537.

197 See McQuoid-Mason ***Law of Privacy*** at 198-199.

action by which a person claims an amount of money for actual monetary loss. Fault should not be required in actions for satisfaction or damages. The collection and use of personal information (especially by means of electronic data banks) pose such a serious threat to an individual's personality[198] that it is probably fair and justifiable to hold an information institution liable even where intention or negligence is not present.[199]

Private defence

2.3.55 Private defence is present when the defendant defends himself against another's actual or imminently threatening wrongful act in order to protect his own legitimate interests or such interests of someone else. Acts of private defence justifying an infringement of privacy seldom occur.[200] Nevertheless, although such situations are not ruled out, this defence is not relevant in the information-protection field.

Impossibility

2.3.56 Where it is reasonably (not physically) impossible for a person to ward off damage to another, he may raise the defence of impossibility which will exclude the wrongfulness of his omission.[201] This defence is particularly apposite with regard to information processing. If a data controller can prove that it has done everything reasonably possible to ensure compliance with the information protection principles, the wrongfulness of its processing will be excluded. [202]

(ii) Defences excluding intention

2.3.57 In the common law the general principles of the actio injuriarium apply to defences excluding intention. Once the other elements of an action for invasion of privacy have been proved, animus injuriandi will be presumed. The evidential burden then shifts to the defendant to show absence of intention.[203]

---

198 See also Neethling 2002 ***THRHR*** at 584. See generally on strict liability Neethling, Potgieter and Visser ***Delict*** at 329 ff.

199 See Neethling ***Privaatheid*** at 363; ***Neethling's Law of Personality*** at 278; See also para 2.3.32 above regarding Neethling's proposal that negligence liability should also be considered as an alternative to strict liability.

200 See ***Neethling's Law of Personality*** at 242-3.

201 See Neethling, Potgieter and Visser ***Delict*** at 85.

202 See ***Neethling's Law of Personality*** at 280 fn 136.

203 McQuoid-Mason ***Law of Privacy*** at 237 and references to courts cases therein.

2.3.58 The categories of the defences which may be used to exclude intention are not closed. They include rixa, jest, mistake and any other defence which shows subjectively that the defendant did not have the intention to injure, such as insanity or intoxication.[204]

2.3.59 Since fault is not a requirement for an action based on the infringement of a constitutional right to privacy, strict liability may be imposed for breach of this right.

2.3.60 The constitutional right to privacy may be regarded as so fundamental that defendants may not argue that they were ignorant of the unlawfulness of their act. Alternatively, they may be held liable on the basis of negligence if their ignorance was unreasonable.[205]

c) Remedies

2.3.61 The generally accepted main remedies for common law invasions of privacy are: (i) the actio iniuriarum; (ii) the actio legis Aquiliae; and (iii) the interdict.[206] It has also been decided that the disused common law remedy of a right to retraction and apology should be revived.[207]

2.3.62 In the case of an infringement of or threat to the right to privacy as a fundamental right, in terms of section 38 of the Constitution the prejudiced or threatened person is entitled to approach a competent court for appropriate relief, including a declaration of rights.[208] Where a delictual remedy will also effectively vindicate the fundamental right to privacy and deter future violations of it, the delictual remedy may be considered to be appropriate constitutional relief and in this way may serve a dual function.[209]

i) Actio injuriarum

---

204 McQuoid-Mason in Chaskalson et al ***Constitutional Law of South Africa*** at 18---8.

205 Cf McQuoid-Mason ***Law of Privacy*** at 237.

206 See ***Neethling's Law of Personality*** at 250-254.

207 See ***Mineworkers Investment Co (Pty) Ltd v Modibane*** 2002 (6) SA 512 (W); see also ***Dikoko v Mokhatla*** 2006 (6) SA 235 (CC) 258,274; Neethling J and Potgieter JM "Herlewing van die Amende Honorable as Remedie by Laster" 2003 66 ***THRHR*** (hereafter referred to as "Neethling & Potgieter 2003 ***THRHR***")329 ff; cf McQuoid-Mason ***Acta Juridica*** at 234 and his reference to Midgley JR "Retraction, Apology and Right of Reply" 1995 58 ***THRHR*** 288 at 296;but see ***Young v Shaikh*** 2004 (3) SA 46 (C) 57.

208 Eg, a statute limiting the right to privacy in an unreasonable manner may be set aside or interpreted in a restrictive manner (see Neethling, Potgieter and Visser ***Delict*** at 22).

209 See ***Fose v Minister of Safety and Security*** 1997 (3) SA 786 (CC) at 836-837; Neethling, Potgieter and Visser ***Delict*** at 23.

2.3.63 If a person's privacy is wrongfully and intentionally infringed, he may recover sentimental damages or satisfaction (solatium) for injured feelings.[210] In privacy cases the plaintiff is being compensated for the emotional suffering as a result of having his or her private life infringed.[211]

2.3.64 The amount of compensation is in the discretion of the court and is assessed on what is fair and reasonable.[212] Factors which may play a role in the assessment of the amount of the satisfaction are still largely absent from case law.[213] Also note that the Constitutional Court has held that additional constitutional punitive damages should not be awarded in terms of the Constitution for infringements of fundamental rights and freedoms.[214] But because of the constitutional entrenchment, the amount of satisfaction may nevertheless be increased.[215]

ii) Actio legis Aquiliae

2.3.65 Where the plaintiff has also suffered actual monetary loss as a result of the violation of privacy, he could recover damages by means of the Aquilian action. Negligence is sufficient for liability.[216]

iii) Interdict

2.3.66 Where a person is confronted with a threatening or continuing infringement of his or her right to privacy, an interdict should be obtainable.[217] Fault on the part of the perpetrator is not a requirement.[218]

---

210 ***Jansen van Vuuren ao NNO v Kruger*** supra at 857-858.

211 McQuoid-Mason ***Law of Privacy*** at 170.

212 See ***Neethling's Law of Personality*** at 253; ***Jansen van Vuuren ao NNO v Kruger*** supra at 857-858.

213 In ***Jansen van Vuuren ao NNO v Kruger*** supra at 857 Harms AJA said: "It is extremely difficult in this matter to make such an award because there are no obvious signposts. Nevertheless, the right to privacy is a valuable right and the award must reflect that fact." But see ***Neethling's Law of Personality*** at 253-4.

214 McQuoid-Mason ***Acta Juridica*** 2000 at 235 and the reference to ***Fose v Minister of Safety and Security*** supra at paras 69-73 per Ackermann J.

215 Cf ***Afrika v Metzler*** 1997 (4) SA 531 (NmHC) at 539; see also Neethling, Potgieter and Visser ***Delict*** at 18.

216 See ***Neethling's Law of Personality*** at 254.

217 See ***Rhodesian Printing and Publishing Co Ltd v Duggan*** **ao** supra.

218 See in general Neethling, Potgieter and Visser ***Delict*** at 260-261.

2.3.67 The impact of the Constitution has been to make the courts more circumspect in granting interdicts which impose a prior restraint on other fundamental rights (eg freedom of expression) because such constraints are regarded as bearing a heavy presumption against constitutional validity.[219] Otherwise they do not require a different approach from the previous common law position.[220]

iv) Retraction and apology

2.3.68 It was assumed that this Roman-Dutch law remedy had fallen into disuse in South African law. Now the remedy has been revived.[221] This revival can be supported for various reasons, inter alia because it is in conformity with the Bill of Rights, achieving a fairer balance of the fundamental rights to freedom of expression and a good name.[222] It may, in appropriate circumstances, also be "an appropriate remedy" for the protection of the right to privacy. A prompt and unreserved apology could also be a factor affecting the determination of the reasonableness (wrongfulness) of an act,[223] as well as a factor in the assessment of the amount of satisfaction.[224]

2.4 Safeguarding the right to privacy with particular reference to information protection

2.4.1 As stated in Chapter 1 above,[225] information protection is an aspect of safeguarding a person's right to privacy. The so-called traditional principles of privacy protection in the South African law, examined in this Chapter, should, therefore, be fully utilised when regulating the processing of personal information. These principles are based on the ordinary delictual principles as influenced by the Constitution (the principles regarding the actio injuriarum). Information protection should be seen merely as a particular application of those principles.

a) Proposals in Discussion Paper 109

---

219 ***Mandela v Falati*** 1995 (1) SA 251 (W) at 259-60.

220 McQuoid-Mason ***Acta Juridica*** at 236.

221 See ***Mineworkers Investment Co (Pty) Ltd v Modibane*** supra; Cf also ***Dikoko v Makhatla*** supra 258.

222 See Neethling & Potgieter 2003 ***THRHR*** at 333.

223 McQuoid-Mason ***Acta Juridica*** at 236 referring to Burchell ***Personality Rights*** at 496.

224 See Neethling and Potgieter 2003 ***THRHR*** at 333.

225 Para 1.2.2 and further.

2.4.2 In Discussion Paper 109 the Commission submitted that effective information protection could only be achieved through regulation by legislation. [226]

2.4.3 It was argued, firstly, that in view of the inherent conservatism of the courts, as well as the fact that the protection of privacy is, in a sense, still in its infancy in South African law, it would be improbable that the application of the information principles by the courts would occur often or extensively enough in the near future to ensure the protection of personal information. [227] Moreover, the major engine for law reform should be the legislature and not the judiciary, particularly so in this case because the introduction of an information protection regime would not merely involve incremental changes of the common law but radical law reform.

2.4.4 Secondly, the individual should also be able to exercise a measure of active control over his or her personal information.[228] In fact, the traditional protective measures would have little value if there is no active individual control over the processing of personal information. The active control principles, however, differ completely from traditional privacy protection under the actio iniuriarum and therefore are unique in the field of personality protection.[229] The Commission's conclusion was that such measures could therefore be created by legislation only.

b) Evaluation

2.4.5 An overwhelming majority of commentators agreed with the Commission's submission that effective information protection will only be achieved through regulation by legislation. [230] They

---

226 See ***Neethling's Law of Personality*** at 272-3 where these arguments are set out.

227 See also Neethling 2002 ***THRHR*** at 589.

228 See ***Neethling's Law of Personality*** at 278-9 where the following remarks are made: A person should be entitled to -- (i) be aware of the existence of processed data on himself processed by a data controller; (ii) be aware of the purpose(s) for which such data is processed; (iii) be afforded reasonable access to data concerning him stored by a data controller; (iv) be informed by a data controller to which third parties the data was communicated by that controller; (v) procure or effect a correction of misleading data at the data controller; and (vi) procure or effect a deletion of false data, or obsolete data, or data obtained in an unlawful manner, or data not reasonably connected with or necessary for the purpose specified at the data controller.

229 This active control over personal information can nevertheless be based on the common law and Constitutional Court's recognition of the fact that the right to privacy encompasses the competence of a person to determine for himself (that is, control) the destiny of his private facts or the scope of his interest in his privacy (see ***Neethling's Law of Personality*** at 31, 273 fn 64; ***National Media Ltd ao v Jooste*** supra at 271-272; ***Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit NO*** supra at 557).

230 Law Society of South Africa's e-law committee; Zion Christian Church; Lawyers for Human Rights; Dr MDC Motlatla; LOA. Stuart Stoker, Law Reform Commission of Hong Kong referred the Commission to the Hong Kong Personal Data (Privacy) Ordinance (Cap 486) enacted in 1995 at http://www.legislation.gov.hk/eng/home.htm that has been well received in both the public and the private sectors (Privacy Commissioner's web site is http://www.pco.org.hk/).

supported the general tenor of the Bill [231] and regarded it as an important piece of legislation.[232]

2.4.6 It was argued that the proposed Protection of Personal Information Bill, once enacted, will have a very wide ranging effect and will substantially improve information handling as well as reduce unwarranted intrusions into privacy [233] (especially by private entities seeking personal gain).[234] One commentator added that the costs of defending one's right to privacy by way of litigation are so high that the average person cannot afford to do so. Enacting proper legislation will therefore prevent the abrogation of the right to privacy through disuse.[235]

2.4.7 The opinion was expressed that the Commission has made substantial progress in trying to achieve a balance between privacy rights and the requirements for information in normal business operations within the Act, especially as it affects the banking sector. While the requirements imply implementation of new processes and systems and changes to client contracts, it is in line with international standards and to this end, is a necessary piece of legislation.[236]

2.4.8 Overall, respondents agreed that the proposed Bill will bring our country into line with international requirements and developments, and therefore ensure that South Africa is on par with international best practice. This would be especially true in so far as the European Union is concerned which is an important trading partner.[237]

2.4.9 The maturing of the Internet as a tool for business automation over the last ten years, has brought with it a significant change in the expectation of regulated Information Communication Technology ("ICT") related legal requirements. Although it may be a financial strain for companies to comply with these laws, most companies respect the laws that govern them and recognise compliance with legislation as a tool for good governance.[238] The Bill is also regarded as generally

---

231 Telkom; M Chetty; Department of Provincial and Local Government; SNO (Second National Operator) Telecommunications (Pty) Ltd; Vodacom (Pty)Ltd; Innovative Medicines SA (IMSA); Society of Advocates of Kwazulu-Natal; Dr MDC Motlatla; Prof Thaddeus Metz; SAFPS; Board of Health Care Funders; Momentum Health; Sovereign Health.

232 Telkom; Vodacom (Pty)Ltd; Nedbank Ltd.

233 Law Society of South Africa; Land and Agricultural Development Bank; Department of Public Works.

234 Department of Public Works.

235 JD Enraght-Moony.

236 Nedbank Ltd.

237 Law Society of South Africa; Vodacom (Pty)Ltd; MTN; ESKOM.

238 TELKOM.

technologically neutral and clear[239] which puts it in a good position to face the challenges posed by increasingly sophisticated technology.

2.4.10 The opinion was expressed that the proposed Bill is a very important piece of legislation for health researchers in South Africa, and that it will complement the legislation and guidelines already in use to ensure that health research in South Africa does not infringe the privacy rights of citizens.[240]

2.4.11 The Commission was commended for a thorough, comprehensive and well researched Discussion Paper[241] and appreciation was expressed for the fact that the Commission had considered the written comments submitted on the preceding Issue Paper.[242]

2.4.12 The Commission was, however, urged to identify the measures that will meet the objectives of the draft Bill in the least intrusive, proportionate, appropriate and targeted manner.[243]

2.4.13 Some commentators supported the Bill in principle, but were concerned about its implementation in practice. It was argued that many private and public bodies may not have the skills or resources to implement the Bill effectively. Ways should be found to reduce the Bill's administrative burden on such bodies.[244] Compliance with the proposed requirements and administrative procedures will furthermore inevitably lead to an increase in the cost of regulation. The cost of regulation is normally passed through to the consumer and poorer consumers tend to bear a heavier burden. [245] A balance needs to be maintained between the constitutional right to privacy and the constitutional right to freedom of economic activity.[246]

---

239 Law Society of South Africa.

240 SA Medical Research Council.

241 See eg Vodacom (Pty)Ltd; Provincial Administration of Western Cape; Dr MDC Motlatla; SAFPS.

242 Vodacom (Pty)Ltd; SA Medical Research Council.

243 Vodacom (Pty)Ltd; SACOB.

244 Office of the Director-General, Department: Land Affairs.

245 ESKOM.

246 LOA.

2.4.14 It was also mentioned that there is an increase in compliance complexity for businesses that operate globally. A list of principles should be recognised in order to secure the balance between the interests of data subjects and the compliance burden associated with this protection. [247]

2.4.15 A small minority of commentators did not support the legislation on principle.[248] It was argued that any further regulation of industry would undermine business growth, especially in the SMME market and that the matters addressed by this Bill are already appropriately addressed by other legislation (eg PAIA, Employment Equity Act and the like) as well as at common law.[249] It was advised that the Commission should consider amendments to PAIA rather than the enactment of a new Bill.[250]

---

247 SACOB referred to the following: proportionality (information compliance requirements must be proportional to the regulatory objectives sought); consistency (differences between the information compliance requirements intended under the South African legal system and those in force elsewhere should be objectively assessed and where appropriate justified for their impact on business); technology neutrality (information compliance requirements must be technology neutral and stated in terms of functional objectives, rather than in government prescribe solutions); future - proof (compliance requirements should be suitably generic to accommodate future changes in technology); standards setting (standards used in compliance requirements should be market-driven, and determined under an open process in which Business advice on commonly-used business standards and references should be considered); unambiguous (compliance requirements and penalties associated with non-compliance must be clearly expressed); non discriminatory (compliance requirements in laws should not favour government – control over other available compliance products/services); enforcement (businesses must be allowed a reasonable time in which to meet compliance objectives); economic impact/RIA (the cost implications associated with compliance policies and practices must be measured); flexibility (private sector compliance may require different factors to be taken into account (eg sector, size, economic importance); pro-competitive (compliance requirements should avoid creating competitive disadvantages within and outside the national border); pro-trade (compliance requirements should not create obstacles to international trade and introduce entry barriers for foreign products and services); resources & preparedness (before the introduction of compliance requirements, the enforcement agency must be timeously trained and equipped to fulfill its function); interim procedures (a reasonable period must be allowed for businesses to adjust to the compliance requirements); appeal mechanism (an independent appeal mechanism with the power and means to adjudicate in a reasonable timeframe).

248 MFRC; CAPES (Confederation of Associations in the Private Employment Sector) and SAPS.

249 CAPES.

250 SAPS.

c) Recommendation

2.4.16 The Commission recommends that formal legislation on the protection of personal information be enacted as the Protection of Personal Information Bill.[251]

251 See a copy of the Bill contained in Annexure C. In this report the Protection of Personal Information Bill will be referred to as "the Bill" or "POPIA". The acronym POPIA is used notwithstanding the fact that the Bill has not been enacted yet since the Bill has become known as such during the consultation phase and it will prevent confusion if the user name of the Bill, and later the Act, could remain the same during and after the Parliamentary process.

CHAPTER 3: PROPOSED INFORMATION PROTECTION LEGISLATION FOR SOUTH AFRICA: THE PROTECTION OF PERSONAL INFORMATION BILL

3.1 Introduction

3.1.1 As noted in Chapter 2 above,[1] the Commission recommends that legislation should be enacted in the form of a Protection of Personal Information Bill in order to ensure the effective protection of personal information in South Africa.[2] This chapter provides a broad outline of the purposes or objects of the Bill as well as a more detailed discussion on its substantive scope.

3.1.2 The proposed Bill is a general information protection statute, which will be supplemented by codes of conduct for the various sectors and will be applicable to both the public and private sector. It covers both automatic and manual processing and will protect identifiable natural and juristic persons.

3.1.3 The Draft Bill comprises twelve Chapters. Chapter 1 contains certain general provisions including an introductory section setting out the purposes of the Act. Chapter 2 deals with the application of the Act. Chapter 3 sets out the conditions for the lawful processing of personal information (information protection principles) with the exemptions in Chapter 4. Chapters 5, 6 and 7 deal with the various aspects of supervision, namely the establishment and duties of a regulatory authority, notification and prior investigation of processing and codes of conduct. The rights of data subjects in specific circumstances are dealt with in Chapter 8. Chapter 9 provides for transborder information flows. Enforcement, offences and penalties are discussed in Chapters 10 and 11. Finally, the miscellaneous and transitional provisions are contained in Chapter 12. The Bill will be discussed in detail in the chapters to follow.

3.1.4 During the consultation phase, commentators cautioned that consistency in terminology, definitions and concepts (such as privacy and information protection) when used in different laws

---

1 Par 2.4, "Safeguarding the right to privacy with particular reference to information protection".

2 The outline for this report which supports the proposed Bill, has furthermore been set out in Chapter 1.

and regulations, such as the Promotion of Access to Information Act[3] and the Electronic Communications and Transactions Act[4], is of the utmost importance.[5]

3.1.5 In this regard it was furthermore noted[6] that in information protection legislation itself, two approaches can be identified:

a) The EU approach which refers to the "processing" of data. "Processing" is a term that, at the very least, includes the activities of the collection, use and disclosure of personal information; and

b) The North American/Australian approach which refers separately to the "collection", "use" and "disclosure" of personal information.

3.1.6 The Commission has opted for the use of the term “processing”[7] in order to ensure that all relevant activities are included. Other important terms used are “responsible party”[8] (sometimes referred to as the “data controller” in other jurisdictions), “data subject”[9] , “record”[10] and “personal information”.[11] The Commission has furthermore tried to harmonise the definitions

---

3 Act 2 of 2000.

4 Act 25 of 2002.

5 Vodacom (Pty) Ltd.

6 IMS.

7 **"processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, degradation, erasure or destruction of information.

8 **"responsible party"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

9 **“data subject”** means the person to whom personal information relates.

10 **“record”** means any recorded information -

(a) regardless of form or medium, including any of the following -
  (i) writing on any material;
  (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment (whether hardware or software or both), or other device; and any material subsequently derived from information so produced, recorded or stored;
  (iii) label, marking, or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
  (iv) book, map, plan, graph, or drawing;
  (v) photograph, film, negative, tape, or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced;
(b) in the possession or under the control of a responsible party;
(c) whether or not it was created by a responsible party; and
(d) regardless of when it came into existence.

11 **“personal information”** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to -

in the Bill with similar definitions in other existing information legislation.

3.2 Purposes/Objects of the Bill

3.2.1. A 'purposes' or 'objects' clause of a Bill outlines the underlying purposes of the legislation and may facilitate the interpretation and understanding of the detailed provisions of the legislation. Currently the Interpretation Act [12] does not provide any guidance on the interpretation of such a clause. However, the South African Law Reform Commission has recently published a Discussion Paper[13] for information and comment in which the issue of pre-ambles and objects clauses has been discussed. Clause 7 of the Interpretation of Legislation Bill, 2008, proposed in this Discussion Paper provides that any interpretation of legislation in terms of an Act must be consistent with the purpose and scope of the legislation.[14] Since 1994 the inclusion of express purpose provisions in legislation has become fairly common in South Africa.[15]

3.2.2 An express declaration of the objects of a Bill is especially important in principled-based legislation such as the present Bill because principles require constant interpretation and application to particular contexts and an objects clause provides a reference framework to assist

---

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
b) information relating to the education or the medical, financial, criminal or employment history of the person;
c) any identifying number, symbol, email address, physical address, telephone number or other particular assigned to the person;
d) the blood type or any other biometric information of the person;
e) the personal opinions, views or preferences of the person;
f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g) the views or opinions of another individual about the person; and
h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

12 Interpretation Act 33 of 1957.

13 South African Law Reform Commission ***Statutory Revision: Review of the Interpretation Act 33 of 1957*** Project 25 Discussion Paper 112 September 2006.

14 The proposed section 7 reads as follows:

7.(1) Legislation must be interpreted -
(a) as applying to circumstances as they arise; and
(b) in accordance with the contemporary meaning of its language.
(2) Any interpretation of legislation in terms of subsection (1) must be consistent with the purpose and scope of the legislation.

15 See eg section 1 of the Labour Relations Act 66 of 1995 and section 2 of the National Water Act 36 of 1998.

with this.[16]

a) Proposals in Discussion Paper

3.2.3 The Protection of Personal Information Bill included in the Discussion Paper[17] contained a clause setting out the objects of the legislation.[18]

3.2.4 The stated objects were to safeguard the processing of all personal information while at the same time balancing the right to privacy with the public interest in the free flow of information and the right of access to information. The importance of supporting new technology being developed continuously was also underscored as was the promotion of awareness of the Bill.

b) Evaluation

3.2.5 In general, commentators agreed with the objects and principles of the legislation and reserved their comments to points of detail only. See also the discussion in Chapter 2 above of the submissions received on the need for privacy legislation. The hope was expressed [19] that any

---

16 Australian Law Reform Commission ***Review of Australian Privacy*** Discussion Paper 72 September 2007 (hereafter referred to as ***ALRC Discussion Paper***") at para 3.86.

17 Hereafter referred to as "the Discussion Paper Bill".

18 Clause 1 of Chapter 1 of the Discussion Paper Bill reads as follows:

Objects of Act

1.(1) The objects of this Act are –

(a) to give effect to the constitutional right to privacy-

(i) by safeguarding a person's personal information when processed by public and private bodies;
(ii) in a manner which balances that right with any other rights, including the rights in the Bill of Rights in Chapter 2 of the Constitution, particularly the right to access to information;
(iii) subject to justifiable limitations, including, but not limited to effective, efficient and good governance and the free flow of personal information, particularly transborder transfers.

(b) to establish voluntary and mandatory mechanisms or procedures to protect personal information in order to contribute to economic and social development in an era in which technology increasingly facilitates the circulation and exchange of information; and

(c) generally, to promote transparency, accountability and effective governance of all public and private bodies by, including, but not limited to, empowering and educating everyone to understand their rights in terms of this Act in order to exercise their rights in relation to public and private bodies;

(2) When interpreting a provision of this Act, every court must prefer any reasonable interpretation of the provision that is consistent with the objects of this Act over any alternative interpretation that is inconsistent with these objects.

19 SAFPS.

regulations that may emanate from this legislation would be the subject of debate between relevant role players prior to their publication. The necessity of including Clause 1(2) was questioned.[20]

c) Recommendation

3.2.6 In evaluating the comments received the Commission is satisfied that the inclusion of an objects clause in the proposed Bill is warranted. The objects clause should make it clear that the main aim of the legislation is to protect the constitutional right to privacy with regard to the processing of personal information. However, it should also expressly recognise that the right to privacy is not an absolute right and that the Bill is intended to provide a framework within which the right to privacy should be balanced against other rights, particularly the right of access to information.

3.2.7 The objects should, furthermore, include the establishment of information protection principles which will provide the minimum threshold requirements for the lawful processing of personal information in harmony with international standards. Specific reference to international standards will imply that relevant international instruments and jurisprudence may be consulted in order to assist when interpreting and applying the legislation.

3.2.8 Finally, the Bill should ensure the rights and remedies of persons to protect themselves against the unlawful processing of their personal information by the institution of a regulatory authority to monitor, supervise and enforce the rights set out in the Bill.

3.2.9 The Commission recommends that the objects of the Bill be set out as follows:

Purpose of the Act

20 ESKOM Holdings Ltd; Department of Communications.

2.(1) The purpose of this Act is -

(a) to give effect to the constitutional right to privacy, by safeguarding a person's personal information when processed by responsible parties, subject to justifiable limitations that are aimed at -

(i) balancing the right to privacy against other rights, particularly the right of access to information;

(ii) protecting important interests, including the free flow of information within the Republic and across international borders;

(b) to regulate the manner in which personal information may be processed, by establishing principles, in harmony with international standards, that describe the minimum threshold requirements for lawful processing of personal information;

(c) to provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(d) to establish voluntary and compulsory measures, including an Information Protection Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act;

(2) This Act must be interpreted in a manner that gives effect to the purposes of the Act set out in subsection (1).

3.3 Substantive scope of the proposed legislation

a) Proposals in Discussion Paper

3.3.1 The Commission's preliminary proposals as set out in the Issue Paper[21] and confirmed in the Discussion Paper,[22] were that the investigation into the protection of personal information should include:

---

21 Issue Paper 24.

22 South African Law Reform Commission **Privacy and Data Protection** Project 124 Discussion Paper 109 October 2005 (hereafter referred to as "the Discussion Paper").

a) automatic/electronic and manual/paper files;
b) information pertaining to both natural and juristic persons;
c) information kept by both the public and the private sector;
d) sound and image information;
e) professional information;
f) sensitive information; and
g) critical information to the extent indicated.

3.3.2 Personal information kept in the course of a purely personal or household activity and de-identified information were excluded. Provision was also made for responsible parties to approach the Commission for the exemption from specific information principles under specified circumstances. Comment was invited in all instances.

3.3.3 Some respondents to the two discussion documents[23] indicated that the scope of the inquiry and the legislative efforts to follow should pertain to all the areas listed.[24] Others felt that only information kept in the course of personal or household activity should be excluded.[25] A third group was of the opinion that information on household activity and critical information should be excluded.[26] A proposal was also put forward by a health organization[27] to the effect that a distinction should be drawn between personal information and professional information (which would also include provider information) and that anonymising or de-identified information should be excluded from the scope of the legislation. Three respondents[28] presented arguments for their organisations to be accommodated as separate categories to be excluded completely from the Bill.

3.3.4 Specific arguments were raised in each case and will be discussed under the following headings:

---

23 Strata; Financial Services Board.

24 The Financial Services Board stated that the proposed law should be as wide as possible to prevent a situation where a number of different laws have to be passed resulting in a fragmented situation which could impact negatively on some of those laws where interpretation thereof has to take contextual considerations into consideration. The proposed law should then cover all personal information in whatever format it is held or may be distributed and should also cover all methods of collecting, distributing and processing thereof.

25 The Internet Service Providers' Association; Gerhard Loedolff, Corporate Consultant (Business Assessment) Eskom; SAHA; Vodacom (Pty) Ltd; The Banking Council; Medical Research Council and Private Health Information Standards Committee. X-rays as image data should, for instance, also be included.

26 Liberty; Society of Advocates of Natal; SAFPS; SAPS.

27 IMS Health.

28 Ombudsman for Long-term Insurance, Chief Registrar of Deeds; SAFPS.

* automatic and manual files (para 3.3 (b) (i))
* existing and future information bases (para 3.3 (b) (ii))
* sound/image information (para 3.3 (b) (iii))
* natural v juristic persons (para 3.3 (b) (iv))
* public v private sector information (para 3.3 (b) (v))
* critical information (para 3.3 (b) (vi))
* special personal information (sensitive information) (para 3.3 (b) (vii))
* household activity (para 3.3 (b) (viii))
* anonymised/ de-identified information (para 3.3 (b) (ix))
* professional information (including provider information) (para 3.3 (b) (x))
* information processed for journalistic, artistic of literary purposes (para 3.3(b)(xi))
* information in the public domain (par 3.3 (b) (xii))

b) Evaluation

(i) Automatic and manual files

3.3.5 Respondents[29] unanimously supported the view of the Commission that information protection legislation should incorporate both manual and electronic files,[30] in accordance with the EU Directive.[31] [32]

3.3.6 It was stated that all records should be incorporated regardless of the medium or form which they take,[33] especially since offline paper-based databases are as important as electronic

---

29 The Internet Service Providers' Association; Financial Services Board; Neo Tsholanku, Eskom Legal Department; SABC; LOA; ENF for Nedbank Ltd; Vodacom (Pty) Ltd; Nedbank Ltd; The Banking Council.

30 From the definition in the Open Democracy Bill [B67-98] of "records" as "recorded information regardless of form and medium" (cl 1(1)) it is evident that both manual and computer records were intended to be included in the scope of that Bill.

31 Article 3 of the EU Directive stipulates that the Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

32 It should, however, be noted that in the Electronic Communications and Transactions Act, Act 25 of 2002 (hereafter referred to as "ECT Act") paper based data bases are not included. The Act defines "electronic transactions" as follows:

"electronic" includes created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic, optical or any similar means;
"transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-Government services.

33 SABC.

databases. Much information in the long-term insurance industry is, for instance, retained electronically. Such electronic data may be collected by automatic systems, such as telephonic call centres and the like, but may be manually captured by data operators on computer systems. In addition, there is a great deal of information, which is retained in paper form.

3.3.7 Caution should, in any case, be exercised when making reference to "automatic" and "manual" files. All information which is saved in files, is done so because of prior instructions given "manually". For instance, any "automatic" electronic system will have had prior "manual" programming.[34] These phrases are therefore inappropriate. On the other hand, a "manual" file is handled by "hand" but the definition does not preclude some sort of "automatic" processing to compile a manual file.[35]

3.3.8 With current and future technological advances, there is already a substantial use of electronic and digital databases. This is likely to increase exponentially as the use of digital technologies become more pervasive. Already personal and private information is being stored in forms not provided for in current legislation. For instance, the use of biometrics (finger print scanning, retina scanning and facial image scanning) is a reality of modern life. See also the discussion on sound and image information below in para 3.3 (b)(iii).

3.3.9 The Commission confirms its proposal as set out in the discussion papers and submits that both manual and automatic files should be dealt with in the legislation. However, it is decided that, in accordance with article 3 of the EU Directive, [36] information processed by non-automatic means should only be included where the information forms part of a filing system or are intended to form part of such a system. See clause 3 set out at 138 below.

(ii) Existing and future information bases (grandfathering[37])

---

34 LOA.

35 Liberty.

36 See footnote 31 above.

37 A grandfather clause is an exception that allows an old rule to continue to apply to some existing situations, when a new rule will apply to all future situations.

3.3.10 In their responses some commentators argued that the proposed "Privacy Act" should only apply from the date of promulgation. One institution[38] indicated that it has a database of material that stretches back to the first decade of the previous century and indicated that it would be prohibitively costly and expensive to have to categorise and audit the material that it has in its archives.

3.3.11 The concern was furthermore expressed[39] that insurers would no longer be able to source new clients from existing consumer or affinity databases, where consent from the data subject has not been obtained and this would therefore have a severe impact on the insurance direct marketing industry. [40] The Commission acknowledged that insurers have large client databases, which have been generated over decades.

3.3.12 In discussing these comments it should, at the outset, be noted that the proposed Bill does not make provision for a general grandfather clause. The definition of "record",[41] like that in the Promotion of Access to Information Act, stipulates that the Bill applies to a record regardless of when it came into existence. All the provisions of POPIA, including the consent principle, will therefore apply to all personal information held by an organisation, regardless of when it was collected.

3.3.13 However, POPIA is not a consent-driven Bill.[42] This means that express consent is only one of the possible ways of complying with clause 10 of the Bill and it does not necessarily follow that a responsible party must seek the express consent of established customers to the continued processing of personal information.

3.3.14 In Canada the Office of the Privacy Commissioner published a Fact Sheet indicating best practices for dealing with pre-legislation information.[43] The following guidelines may also be useful in the South African context:

---

38 SABC.

39 SAIA; LOA.

40 See also the full discussion on direct marketing in Chapter 5.

41 Clause 1 of the Bill.

42 See the full discussion on clause 10 in Chapter 4 below.

43 Office of the Privacy Commissioner of Canada "Best Practices for dealing with pre-PIPEDA personal information (grandfathering)" Fact Sheet accessed at http://www.privcom.gc.ca/fc-fi/on on 21 February 2008.

a) Destroying or erasing older files, as is the practice during the ordinary course of business, may be the most appropriate and straightforward way to deal with existing files. Under Principle 3 of the Bill personal information should only be retained for as long as it is necessary for the fulfilment of the purposes for which it was collected. Information, furthermore, becomes outdated very quickly since the personal information of persons change continuously and it is simply not good business practice to rely on outdated information. Reasonable minimum and maximum retention periods for handling of customer files in future should be set.

b) The extent to which a responsible party is obliged to seek express consent from established customers depends on several considerations:

   (i) Whether the responsible party made a reasonable effort to inform the customer of its purposes at the time of collecting the personal information;

   (ii) Whether the information is still being used or disclosed, and if so, whether it is being used or disclosed for the same purposes for which it was collected;

   (iii) Whether the information is being used or disclosed for unidentified secondary purposes; and

   (iv) Whether the customer would reasonably expect the organisation to continue using or disclosing the information for its current purpose.

These principles, of course, apply as much to a responsible party's established customers as to its new customers.

3.3.15 The Commission confirms its previous decision not to include a general grandfathering clause in the Bill. It is the Commission's opinion that many of the problems regarding pre-legislation information can be solved through the gradual implementation of the privacy principles according to accepted business practice. Transitional arrangements have, furthermore, been introduced in clause 103 of the Bill in order to provide the responsible parties with enough time to comply with the provisions of the Bill. It should also be noted that the Bill has taken five years to develop, during which time responsible parties have already had the opportunity of introducing good business practice in their organisations where necessary.

(iii) Sound/image information

3.3.16 There appears to be consensus amongst respondents that the investigation should cover both sound and image information,[44] given the advancement of information technology and the use of sound and image information as means of identification and verification of the interaction of individuals.[45] There is clearly a lacuna in the existing guidelines and legislation in South Africa with regard to this type of information.[46]

3.3.17 Sound and image information should include paper data, sound, video, but also other forms of electronic information such as ECGs, EEGs, CAT-scans, etc.[47]

3.3.18 The Commission recommends the inclusion of sound/image information in the scope of the legislation. See clause 3 set out below at 138 as well as the definition of "record" in clause 1 of the Bill.

(iv) Natural v juristic persons

3.3.19 In the discussion papers the following points were made:

a) The South African courts apply the common law principles developed for the protection of the privacy of natural persons also to juristic persons:[48]

* In ***Financial Mail (Pt) Ltd v Sage Holdings Ltd***[49] the court expressed the view that the actio injuriarum should be available for a violation of the privacy of a juristic person even if one cannot, in the case of a juristic person, speak of feelings being

---

44 The Internet Service Providers' Association; Financial Services Board; Neo Tsholanku, Eskom Legal Department; ENF for Nedbank Ltd; LOA; The Banking Council.

45 ENF for Nedbank Ltd.

46 The Banking Council.

47 LOA.

48 See ***Motor Industry Fund Administrators (Pty) Ltd v Janit*** supra at 60 (confirmed on appeal: 1995 (4) SA 293 (A)) and ***Financial Mail v Sage Holdings*** supra 462-463***; Neethling's Law Of Personality*** 32 fn 336, 68ff, 71-73; for a discussion of these cases see Chapter 2 above as well as the Nadasen submission.

49 Supra.

outraged or offended. The basis for this protection is that privacy, like reputation (fama), can be infringed without injured feelings.[50]

* The court in ***Janit v Motor Industry Fund Administrators (Pty) Ltd***[51] affirmed the view expressed in the *Sage Holdings* case that a company would be entitled to regard the confidential oral or written communications of its directors and employees as sacrosanct and would, in appropriate circumstances be entitled to enforce the confidentiality of such communications. Interestingly, in the *Janit* case, the view was articulated that the theft of confidential discussions of a board of directors constituted an unlawful invasion of their privacy and any disclosure of such information, would itself constitute an invasion of the respondent's privacy.[52]

Furthermore, where another person, who was aware that the information was unlawfully obtained and that they contained private and confidential discussions of the respondent's directors, helped himself to that information, such a person thereby violated and infringed their right to privacy.[53]

b) The Constitution sets out the applicability of the Bill of Rights to a juristic person in s 8(4) of the Constitution which states:

> A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person.

This means that juristic persons can possess only the rights which are compatible with their nature or naturally apply to them.[54]

---

50 At 462; ***Neethling's Law of Personality*** at 71; Neethling J "Data Protection and Juristic Persons" (2008) 71 ***THRHR*** (hereafter referred to as "Neethling "Data Protection and Juristic Persons"): Privacy and identity can be infringed without the victim being aware of it.

51 1995 (4) SA 293 (A).

52 At 303.

53 At 305 B-D.

54 See Neethling "Data protection and Juristic Persons" at 71.

c) In **Investigating Directorate: Serious Economic Offences ao v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty) Ltd ao v Smit NO ao**[55] the Constitutional Court held that juristic persons enjoy the right to privacy, but is not protected to the same extent as natural persons since juristic persons are not the bearers of human dignity.[56] The level of justification for any particular limitation of the right would have to be judged in the light of the circumstances of each case.

d) Internationally few countries provide privacy protection for juristic persons.[57] However, there seems to be a movement towards broader protection.[58]

e) In each case one would have to ascertain whether appropriate circumstances exist for companies to rely on to protect their privacy interests.

f) It would appear that only natural persons (ie not juristic persons) are protected by the provisions of the Promotion of Access to Information Act,[59] since "personal information" is defined[60] as information about an identifiable individual. [61]

---

55 Supra.

56 Langa DP at 557, inter alia said:

> The right to privacy is applicable, where appropriate, to a juristic person... Juristic persons are not the bearers of human dignity. Their privacy rights, therefore, can never be as intense as those of human beings. However, this does not mean that juristic persons are not protected by the right to privacy. Exclusion of juristic persons would lead to the possibility of grave violations of privacy in our society, with serious implications for the conduct of affairs.... Juristic persons therefore do enjoy the right to privacy, although not to the same extent as natural persons.

57 See discussion on the OECD and EU prescripts below; See also the discussion in European Union Art 29 Data Protection Working Party ***Opinion 4/2007 on the concept of personal data*** adopted on 20 June 2007 at 23.

58 See discussion below.

59 Roos at 499.

60 The definition of "personal information in PAIA reads as follows:

> "Personal information" means information about an identifiable individual, including, but not limited to-
>
> a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
> b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
> c) any identifying number, symbol or other particular assigned to the individual;
> d) the address, fingerprints or blood type of the individual;
> e) the personal opinions, views, or preferences of the individual, except where they are about another individual, or about a proposal for a grant, an award or a prize to be made to another individual;
> f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature of further correspondence that would reveal the contents of the original correspondence;
> g) the views or opinions of another individual about the individual;
> h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
> i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.

3.3.20 Most respondents to the discussion papers[62] agreed that the investigation should be aimed at protecting both the fundamental rights of natural persons (in particular their right to privacy) and the legitimate interests of juristic persons. [63]

3.3.21 In one submission[64] it was, however, argued that the inclusion of juristic persons in this way may be unconstitutional. It was argued that the incorporation of juristic bodies in privacy legislation would not conform to the Constitution as such an inclusion would not be reasonable and justifiable in an open and democratic society [65]

3.3.22 Another commentator[66] stated that excluding juristic entities from the ambit of the Bill would not mean that juristic entities are not entitled to protection of privacy. They would remain subject to the current common law as expanded by the courts. However, public policy does not demand their inclusion in the Bill. The practicality and administrative costs of compliance will outweigh any benefits. The argument was also posed[67] that the statutory privacy protections do not usually apply to corporations and businesses.[68]

3.3.23 The fact was reiterated that these statutes represent a response to a perceived threat caused by increasing computerisation and the ability to process and aggregate information, rather than an attempt to protect a human right. It is therefore not a desire to protect the

---

61 The definition of “personal information” in the **Electronic Communications and Transactions Act** is based on that of **PAIA**. It is furthermore interesting to observe that PAIA lists amongst the grounds on which the refusal to grant access to the records of private persons, the mandatory protection of the privacy of a third party who is a natural person. No such exclusionary provision is made in respect of juristic persons.

62 Internet Service Providers’ Association; Liberty; Sagie Nadasan; Sanlam Life: Legal service; Financial Services Board; Neo Tsholanku, Eskom Legal department; ENF for Nedbank Ltd; SABC; LOA; The Banking Council; SNO (Second National Operator) Telecommunications (Pty) Ltd; Law Society of South Africa; Innovative Medicines SA (IMSA); SA Medical Research Council; Contemporary Gazette, Pieter Stassen; Nedbank Ltd.

63 See also the discussion in subpara (x) below regarding professional information.

64 IMS.

65 Michalsons for IMS Health.

66 Standard Bank.

67 Michalsons for IMS Health.

68 In this respect the Commission was referred to the Ontario Commissioner who has consistently held that information about a sole proprietorship is just that: information about the sole proprietorship and not about the principal of that proprietorship. In Order 1633, former Ontario Information and Privacy Commissioner Sydney Linden wrote:
“Had the legislature intended "identifiable individual" to include a sole proprietorship, partnership, unincorporated associations or corporation, it could and would have used the appropriate language to make this clear. The types of information enumerated under subsection 2(1) of the Act as "personal information" when read in their entirety, lend further support to my conclusion that the term "personal information" relates only to natural persons.”

purported "privacy rights" of companies that is at stake but rather the concern to limit the uncontrolled uses of information technology. See also the discussion on the position in the USA in Chapter 9 below.

3.3.24 In a contribution received from the Credit Bureaux Association[69] it was argued that whilst it may be understood why a juristic person should be entitled to the broad right to privacy which would include not having its property searched, its possessions seized or the privacy of its communications infringed, it is difficult to understand why a juristic person should be entitled to the specific right of personal information privacy. The cases cited above [70] could be interpreted accordingly. It could therefore be argued that the nature of the specific right to personal information privacy is such that it only envisages protection being afforded to information about natural persons. If the right to personal information is extended to juristic persons it should be to the extent that it is necessary to protect the confidential, oral and written communications of directors, employees, or any other natural person associated with the juristic person. It should, however, not be extended to include information identifying and describing the juristic person, nor information about a juristic person's financial and legal standing, nor natural persons who exercise management and control of the juristic person.

3.3.25 It was also mentioned that, from a practical viewpoint, no limitations should be placed on the flow of information about SMMEs and BEE companies to facilitate business to business transactions between such companies and other businesses. The "business to business" transaction environment is different form the "business to consumer" transaction environment and trade may be hindered if restrictions are imposed on the flows of commercial data when granting credit to businesses, procurement and the utilisation of marketing information.

3.3.26 The Commission was furthermore (in more than one submission) referred to two studies dealing with the question whether juristic persons should be included in the scope of the privacy legislation. The first was the European Commission study on the protection of the rights and interests of juristic persons with regard to the processing of personal information relating to such persons[71] and the second an article written by S Nadasen entitled "Data Protection for

---

69 Adv Ashina Singh "CBA Submission RE: Draft Bill for the Protection of Personal Information" dated 25 May 2007.

70 See para 3.3.19 above.

71 Korff D for the Commission of the European Communities ***EC Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons***(Study Contract ETD/97/B5-9500/78) Final Report by Douwe Korff (contractor) (hereafter referred to as " Douwe Korff **EC Study**") accessed on 5/4/2004 at http://europa.eu.int/comm/internal_market/privacy/docs/studies/legal_en.pdf.

Companies: Natural v Juristic Persons: Privacy and More".[72] Both will be discussed in some detail below.

3.3.27 The report by Douwe Korff contains a comprehensive discussion of the international and, more specifically, the European position regarding the protection of personal information of juristic persons.

3.3.28 Korff, after surveying the law and practice in some European countries, observes the following:

(a) In some countries information protection is seen as deriving from the "right to (human) personality" or to "human dignity" or "honour" or to personal or family "characteristics" – the aim being the protection of privacy, or the private life or private sphere of individuals. From this perspective, companies and other juristic persons, not possessing human personality, human dignity or family characteristics do not require privacy or a protected private sphere. Accordingly, not only should companies or juristic persons be open to scrutiny, but the extension of information protection to them is misconceived.

(b) However, other countries, while recognising the relationship between information protection and these classical rights, identify other "legitimate interests" affected by information processing. These interests, which are deemed worthy of protection, include the interest of everyone in "significant decisions" affecting them being taken on factual, accurate and relevant information, or the related interest in being able to challenge decisions reached on the basis of erroneous or irrelevant information. Some countries have seen the adoption of constitutional provisions which to some extent recognise information protection as a new, sui generis right, linked with, but distinct from, and wider than, privacy.[73]

3.3.29 The international information protection instruments remain somewhat ambiguous about

---

72 Nadasen S "Data Protection for Companies: Privacy and More" **Insurance and Tax** Sept 2003 also submitted by Dr Nadasen as part of the submission from Sanlam Life.

73 The collection of information on race, religious-, philosophical- or political beliefs or trade union membership could affect the freedom of religion or belief, the freedom to educate one's children in accordance with one's beliefs, the freedom of association and the freedom from discrimination of both the individual and the group. The fact that information protection was increasingly seen as a *sui generis* right, related to but distinct from Articles 8 and 10 of the ECHR, was one of the main reasons for drafting a separate international legal instrument in the field: the Council of Europe Data Protection Convention.The other reason was that the Human Rights Convention is open only to Member States of the Council of Europe, whereas the Data Protection Convention was drafted in such a way as to allow non-European States too to become a party.

the nature, objects and aims of information protection.[74] They link information protection "in particular" with the right to privacy and freedom of expression, but they also acknowledge that these concepts do not suffice to define the interests at stake; that other interests - some of them equally fundamental in a State under the rule of law - are also affected; and that these wider interests, at least, may also pertain to juristic persons.[75] The ISDN Directive[76] was the first Directive to give formal expression to this increasingly explicitly recognised fact, and also confirmed that, in certain contexts, a distinction between natural and juristic persons is difficult to make or justify in practice.[77]

3.3.30 The experience of EU Member States shows that the making of an absolute distinction between natural and juristic persons (with the first being given full protection and the latter none) is difficult to defend on rational or practical grounds. Some collective bodies composed of individuals, such as partnerships in England, lack independent juristic status but may

---

74 As the Explanatory Memorandum to the OECD Guidelines puts it:
"Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data." (Explanatory Memorandum, para. 31)
Thus, the Council of the OECD left it at the above acknowledgment that it might be "advisable" to extend a measure of data protection to legal persons, in some instances: the OECD Guidelines themselves do not anywhere envisage their application to legal persons, even as an option. The UN Guidelines, while still very tentative, go somewhat further in that they themselves state, in Principle 10, that: 4 The OECD Guidelines say that the data must be "complete".
"Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals."
In Europe, there has been greater willingness to explicitly acknowledge the legitimacy of extending data protection to legal persons as such - even if the choice of whether to do so was initially left to individual States. Thus, the Council of Europe Convention stipulates, in Article 3(2):
"Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:
a. ...
b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality."
Article 2(a) of the EU Directive defines personal data as information relating to a natural person but similarly recognises the legitimacy of extending data protection by stipulating that:
"[the existing legislation in the Member States] concerning the protection of legal persons with regard to the processing [of] data which concerns them is not affected by this Directive" (Preamble (24)).

75 Whatever the limitations on the right to "private life" (further discussed below), the wider "legitimate interests" affected by unfettered data processing, noted above, are not intrinsically limited to "natural persons": "legal persons" too have an interest in how their creditworthiness is assessed, in fairness in legal proceedings, and non-discrimination.

76 Directive 97/66/EC of the European Parliament and of the Council dated 15/12/97 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. Referred to as the ISDN Directive. Replaced by 2002/58/EC dated 12/7/2007.See para 5.1.37 below.

77 This trend has culminated (for now) in the formal, mandatory extension of the ISDN Directive to such persons:
"... in the case of public telecommunications networks, specific legal regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of natural persons ***and legitimate interests of legal persons***, in particular with regard to the increasing risk connected with automatic storage and processing of data relating to subscribers and users" (Preamble (7)). This principle was contained in Preamble 7 and 12 of Directive 2002/58/EC. However, it was also indicated that the Directive does not impose an obligation on member states to extend the application of the EU Directive to juristic persons.

nevertheless operate as a distinct economic entity. In other cases, eg. as regards financial transactions, information on juristic persons can be impossible to separate from information on individuals.

3.3.31 Even when juristic and natural persons can be distinguished, the distinction is, for information protection purposes, often not necessarily the most appropriate one to make. Some 'natural persons' (eg one-person businesses), in some respects, require less protection than other 'natural persons' (eg consumers), and some 'juristic persons' (eg religious, political, or trade union associations) require more protection than other 'juristic persons' (eg large corporations). Indeed, in some circumstances, some 'natural persons' may require less protection than some 'juristic persons'; and the absence of any protection for some 'juristic persons' could even, in some circumstances…breach international human rights law.

3.3.32 Therefore, three groups are identified among the Member States of the European Community, namely: states which are of the view that information protection is inherently limited to natural persons; those who are of the view that a measure of information protection should be extended to juristic persons as a matter of principle and, states which appreciate arguments in favour of the latter position but which have refrained from extending protection in this way for practical reasons.

3.3.33 Korf concludes that the crucial point for the present study is that these wider interests affected by information processing – and the corresponding guarantees in the Human Rights Convention and the general principles of Community Law – cannot be said to be inherently limited to natural persons. It was recognition of these wider issues, and in particular of the fact that the interests protected by information protection are not exclusive to natural persons (rather than a 'purely formalistic' approach), which in Europe led Austria, Denmark, Iceland, Italy, Luxembourg and Switzerland to extend their laws to juristic entities.[78]

3.3.34 A number of distinct areas in which the extension of information protection to juristic persons has the most immediate, practical effect have been identified and they are as follows:

a) The protection of the interests of juristic persons concerning the processing of business information by credit reference agencies and the like;
b) The protection of the interests of juristic persons in relation to the processing of

78 See also the Argentinian position.

information on users and subscribers of telecommunications services;

c) The protection of the interests of juristic persons relating to the processing of business information supplied by them to State institutions for statistical purposes;[79]

d) The protection of the interests of juristic persons relating to direct marketing;

e) The protection of the interests of juristic persons concerning the processing of information which is used by public and private bodies to take decisions which 'significantly affect' them;[80]

f) The scope of the protection afforded to one-person businesses; and

g) Information held by various persons and bodies which collect data, including not only financial information concerning the juristic person, but for instance the corporate strategies of those juristic persons, the number of employees employed by them, the identities of those employees, the status of those employees within the juristic person and also the financial remuneration provided to those employees.[81]

3.3.35 Since the extension of information protection to juristic persons by some, but not all, Member States could be problematic, Korff recommended (a recommendation reiterated in the EU Study on the Implementation of the Data Protection Directive in 2001) that consideration be given to extending specific elements of the protection of the Directive to juristic persons in specific areas to all European countries.

3.3.36 In his article referred to above, Nadasen, discusses the report of Korff and then specifically considers what could constitute "appropriate circumstances" or situations in South African law (as required in the *Hyundai* case) which companies could rely on to protect their interests by an appeal to the protection of their privacy as it may relate to information protection. In discussing the case law, he reiterates the view that juristic persons have a right to privacy,[82]

---

79 Companies are required to provide ever-increasing, detailed information on their financial, environmental and other activities, under national or Community legislation. While the need to provide such information is generally accepted (although sometimes somewhat grudgingly), concern has been raised about the proper use of such information. In particular, certain data, provided for eg statistical purposes could, in the hands of a competitor, be used to the detriment of the undertaking which provided the data, and thus affect competition. It has also been noted that the State agencies to which such data is sent are increasingly privatised, and thus have a commercial interest in using (or indeed selling) the data.

80 The LOA argued that if financial information regarding natural persons is protected, then the financial information of juristic persons should also be protected.

81 LOA.

82 ***Sage Holdings Ltd ao v Financial Mail (Pty) Ltd ao*** supra and ***Motor Industry Fund Administrators(Pty) Ltd ao v Janit ao*** supra. See discussion above.

but that the extent of the protection has to be judged in each case[83] and acknowledges the fact that a company's right to privacy may be limited for several reasons.[84]

3.3.37 Nadasen therefore concludes that the question of whether or not privacy could be extended to include the protection of the carrying on of business, must depend on the

---

83 ***Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit NO*** supra.

84 In ***Bernstein ao v Bester ao NNO*** 1996 (2) SA 751(CC); 1996 (4) BCLR 449 (CC) the Court suggested that the public's interest in ascertaining the truth surrounding the collapse of a company, a liquidator's interest in a speedy and effective liquidation of a company and the creditors' and contributors' interests in the recovery of company assets could constitute a legitimate limitation to personal privacy.

Similarly, in ***President of the RSA v South African Rugby Football Union*** 1999 (4) SA 147 (CC) it was noted that in terms of the Commissions Act a witness before a commission may be asked questions or required to produce documents which will limit his or her right to privacy. The court cautioned that in any particular case, the questions put and the documents sought must be relevant to the scope of the commission's investigation and that the investigation must be a matter of public concern – for the court, if the questions asked or documents requested sought were relevant then, "in all probability an invasion of privacy will be permissible".

Furthermore, in ***Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit NO*** supra, the court affirmed that in the proportional analysis of competing interests, in limiting the right to privacy, a balance had to be struck between the interests of the individual and that of the State, a task that lie at the heart of the inquiry into the limitation of rights.

In ***Gardener ao v Walters NNO*** (in re ***Ex parte Walters ao NNO***) 2002 (5) SA 796 (C) the respondents, the joint liquidators of a public company in liquidation, had obtained orders for the issue of letters of request to the Royal Court of Jersey to recognise their appointment as duly appointed liquidators and to allow them to institute proceedings in Jersey for the investigation and recovery of the company's assets. The applicants contended, *inter alia*, that the order of the Jersey Court giving effect to the letters of request could affect their privacy. In dismissing the appeal, the court characterised the appeal to privacy as one which " borders on the grotesque". Not only was a proper and thorough investigation warranted, but the appeal to privacy, in the courts view, was -

> 'illustrative of the attitude of so many managers of companies who seem to believe that they should be allowed to walk away scot-free from financial disasters which they have created'.

Relying on the *Bernstein* case, the court in ***Shelton v Commissioner for the SARS*** 2000 (2) SA 106 (E) concluded that -

> " …It is apparent from the judgment that the concept of privacy does not extend to include the carrying on of business activities."

Nadasen mentions that the above statement could arguably be used to sustain the contention that, while a juristic person does enjoy a measure of privacy, that protection does not extend to include the carrying on of business activities. The Constitutional Court said the following in the ***Bernstein*** case -

> Examples of wrongful intrusion and disclosure which have been acknowledged at common law are entry into private residence, the reading of private documents, listening to private conversations, the shadowing of a person, the disclosure of private facts which have been acquired by a wrongful act of intrusion, and the disclosure of private facts contrary to the existence of a confidential relationship. These examples are all clearly related to either a private sphere, or relations of legal privilege and confidentiality. *There is no indication that it may be extended to include the carrying on of business activities.* " [emphasis added]

Nadasen submits that the above passage lists examples of the protection of privacy which have been afforded at common law and is not a statement of law that privacy cannot be extended to include the carrying on of business. Reading the sentence within the context of the entire paragraph, it is submitted that the meaning to be ascribed is the following: there is no indication *in the common law* that it may be extended to include the carrying on of business. Furthermore, the Constitutional Court did not say that the application of the common law leads to the conclusion that "it *cannot* be extended to include the carrying on of business activities". The Constitutional Court, it is submitted was only summarising the application of the common law to the protection of privacy.

He therefore concludes that, with respect, the court in the ***Shelton*** case failed to appreciate the context of the statement as it also, with respect, misconceived the import of the particular sentence, namely, an observation and not a fixed principle of law. The approach adopted in the ***Shelton*** case also leads to the difficult task of having to categorise where business activities end in order for an appeal to the right to privacy to be applicable.

application, *in concreto* , of section 8 (4) of the Constitution.[85]

3.3.38 He refers to the Korf analysis[86] referred to above and concludes that while there is no uniform approach in foreign jurisdictions, it is submitted that the Constitutional Court in the *Hyundai Motor Distributors* case has already set the basis for the recognition of the information protection of companies to be located firmly within the protection afforded to the right to privacy. However, the peculiar nature of information protection, in regard to juristic persons and as evinced by the experience of other countries, also suggest that information protection is *sui generis*, and traverses other rights in addition to that of privacy.

3.3.39 He also refers to the position in the United States [87] where a distinction between juristic and natural persons is found in the Privacy Act of 1974[88] which only protects natural persons.[89] Similarly, the Fair Credit Reporting Act (the "FCRA") only protects consumer credit reports[90] of "individuals"– it specifically excludes so called commercial credit reports[91] and by definition any entity other than an "individual".[92] A credit report generated for an application for a business loan for the same individual would not be covered. Privacy protections under the FCRA will therefore depend on whether one is asserting privacy rights over information processed in a personal or professional capacity.

---

85 Admittedly, as was stated in the ***Hyundai Motor Distributors*** case, the privacy afforded to juristic persons can never be as intense as those of human beings. But, the Constitutional Court also asserted that this did not mean that juristic persons are not protected by the right to privacy.

86 Douwe Korf ***EC Study***.

87 A wide assortment of privacy laws are found in the individual States and at the federal level, but no national general privacy law has been enacted for the private sector, eg. the Fair Credit Reporting Act (1970), the Family Educational Rights and Privacy Act (1974), and the Right to Financial Privacy Act (1978). During the 1980s, Congress passed the Privacy Protection Act (1980), the Electronic Communications Privacy Act (1986), the Video Privacy Protection Act (1988), and the Employee Polygraph Protection Act (1988). In the 1990s, Congress passed the Telephone Consumer Protection Act (1991), the Driver's Privacy Protection Act (1994), the Telecommunications Act (1996), the Children's Online Privacy Protection Act (1998), the Identity Theft and Assumption Deterrence Act (1998), and Title V of the Gramm-Leach-Bliley Act (1999) governing financial privacy. See the discussion in the prepatory materials to the Standards for Privacy of Individually Identifiable Health Information; Final Rule. 65 F.R. 82462, (to be codified at 45 CFR Parts 160 and 164), 65 F.R. 82462, referred to as "HIPAA Final Rule".

88 5 U.S.C. § 552a.

89 Supra at (a)(2).

90 "Where the information concerns the subject's business history or status (i.e., is collected and provided by a commercial reporting agency for use in business transactions), of course, its communication to the user does not constitute a "consumer report" under Section 603(d).

91 Fair Credit Reporting Act, 15 U.S.C. § 1681a (d); ***Emerson v. J.F. Shea***, 76 Cal. App. 3d 579, 143 Cal Repr. 170 (1978)***; Yeager v. TRW Inc***., 961 F.Supp 161 (ED Texas, 1997).

92 Ibid., 15 U.S.C. § 1681a (c).

3.3.40 Whether to include juristic persons within the ambit of information privacy legislation is an issue that has not been conclusively determined in the international sphere. The Commission, however, received considerable support for its preliminary proposal to include juristic persons in the ambit of the proposed Bill and has therefore decided to confirm its position.

3.3.41 A juristic person, just like a natural person, has a sphere of privacy in which it has a legitimate interest and which is therefore worthy of legal protection.[93] **Juristic entities as well as natural persons are affected by the increased processing of information on them. It is therefore necessary to impose certain duties on persons processing information, while giving the subjects of such processing certain rights, to ensure that the processing of information on them does not harm their legitimate interests.**

3.3.42 The fact that the right to privacy is entrenched in the Constitution places an obligation on the legislature to initiate steps to rectify the position where these rights are lacking fulfilment under the law, especially since the common law is still in its infancy and clearly deficient in this regard.[94]

3.3.43 The aim of privacy legislation is not to stem the flow of information, but to regulate it. This will also be the position regarding juristic persons. Worldwide, privacy legislation is regarded as an example of ordinary good business practice. If juristic persons were excluded from the application of the proposed data protection measures, credit bureaux, for example, would be in a position to collect and use information on the creditworthiness of companies without any constraints except perhaps those imposed by the totally inadequate traditional common law data protection principles.[95]

3.3.44 The Bill furthermore makes provision for a number of exceptions and exemptions that may be used by juristic persons in order to deal with any practical

---

93 Neethling ”Data Protection and Juristic Persons” at 71.

94 Neethling “Data Protection and Juristic Persons” at 71.

95 ***Neethling Law of Personality*** 273-280; Neethling “Data Protection and Juristic Person” at 71.

difficulties that may occur. [96] See clause 3 at 138 below and the definition of "personal information" in clause 1 of the Bill.

(v) Public v private sector

3.3.45 Most of the respondents agreed with the position as set out in the discussion papers that the investigation should cover both the private and the public sector.[97]

3.3.46 It was argued that any legislation dealing with privacy protection is all encompassing, not just in respect of the form of the databases, but also in respect of the nature of the entities which collect personal information. As both public and private entities are affected by questions of privacy and information protection, there seems to be no reason why either sector should be excluded.[98] Consumers would be adversely affected if governmental agencies were not subject to security protection.[99] [100]

3.3.47 One commentator, however, submitted that the investigation should only focus on information kept by the private sector. It was argued that existing laws and policies provide at least a degree of protection and control over information kept by the public sector. Most of the information kept by law enforcement agencies can be regarded as sensitive information which should be kept out of the public domain. The same cannot be said about information gathered and kept by the private sector, which in most instances, is not regulated by legislation at all and is often driven by financial gain, competition and specific customer needs.[101]

---

96 For a distinction between the right to privacy of a juristic person, the right to privacy of natural persons attached to a juristic person and the immaterial property rights to the trade secrets of a juristic person, see ***Neethling's Law of Personality*** 32 fn 336.

97 The Internet Service Providers' Association; Sanlam Life: Legal Services; Neo Tsholanku, Eskom Legal Department; SABC; LOA; The Banking Council.; Law Society of South Africa.

98 SABC.

99 The SABC also requires that State Owned Enterprises should have limited access, under appropriate guidelines to protect competition, with respect to databases of private sector entities where such databases could be used by State Owned Enterprises where their rights are being affected. The SABC is of the view that in order to further its interests, and consequently those of the State as the sole shareholder and the public in respect of the collection of outstanding licence fees, the SABC and its agents/ representatives should be allowed access to the databases of other entities, including the databases of pay-channels such as M-Net.

100 LOA.

101 SAPS; See discussion on critical information below.

3.3.48 A commentator suggested that the Bill was not comprehensive since it has neglected to regulate specific industries such as the retail industry and credit bureaux when it comes to processing and distribution of personal information data.[102] It is, however, important to realise that the Bill is generic in nature and in fact includes any responsible party in both the private and the public sector that processes information.

3.3.49 Taking into consideration the points made, it was decided that the proposed Bill should be applicable to both the public and the private sector.

3.3.50 In the Issue paper the further question was posed whether a distinction should be drawn between the public and the private sector in drafting privacy legislation and if so, what these differences should be? [103]

3.3.51 Some commentators were of the view that no distinction should be drawn between the two entities.[104] They argued as follows:

* Information privacy legislation needs to cater for everyone that collects information.[105]
* Unless the same principles apply in both the public and the private sector, there would be no consistency in the law.[106] Different rules will leave room for game playing and waste of public funds just to keep outside the reach of the law.[107]
* Both the public and the private sectors have in their possession innumerable personal records and both have responsibilities towards their data subjects.
* PAIA treats these two sectors similarly, with minimal material distinction. There is therefore merit in being consistent by creating new legislation that also removes as far as possible the distinction between these two sectors.[108]

---

102 Department of Public Works.

103 Question 4, Issue Paper 24.

104 See eg. Medical Research Council; Private health Information Standards Committee; LOA; Gerhard Loedolff, Eskom; Eskom Legal Department; SAFPS; Strata; Liberty; Society of Advocates of Kwa-Zulu Natal.

105 LOA.

106 LOA.

107 Gerhard Loedolff, Eskom.

108 Liberty; LOA.

* If critical information is to be included in any protection law, then, in that area, there is room to justify the distinction, on the basis that the State ought to be allowed to gather and use private information for legitimate purposes.[109]
* It is particularly important that the provisions of the Bill encourages the correct practices with regard to personal information in the public sector, as the nature and form of the databases of such information, such as is maintained by the Home Affairs department, the police services etc., is extensive and of critical importance. Hence, these records, in particular, should be maintained in accordance with the principles of the Bill, including being updated and ensuring that the information is correct and accurate. [110]

3.3.52 Other respondents, however, argued that due regard should be given to the different and differing interests which the public and private sectors have in information:[111]

* For example, the use of medical information for the assessment of risk in cases of proposed contracts of insurance differs from the State's use of medical information to compile public health profiles or for state public health interventionist strategies.
* The public sector is empowered by specific legislation to fulfill certain duties whilst their interest in good governance and the security of the Republic also outweighs that of the private sector. The public sector, representing Government, is furthermore entitled by certain laws to limit the privacy of the individual, eg interception and monitoring of communications, search and seizures, etc. Entities such as private investigators have few, if any powers to infringe the privacy of individuals. They are furthermore only accountable to their (paying) clients and not to the public in general.[112]
* One should recognise the public interest in the public sector's retention of certain records and public access to them in cases in which retention by and availability from the private sector would be inappropriate in light of the constitutional right to privacy. [113]

---

109 Society of Advocates of Kwazulu Natal (JC King); SAFPS.

110 Nedbank Ltd.

111 Sanlam Life: Legal Services; Vodacom (Pty) Ltd; The Banking Council; SAHA; Internet Service Provider's Association.

112 SAPS; Financial Services Board.

113 SAHA. SAHA is particularly concerned to ensure considerations of privacy should not limit transfer of records to the National Archives or provincial archives services or access to documents held by them any more extensively than strictly necessary for protection of the constitutional right to privacy.

* The private sector, on the other hand, should be allowed flexibility through the development and application of self-regulatory measures such as codes of conduct.[114] Although the two sectors are treated similarly in most national laws, there is a differentiation between the sectors in international information protection instruments. The public sector bodies are subjected to more stringent regulation than private sector bodies. [115]

3.3.53 There were also commentators who drew the Commission's attention to the fact that the distinction between public and private bodies is not always very clear: [116]

* Many bodies from the private sector take decisions which have a profound impact upon public policy.
* In South Africa, we do not only find a distinction between the public and private sector bodies but we also find some form of rules or legislation specific to state owned enterprises. [117]
* In many instances (the SABC, for eg) there is an overlap of laws and regulations which apply to both the public and private sector bodies. When the SABC performs a public function in terms of the Broadcasting Act, it is on the whole also performing a commercial interest by generating revenue as a corporate entity.[118]
* There are many other state owned enterprises like the SABC that are faced with similar uncertainties when, for example, their activities do not fall exclusively within either of the public or private sectors. Attempts to re-categorise an entity every time a problem arises will cause undue delay and unnecessary costs for all affected entities.[119]

3.3.54 The recommendation of the Commission is, therefore, that no distinction should be drawn between information processed by public and private bodies. The

---

114 The Banking Council.

115 SABC.

116 SABC; ISPA.

117 SABC; As an example reference was made to the SABC which is a State Owned Enterprise governed by various legislation. Further to the public law legislation, the SABC is obliged to comply with the Broadcasting Act, the IBA Act, its licence conditions, various regulations such as those prescribing local content quotas, Codes of Conduct pertaining to the broadcasting industry, as well as company law principles. In addition, the SABC is obliged to structure its business practice and model as set out in the Protocol on Corporate Governance in the Public Sector.

118 SABC.

119 SABC.

proposed Bill will therefore deal similarly with both sectors. See the definition of "record" in clause 1 of the Bill and clause 3 at 138 below.

(vi) Critical information

3.3.55 Personal information processed in the course of an activity which falls in operations concerning public security, defence and policing is referred to as "critical information" for the purposes of this investigation.[120]

3.3.56 In its discussion papers the Commission identified two important points in so far as critical information is concerned. Firstly, one should determine what the definition of critical information is.[121] Secondly, one would have to decide how critical information should be protected: should it be excluded from all the information protection principles, only some of them, or should the scope of the obligations and rights provided for in the principles be restricted in specific circumstances?

3.3.57 At the outset it should be noted that a new Bill, the Protection of Information Bill[122] is currently being developed by the Ministry of National Intelligence. Reference will be made where applicable to the clauses contained in this Bill. The position as set out in the Discussion Paper will, however, be retained since the final format of the Bill is not known at this stage and the impact on other related pieces of legislation has not been determined yet.

A) Definition of critical information

3.3.58 "Critical information" and "special/sensitive information"[123] should be distinguished for purposes of our discussion. Whereas critical information deals with state security and crime, special information is concerned with confidential aspects of information of a very personal kind such as race, ethnicity, political opinions, religious or philosophical beliefs, trade-union

---

120 Term used in the ECT Act. See, however, the discussion on the newly proposed Protection of Information Act below.

121 Eg, if someone would be able to hack into the JSE and bring it down for a week, it would have a far more catastrophic effect on our country than fighting a war on our borders for a couple of years.

122 Protection of Information Bill [B28-2008] .

123 Sometimes referred to as "sensitive" information. However, see the Protection of Information Act 84 of 1982.

membership, and the processing of information concerning health or sex life or criminal record. It also includes, for purposes of our discussion, the personal information of children. Special information could, of course, also become critical information where it is relevant to the protection of state security or criminal activities. See the discussion below in Chapter 4.

3.3.59 The so-called "critical information" or "security information" should furthermore not be equated with personal information that is kept secure in terms of the security safeguards privacy principle. All personal information should be kept secure irrespective of whether it is of a specific kind or not. Once information is classified as critical/sensitive information, it is marked accordingly and given various forms of protection - including restricting access to people with a security clearance at the appropriate level, physical protection (such as storage in approved containers of sufficient strength or meeting other security standards) and restrictions on how it may be transferred from one person to another. However, the fact that information is not classified as critical or sensitive, does not mean that it is freely available.[124] All personal information is subject to the privacy principles.[125]

(a) Position preceding the newly proposed Protection of Information Bill

3.3.60 From our research it is clear that there are currently a number of Acts dealing with critical information.

3.3.61 Terms used in other Acts for describing information relating to the protection of national security or the economic and social well-being of the country's citizens are "classified information"[126] or "information kept, used, made, obtained or related to a prohibited place",[127] as well as "intelligence/security information".[128]

3.3.62 Classified information is defined to be:[129]

---

124 Australian Law Reform Commission ***Keeping Secrets: The Protection of Classified and Security Sensitive Information*** ALRC 98 June 2004 accessed at http://www.austlii.edu.au/other/alrc/publications/reports/98/5.html on 2005/3/18.

125 See discussion in Chapter 4: Principle 7: security safeguards.

126 Public Audit Act 25 of 2004; National Strategic Intelligence Act 39 of 1994; Defence Act 42 of 2002; Intelligence Services Act 65 of 2002 etc.

127 Protection of Information Act, Act 84 of 1982.

128 Intelligence Services Oversight Act 40 of 1994 and National Strategic Intelligence Act 39 of 1994.

129 Minimum Information Security Standards (MISS) at 8. See discussion on MISS in par 3.3.67.

> Sensitive information which, in the national interest, is held by, is produced in or is under the control of the State or which concerns the State and which must by reason of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.

3.3.63 This definition differs from that in a separate specific policy which governs information security within the South African Defence Force.[130] This more narrow military information security policy is contained in a set of South African National Defence Force Orders (SANDF/INT DIV/2/97) which applies principally to the SANDF and Armscor. Classified information is defined in terms of these orders as:

> any information or material which is held by or for, is produced in or for, or is under the control of the State or which concerns the State and which for the sake of national security be exempted from disclosure and must enjoy protection against compromise. Such information is classified either Restricted, Confidential, Secret or Top Secret according to the degree of damage the State may suffer as a consequence of its unauthorised disclosure.

3.3.64 The Intelligence Services Oversight Act 40 of 1994 defines "intelligence" in section 1 as follows:

> 'Intelligence' means the process of gathering, evaluation, correlation and interpretation of security information, including activities related thereto, as performed by the Services;[131]

Security information is not defined.

(b) Protection of Information Bill

3.3.65 The following definitions are set out in terms of the newly drafted Protection of Information Bill -

---

130 Klaaren J "Access to Information and National Security in South Africa" ***National Security and open Government: Striking the Right Balance*** Maxwell School of Citizenship and Public Affairs of Syracuse University New York 2003 695 (hereafter referred to as "Klaaren") at 196.

131 Services' means the Agency, the South African Secret Service, the Intelligence Division of the National Defence Force and the Intelligence Division of the South African Police Service; Agency is defined as follows: 'Agency' means the National Intelligence Agency referred to in section 3 of the Intelligence Services Act, 1994 (Act 38 of 1994). Act 38 of 1994 replaced by Intelligence Services Act 65 of 2002.

a) "Classified information" means the State information that has been determined under this Act or the former Minimum Information Security Standards guidelines to be information that may be afforded heightened protection against unauthorised disclosure;

b) "Intelligence" means any information obtained by a national intelligence structure for the purposes of crime prevention, investigation and combating or for the purpose of informing any government decision or policy-making process carried out in order to protect national security or to further the national interest, and includes the definitions of counter-intelligence, crime intelligence, departmental intelligence, domestic intelligence, domestic, military intelligence, foreign intelligence and foreign military intelligence as defined in section 1 of the National Strategic Intelligence Act, 1944 (Act No. 34 of 1994);

c) "sensitive information" is information which must be protected from disclosure in order to prevent the national interest of the Republic from being harmed.

d) "personal information" has the meaning assigned to it in section 17. According to section 17 personal information is any information concerning an identifiable natural person which, if disclosed, could reasonably be expected to endanger the life or physical safety or general welfare of an individual.

e) Commercial information includes the commercial, business, financial or industrial information held by or in the possession of an organ of state.

The classification levels of personal information are set out in terms of clause 20 and personal information may be classified as "secret"or "top secret" where its disclosure may endanger the life of the individual concerned.

3.3.66 It is hoped that the different aspects of critical information will be dealt with definitively by the new Protection of Information Bill of 2007.[132] It is furthermore important

132 Protection of Information Bill [B28-2008]. A similar argument was posed by Liberty.

[133] that any legislation regarding privacy and information protection should complement each other.[134] It is of utmost importance that there is harmonisation and co-ordination between the different pieces of legislation dealing with information regarding state security and criminal law issues. One should, however, acknowledge the fact that the harmonisation of these pieces of legislation will take time. It should be noted that, in so far as POPIA is concerned, the limited nature of the definition of personal information in the Protection of Information Bill will have the effect that personal information processed by the state will, in general, be regulated by POPIA. It is only where disclosure will physically harm an individual that the PIA will be applicable.

B) Protection of critical information

a) Current position in South Africa

3.3.67 The Protection of Information Act 84 of 1982 is currently the principal Act concerned with the restriction of the disclosure of information.[135] As set out above it is, however, being reviewed and will be repealed once the new Protection of Personal Information Bill is enacted. The principal mechanism by which the Protection of Information Act is currently implemented is a Cabinet-level policy document, the Minimum Information Security Standards (MISS).[136] The MISS is to be implemented by each public institution as well as some private institutions working

---

133 See also ENF for Nedbank Ltd.

134 In order to follow this route the legislation dealing with these matters will have to be harmonised. There are currently numerous acts involved. Some examples are:

* Section 104 of the Defence Act 42 of 2002 deals with the improper disclosure of information;
* Section 11A of the Armaments Development and Production Act 57 of 1968 deals with the prohibition of disclosure of certain information;
* Section 4 of the National Key Points Act 102 of 1980 deals with the furnishing of information to the Minister;
* The Protection of Information Act 84 of 1982 is a broad based act providing for the restriction of the disclosure of information.
* Section 4 and 5 of the Intelligence Services Oversight Act 40 of 1994 deals with access to intelligence, information and documents and secrecy of information.
* National Strategic Intelligence Act 1994 provides for the protection of information and intelligence.
* Section 41 of the Promotion of Access to Information Act 2 of 2000 deals with the national security ground of refusal to access to information.
* Section 56 of the ECT Act 2002 deals with the restrictions on the disclosure of information.
* Section 35 of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 deals with the manner in and periods for which the information at the relevant centres should be kept.

135 See a full discussion by Klaaren J at 195.

136 The MISS was approved by Cabinet on 4 December 1996 as “national information security policy”. See also Part II B of the PSA Regulations amended Nov 2002. New regulations were, however, being drafted by the National Intelligence Agency, but have been incorporated in the newly drafted Protection of Information Bill.

with public ones. According to its preface the MISS "must be maintained by all institutions who handle sensitive/classified material of the Republic".

3.3.68 Various initiatives[137] regarding the protection of critical information [138] have been noted. [139]

3.3.69 All the different initiatives have, however, now been incorporated in the National Intelligence Ministry's review of the Protection of Information Act of 1982. The proposals for a new Protection of Information Bill make provision for the classification and declassification of

---

137 Section 53 of the Electronic Communications and Transactions Act 25 of 2002 ("the ECT Act") provides that when information is important to the protection of national security or the economic and social well-being of the country's citizens, the Minister may declare them to be "critical databases". The Act then sets out the special treatment that these databases will enjoy. Chapter IX of the Act deals with the registration of critical data bases (section 54), the management of critical data bases (section 55), restrictions on disclosure of information (section 55), the right of inspection (section 57) and non-compliance with the chapter (section 58).

While these considerations may have their value, the reality is that there have been no ministerial declarations to this effect in terms of the Act. In November 2003 the Minister of Communications awarded a tender to a consortium of Consultants to undertake an inventory of all major data bases in South Africa.

The purpose was to assist the Minister to -

(a) put in place regulations, with respect to the development, maintenance, validity, integrity and security of these databases and related systems,
(b) review progress and compliance on an ongoing basis,
(c) refine policy, legislative and regulatory requirements where appropriate; and
(d) ensure that databases and information, in the Republic of South Africa, that could negatively impact on companies and citizens, are developed, maintained and secured to meet appropriate standards.

It is therefore unsure what the effect of the ECT Act will be, especially since section 55 dealing with the management of critical databases also provides as follows in section 55(3):

This Chapter must not be construed so as to prejudice the right of a public body to perform any function authorised in terms of any other law.

138 The Minister for Intelligence Services furthermore launched the Classification and Declassification Review Committee in February 2003 with the aim to develop criteria for the management of the protection of classified information and the access of information that has been declassified. The Review Committee adopted the following terms of reference:

* To scrutinise existing legislation, regulations, policies and procedures relating to the classification and declassification as well as custody of sensitive information;
* To study international practices in respect of legislation, practices etc.
* To examine the practical application of the above in respect of facilities and controls in various government departments;
* To study policies and practices in the private sector (eg banks, financial institutions, construction and service industries);
* To examine the storage of sensitive information; and
* To formulate recommendations regarding amendments to legislation, policies and procedures, especially with regard to the harmonisation of legislation, policies and standards.

Existing legislation had to be reviewed to ensure a synergy and that it meets with Constitutional obligations. A clear policy and guidelines for classification and declassification is needed to manage the protection as well as access of critical information.

139 The National Strategic Intelligence Act 39 of 1994 provides in section 6 that the Minister (member of cabinet designated by the President to assume the responsibility for intelligence services as contemplated in section 209 (2) of the Constitution) may, after consultation with the Joint Standing Committee on Intelligence, and in consultation with the relevant Government Departments affected, make regulations regarding inter alia the protection of information and intelligence. Draft regulations in this regard, intended to replace the MISS, were discussed.

information. State information is defined in terms of protected information, valuable information and designated information. Designated information may also be valuable information, but is also divided into classified information, sensitive information, commercial information and personal information. An intrinsic value approach is incorporated and the Minister will set out national standards and procedures to deal with the information. Information is protected against destruction, loss and unauthorised disclosure.[140]

b) Possible impact of privacy legislation on the protection of critical information

(i) International position

3.3.70 Most information protection laws in other jurisdictions provide for exceptions to the information protection principles with regard to critical information, while critical information is totally exempted from the provisions of some information protection laws.

3.3.71 Taking into consideration the adequacy requirements discussed above, it is important to note how the EU Directive deals with critical information. Art 3(2) of the EU Directive stipulates that the Directive does not apply to the processing of personal information in the course of an activity which falls outside the scope of the Community law (so-called first pillar):

- such as those provided for by Titles V[141] and VI[142] of the Treaty on European Union; and
- in operations concerning public security, defence, State security (including the economic well being of the State when the processing operation relates to State

---

140 SAFPS submitted that there is a clear distinction between what the organs of state security and the private sector would define as "critical information". SAFPS does not wish to comment with regard to state security. However within the private sector it will be necessary to clearly define the term "critical information" to differentiate between information held and retained for purely business purposes and information retained with regard to actual or suspect criminal conduct which, for whatever reason, has not been prosecuted but is held for the purposes of risk management and decision making in normal business activity. In similar vein "critical information" in the insurance industry could well be totally different to "critical information" in the retail industry.

141 Title V: Provisions on a common foreign and security policy for the EU (so-called second pillar).

142 Title VI: Provisions on Cooperation in the Fields of Justice and Home Affairs in the EU (so-called third pillar). Second pillar activities include cooperation regarding peace keeping, disarmament and Europe's long-term security framework. Third pillar activities include cooperation between judicial authorities in civil and criminal law, police cooperation, fighting organised crime, terrorism, trafficking etc.

security matters) and the activities of the State in areas of criminal law.

3.3.72 Article 13(1)((a)-(g) of the Directive furthermore provides for exemptions from specific privacy principles in terms of which legislative measures may be adopted to restrict the scope of the privacy principles in the indicated instances. [143] Two conditions are imposed: The exemptions must be set out in “legislative measures” and they must be “necessary “ to safeguard the public interest in question (national security, defence, public security, prevention etc of criminal offences, important economic interest).

3.3.73 Two levels of processing can therefore be identified: Firstly, the international cooperation of states in these areas (second and third pillar) and secondly, the internal processing of information in these areas (first pillar).

3.3.74 In evaluating the impact of POPIA on the protection of critical information it would at first glance seem, since the EU Directive does not apply, as though the adequacy requirements would not be an obstacle to a blanket exemption of critical information from the Bill. However, it will become apparent below that the developments in the third pillar also influence first pillar activities and that current developments in Europe indicate that a stricter regime is envisaged.

3.3.75 It would be shortsighted for South Africa not to take note of the developments taking place in this field worldwide, but particularly in Europe. Inevitably, the co-operation between Member States and State authorities in the second and third pillars involves access to and processing of a great deal of personal information, often of a sensitive nature.

---

143 Article 13
Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

3.3.76 Already on the 1 December 2004 the European Data Protection Supervisor made the following statement regarding law enforcement:[144]

> Firstly, it seems to me that there are many reasons to assume that data protection in all pillars should be based on the same 'base line' principles of Directive 95/46/EC which presently does not apply to the third pillar. The growing convergence between the first and the third pillar, the end of the pillar structure under the Constitution, and the fact that most member states have implemented Directive 95/46/EC in ways which include third pillar activities, all seem to argue in the same direction. This would not preclude sector-specific rules, where necessary, provided that the same principles and criteria would be applied as anywhere else. To put it differently, no general framework for data protection in third pillar matters could offer sufficient safeguards with respect to those specific areas. This is why we need a differentiated approach addressing different aspects of the problem in different instruments or documents, but these instruments should of course be fully consistent.

3.3.77 Recently a European Court Judgment exposed a loophole in the protection of the personal information of EU passengers when travelling to the US.[145] It is also an example of the need to harmonise the privacy laws worldwide. Since January 2003, European Airlines flying into the US are obliged to provide the US customs authorities with electronic access to the data contained in their automated reservation and departure control systems, referred to as "Passenger Name Records/PNR Data". Based on US laws companies that fail to provide information can be fined a maximum of $5,000 for each passenger. The European Commission was, however, of the opinion that this requirement would be in breach of national laws and Community legislation including the EU Directive and threatened to impose fines if the information was sent. The European airline companies therefore found themselves in an impossible situation. An agreement between the EU and US to solve this problem was found unlawful by the European Court.[146]

---

144 Peter J Hustinx European Data Protection Supervisor at the Scientific Conference on New Ideas and Trends in the Field of Third Pillar and Law Enforcement Data Protection Budapest 1 December 2004 accessed on 26/11/2006 at http://www.edps.europa.eu/publications/speeches/04-12-01_Budapest_EN.pdf.

145 Guild E & Brouwer E "The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US" Centre for European Policy Studies Policy Brief No 109 July 2006.

146 The European Union and the United States has since reached an agreement on 18 July 2007 on the processing and transfer of passenger name record (PNR) data by airlines to the US government. Airlines flying from the EU to the US can transfer passenger information including names, addresses, phone numbers, itineraries and credit card numbers to US government agencies defined in the agreement. This agreement replaces the interim agreement of 6 October 2007reached between the European Community and the United States. Even though passenger information can be

3.3.78 Other developments are the attempts to have the European Constitutional Treaty (a constitution for Europe) ratified by member countries. The treaty makes provision for a collapse of the pillar structure. The European Commission has, furthermore, proposed a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[147] In this proposal the Commission underlines that

> Member States will only fully trust each other if there are clear and common rules for the possible further transmission of exchanged data to other parties, in particular to third countries.

This proposal is still under discussion.

3.3.79 On 8 November 2006 the European Data Protection Authorities made the following joint statement:[148]

> Expanding the crossborder exchange of information, and sharing data stored in national files, subject to the principle of availability, as part of the co-operation between police and judicial authorities at EU level has become the focus of discussions within Europe. In this context, the European Data Protection Authorities already stressed repeatedly that given the Union's obligation to respect human rights and fundamental freedoms, initiatives to improve law enforcement in the EU, such as the availability principle, should only be introduced on the basis of an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection, which is consistent with First Pillar standards. The European Data Protection Authorities call on the Member States to respect and strengthen the civil liberties of the citizens living in the EU to establish an adequate system of data protection arrangements guaranteeing a high and equivalent standard of data protection applicable to all data processing for law enforcement purposes. There is no alternative to creating a high and harmonized data protection standard in the EU Third Pillar. This is a logical consequence of the Hague

---

passed on by the recipient agencies to other US agencies with counter-terrorism functions, none of these agencies will have any direct electronic access to PNR data (the so-called “push” rather than “pull” arrangement). Moreover, these agencies have to respect data protection standards comparable to those imposed upon the recipient agencies. The agreement will entered into force at the end of July 2007 and will be valid for seven years.

147 COM (2005), 4 October 2005.

148 European Data Protection Authorities European Data Protection Supervisor declaration published Wednesday, 8 November, 2006 - 11:49.

> Programme, according to which the safeguarding of freedom, security and justice are indivisible elements of the task of the EU as a whole. Relevant data protection provisions should be adopted and applied as soon as possible in the field of law enforcement, providing for an adequate and harmonised system of data protection arrangements not only applying to data exchange between member states but applying to all personal data processed for law enforcement purposes. A high standard of protection should also apply to the transfer of data to third countries and international bodies, subject to an adequacy finding based on common European standards. Any other, more limited approach will not be workable in practice and will not create the trust needed for effective cooperation in law enforcement .

Although the EU Directive therefore makes provision for an exclusion, current developments in Europe indicate that a stricter regime is envisaged.

(ii) Full exclusion of critical information from privacy legislation

3.3.80 In so far as the question regarding the possible exclusion of critical information from the privacy legislation is concerned, it is interesting to note that countries in Europe have made limited use of the possibility to fully exclude critical information from their information privacy laws.[149] Denmark, Ireland, the UK (for national security)[150] and Spain are exceptions to this rule. They are the countries that have complete or almost complete (and in practice unchallengeable) exemptions from the information principles, the exercise of data subject rights, notification and

---

149 Korff D ***Comparative Summary of National Laws*** EC Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49) Human Rights Centre Cambridge September 2002 (hereafter referred to as "Korff ***Comparative Study***") at 142.

150 Section 28 stipulates as follows:

> 28. - (1) Personal data are exempt from any of the provisions of -
> (a) the data protection principles,
> (b) Parts II, III and V, and
> (c) section 55,
> if the exemption from that provision is required for the purpose of safeguarding national security.
>
> (2) Subject to subsection (4), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions mentioned in subsection (1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact.
> (3)-(12).....

enforcement. Blanket exemptions are, however, not acceptable and the legislative provisions are quite complicated and involved. See the discussion below.[151]

(iii) Separate laws excluded

3.3.81 Some countries subject some or most processing in the areas listed to separate laws.[152] This does not, however, necessarily mean that they are not subject to a regime which is compatible with the principles of the Directive. Processing in connection with defence, security services, police matters etc is subject to special laws or rules which, in turn, must conform to the basic principles in the information protection law. See for instance the Netherlands, Italy, Luxembourg, Germany, Portugal, Sweden.

3.3.82 This is not to say that processing for the kinds of purposes mentioned above and which is subject to the national laws implementing the Directive does not benefit from extensive exceptions and exemptions within those laws. As is clear from Art 13(1) paras (a) -(g) the Directive expressly allows for exemptions and restrictions for the information protection principles, i.e. Art 6(1); the informing-requirements imposed on controllers under Arts. 10 and 11(1); the right of access, rectification or erasure (Art 12); and the duty to publicise details of processing operations (Art 21) with regard to such processing.[153]

3.3.83 However, the Directive does impose two conditions in this respect: such exemptions or restrictions must be provided for in “legislative measures” and they must be “necessary” to

---

151 Different options have been identified -

Option 1: Authorisation at cabinet level -

a) together with authorisation of Information Commission (French example);or
b) together with an appeal to a tribunal (UK example).

Option 2: Netherlands: Separate laws excluded.

Option 3: Exclusion of specific principles (New Zealand and UK example).

Option 4: Position in federal legislation in Canada: Exempt Banks.

The Governor in Council may designate exempt banks.

152 See Art 2 of the Personal Data Protection Act 2000 of the Netherlands.

153 Korff ***Comparative Study*** at 142.

safeguard the public interest in question. In terms of the Directive, compliance with these requirements should furthermore be subject to monitoring by a "supervisory authority" fulfilling the requirements of Art 28 of the Directive.

(iv) Limited exclusion (often in addition to full exclusion/separate laws)

3.3.84 Apart from the very wide exemption with regard to processing for the purpose of safeguarding national security,[154] the law in the UK includes a series of more limited exemptions for personal information processed in relation to crime and taxation matters, health, education and social work etc. Most of these exemptions are limited to what is referred to as "subject information provisions" i.e. informing-requirements and the data subject access requirements, but the crime and taxation exception extends to the "fair processing" principle.[155]

3.3.85 The main point to be made about these exceptions is, however, that they all only apply to the extent that the full application of the provision from which they allow derogations "would be likely to prejudice" the matters concerned.[156] This means that the courts and the information

---

154 See footnote 150 above.

155 Korff ***Comparative study*** at 144;Section 29 (1) and (3) of the UK Data Protection Act 1998.
Section 29 (1) reads:

'Personal data processed for any of the following purposes-
(a) The prevention or detection of crime
(b) The apprehension or prosecution of offenders
are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and Section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.'

Data Protection Principle 1 covers fair and lawful processing of data and the requirement to provide information to data subjects (Data Protection Notices on Applications and Agreements); Schedules 2 and 3 cover the conditions for processing and the conditions for processing sensitive data; Section 7 deals with the provision of information (subject access) to data subjects regarding the identity of the data controller, the purpose of the processing and the recipients of the data. The non-disclosure provisions relate to subject access.

Section 29 (3) reads:

'Personal Data are exempt from the non-disclosure provisions in any case in which: -
(a) The disclosure is for any of the purposes mentioned in subsection (1), and
(b) The application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.'

156 The Information Commissioner also warned the Home Office that the new powers enabling law-enforcement and intelligence agencies to demand the communications records of British telephone and internet users may breach human rights law because website, email or phone logs available strictly for national security investigations can be accessed by police or intelligence officers for more minor cases such as public health and tax collection. The law states that access to this information by law-enforcement agencies should only be on the grounds of national security or for investigating crime related directly or indirectly to national security. Stuart Millar, technology correspondent ***The Guardian*** July 31, 2002 accessed at http://www.guardian.co.uk/guardianpolitics/story/0,3605,765917,00.html on 2002/08/02.

protection authority are able to assess the necessity of any such exceptions and their application in practice, in accordance with the Directive.[157]

3.3.86 This was confirmed by the UK Information Commissioner, who stressed that these exceptions are restrictively applied:[158]

> The Commissioner takes the view that, for any of these three exemptions to apply, there would have to be a substantial chance rather than a mere risk that in a particular case the purposes (crime prevention and -detection and taxation) would be noticeably damaged. The information controller needs to make a judgment as to whether or not prejudice is likely in relation to the circumstances of each case".

3.3.87 In New Zealand section 57 provides that nothing in principles 1-5 and 8-11 applies in relation to information collected, obtained, held or disclosed to, an intelligence organisation. Principles 6 and 7 deal with access to personal information and correction of personal information.

3.3.88 In the USA law enforcement agencies have immunity from almost every significant restriction in the Privacy Act.[159] In so far as national security is concerned, a system of records that is maintained by the CIA may be generally exempted from the Privacy Act's access and amendment provisions as well as from the provision that the information should be collected directly from the data subject as far as possible.

3.3.89 It seems as though national security is more easily exempted than criminal processing. See the position in the UK[160] and New Zealand.[161]

---

157 Korff ***Comparative study*** at 144.

158 Korff ***Comparative study*** at 145.

159 Roos 1998 ***THRHR*** at 525.

160 Data Protection Act 1998
29. Crime and taxation
29. (1) Personal data processed for any of the following purposes-
(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders, or
(c) the assessment or collection of any tax or duty or of any imposition of a similar nature, are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

c) Respondents to the discussion paper

3.3.90 In South Africa, most respondents who commented on this issue agreed that it would be premature at this stage, to exclude critical data bases from all the information protection principles.[162]

3.3.91 Respondents[163]reiterated the view of the Commission that the more critical the information, the more important it may be to ensure that the personal information collected is correct and even more stringently protected and that it will need to be incorporated in the legislation.[164]

3.3.92 It was proposed that the application of such principles should apply at least until the relevant legislation is developed giving sufficient protection to information that may be contained

---

(2) Personal data which-
(a) are processed for the purpose of discharging statutory functions, and
(b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1), are exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in that subsection.

(3) Personal data are exempt from the non-disclosure provisions in any case in which-
(a) the disclosure is for any of the purposes mentioned in subsection (1), and
(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.

(4) Personal data in respect of which the data controller is a relevant authority and which-
(a) consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that authority for either of the following purposes-
(i) the assessment or collection of any tax or duty or any imposition of a similar nature, or
(ii) the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds, and
(b) are processed for either of those purposes, are exempt from section 7 to the extent to which the exemption is required in the interests of the operation of the system.

161 New Zealand Privacy Act 1993
57. Intelligence Organisations
57. Intelligence organisations - Nothing in principles 1 to 5 or principles 8 to 11 applies in relation to information collected, obtained, held, used, or disclosed by, or disclosed to, an intelligence organisation.

162 The Internet Service Providers' Association; Liberty; Neo Tsholanku, Eskom Legal Department; ENF for Nedbank Ltd; SABC; LOA; The Banking Council; Lawyers for Human Rights; Law Society of South Africa; Society of Advocates of Kwa-Zulu Natal.

163 Vodacom (Pty) Ltd; SABC; ENF for Nedbank Ltd.

164 ISPA stated that in light of section 54 of the ECT authorising the Minister to declare a database as a critical database, the data protection principles should apply.

in such data bases and it may be worth preserving their application even after such legislation have been gazetted.[165]

3.3.93 Of the other responses received,[166] many agreed that critical information is a necessary part of allowing the functioning of the State to continue unaffected, but argued that it is imperative that this Bill provide specific and very limited rights in this regard, so as to avoid the abuse of such information by the State.[167]

3.3.94 These respondents felt that it is important that exclusions or exceptions included in the Bill do not allow for the State to have access to personal information beyond what is reasonably necessary for it to carry out its functions and duties.[168] They were therefore not in favour of a total exclusion from the information principles in respect of critical information and advised that these exclusions should be in respect of the relevant sections of the applicable statutes only. They commented that one should always be careful not to confuse " national security" with allowing overweening government and secondly that the Homeland Security attitudes apparent in America should not be allowed to resonate here. However, existing laws dealing with national security defence and police work should be excluded from privacy legislation. [169]

3.3.95 In general it was argued that there is good reason to oppose blanket exemptions to privacy rights.[170] In this case, support for specific exemptions may be appropriate only if the Regulator is provided with strict guidelines as to determine the appropriate balance of rights and a meaningful way in which to make decisions related to possible exemptions.[171] One should allow for individual exemptions in the interests of state security only if done so by providing a definition of state security that identifies specific circumstances in which privacy protection principles may be set aside. In doing so, the legislation needs to identify which of the eight core privacy protection principles may be exempted. Broad and vague exemptions erroneously assume that one must give up core information principles to protect national security. While the global

---

165 The Internet Service Providers' Association.

166 Institutions such as Nedbank Ltd, Lawyers for Human Rights, Law Society of South Africa, Society of Advocates of Kwa-Zulu Natal etc.

167 Nedbank Ltd; Dr MDC Motlala.

168 Nedbank Ltd.

169 Law Society of South Africa.

170 Nedbank Ltd.

171 Lawyers for Human Rights.

community continues to debate the appropriate balance between civil liberties and state interests, South Africa must demonstrate a strong commitment to privacy rights in its legislation, as it did by including the right to privacy in its Constitution.[172]

3.3.96 The Department of Defence indicated its agreement with the Commission's preliminary view that the specific laws dealing with National Security, Defence and Police work should be excluded from the privacy legislation.[173] The DoD does not see any reason why the Protection of Personal Information Bill should not apply to personal information in possession of the DoD relating to its members (eg. personal files) as long as such information is not classified and will not compromise national security and defence work.[174]

3.3.97 A few respondents, however, felt that critical information should be excluded.[175] It was stated that, without wishing to minimize the importance of a citizen's right to privacy, this country faces other issues, for example, that of crime, which must at least for the moment, take precedence. Accordingly, critical information must be excluded from the information protection laws altogether.[176]

---

172 Lawyers for Human Rights.

173 DoD submission dated 6 March 2006.

174 The DoD referred the Commission to the following acts that may have to be harmonised with the new Bill:

a) Section 104(7) of the Defence Act 42 of 2002 which provides that:
"Subject to the Promotion of Access to Information Act 2 of 2000 any person who, without authority, discloses or publishes any information, or is responsible for such disclosure or publication, whether by print, the electronic media, verbally or by gesture, where such information has been classified in terms of this Act, is guilty of an offence and liable on conviction to a fine or imprisonment for a period not exceeding five years"

b) Protection of Information Act 84 of 1982 which is currently being reviewed by a Task Team run by NIA.

c) National Strategic Intelligence Act 39 of 1994 provides for the legal obligations of the NIA. The NIA is gathering , correlating, evaluating and analysing information in terms of an obligation conferred upon it by national legislation for specific purposes also encompassed in national legislation. It is further also clear that the aforementioned is conducted for purposes of state security for which secrecy is a requirement.

d) Section 11(2) of the Intelligence Services Act 65 of 2002.

e) Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

f) Information Security Regulations that will substitute MISS are also in the process of being issued in terms of section 6 of Act 39 of 1994.

g) Internal directives within the Intelligence Service to protect security information and intelligence issued by the Director General of NIA in terms of sections 10(2)(b),10 (3) and 10 (4) of the Intelligence services Act 65 of 2002.

175 SAFPS; SAPS, NIA.

176 Society of Advocates, Kwa-Zulu Natal. The SAPS argued that full effect must be given to the Constitution in respect of privacy relating to data, but that proper limitations, as recognised in democratic societies which allow crime detection, investigation and intelligence functions, must be recognised and protected in the process.

3.3.98 In their first written response to the Discussion paper, NIA and the police indicated that they were in favour of blanket exclusions from the legislation for the police and the agency as entities.[177] They felt that information protection legislation would hamper day to day police functions and create a cumbersome and unnecessary mechanism in as far as it relates to the police. It was submitted that the Bill would negatively impact on the functions, powers and objects of the SAPS. They concluded that there is already adequate legal protection available to individuals whose personal information is processed by the Service or any other entity in the criminal justice system.

3.3.99 This idea was further elaborated on by the SAFPS which requested that it be excluded from the Bill.[178] It was therefore submitted that although the legislature should provide a measure of protection of privacy in general and informational privacy in particular, such protection must specifically exclude any requirement on the provision to consumers of information related to fraudulent activity and crime in general irrespective of whether such information is held by public or private bodies and organisations.

3.3.100 Following subsequent discussions with the police and NIA, agreement was reached to -

a) define personal information in the proposed Bill as set out above;

b) make provision for a limited exemption to the information protection principles with regard to critical information.

---

177 The following suggestion for legislative enactment was provided:
4. This Act does not apply to the processing of personal information -
a) ...
b) ...
c) by or on behalf of the intelligence or security services referred to in the Intelligence Services Act 65 of 2002 for purposes of fulfilling its functions as set out in section 2 of the National Strategic Intelligence Act 39 of 1994.
d) by the South African Police Services for purposes of achieving its objects set out in section 205(3) of the Constitution of the Republic of South Africa 108 of 1996, namely to prevent, combat and investigate crime, to maintain public order, to protect and secure the inhabitants of the Republic and their property, and to uphold and enforce the law, including the performance of its functions relating to intelligence as set out in section 2 of the National Strategic Intelligence Act 39 of 1994.

178 The following arguments were raised:
* Fraud Prevention databases would be able to continue to operate using a variety of data matching techniques (including address based systems and systems that use fuzzy matching techniques) to identify crime, without being constrained by arguments that such processing is unfair. These sophisticated data matching techniques are key tools in the fight against organised financial crime.
* Fraud prevention services and commercial organisations would not be required to provide details of the fraud and crime prevention processing they undertake to consumers as this would alert criminals and tip them off, save as allowed for in terms of the Promotion to Access of Information Act.
* Fraud prevention services and commercial organisations should be required to advise subjects implicated in fraud cases that data about them had been filed on fraud prevention databases.
* Consumers would not have a right of subject access to fraud prevention data as this would alert criminals to the possibility of apprehension and prosecution, would compromise investigations and lead to a different pattern of attack probably from a new location.
* Fraud prevention systems should not be open to public inspection.

The Commission's recommendation is therefore that the processing of personal information carried out on behalf of national security, defence or public safety or the purpose of which is the prevention, investigation or proof of criminal offences should be excluded from the ambit of the Bill to the extent that proper safeguards have been established in specific legislation for the protection of such personal information. Additional provision should furthermore be made for exemptions to be granted to responsible parties in specific circumstances.[179] This seems to be in accordance with the views expressed by the majority of commentators and is also in accordance with international practice. See clause 3 at 138 below.

(vii) Special personal information[180] (sensitive information)

3.3.101 The EU Directive lays down additional conditions (over and above the usual criteria for making processing lawful) for the processing of so-called "special categories of information (usually referred to as special or sensitive information).[181]

3.3.102 Most European countries agree on the main categories of information to be regarded as sensitive information (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and information concerning health or sex life), but some add further categories (information on debts, financial standing, criminal convictions and the payment of welfare benefits).

3.3.103 The U.S. Federal Trade Commission[182] also expressed their concern that information of a much more personal nature, such as race, health, financial standing, sexual orientation, is collected, frequently without any indication of how this information is subsequently to be used. In particular, the disclosure of such information to other parties must be controlled, if not prevented altogether. Very stringent rules should apply to processing special information.

---

179 See para 4.4 in Chapter 4 dealing with exemptions from privacy principles.

180 See, however, Protection of Information Bill for the use of the term "sensitive information" in another context. See also discussion above regarding the differences between critical, sensitive and special information.

181 Article 8(1) of the EU Directive provides as follows:

The processing of special categories of data
1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

182 US Federal Trade Commission ***Privacy Online: A Report to Congress*** June 1998.

In principle, such information should not be processed. However, derogation from the principle should be tolerated under very specific circumstances, such as:

* where the data subject has given explicit consent to process special information, but then only in respect of the purpose for which consent has been given; and

* the processing of special information as mandated by law, but then only to the extent that legitimate general public interest or state security outweighs the invasion of the privacy of an individual.

3.3.104 It was further stated that where it is impossible for the data subject to consent (eg. a blood test of an unconscious victim of a road accident), processing of such special information must be carried out reasonably and in the data subject's best interests and only to the extent necessary.

3.3.105 The specific protection of the personal information of children has furthermore recently become topical. The Commission has decided to make specific provision for the protection of the personal information of children in its final report[183] and also in the proposed Bill.[184]

3.3.106 In principle the processing of special information is therefore a cause for concern worldwide and therefore often subject to certain listed exceptions. These exceptions are usually set out in ways corresponding to the ones listed in the Directive.[185]

---

183 Discussion on the position of children's privacy in Chapter 4 below.

184 Clauses 25 and 32 of the Bill.

185 Article 8(1) of the EU Directive provides as follows:

The processing of special categories of data

1. .....

2. Paragraph 1 shall not apply where:
(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law insofar as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the

3.3.107 The Commission therefore recommends that specific provision be made for the protection of special personal information, including personal information relating to children. See the discussion in this regard in Chapter 4 of the report below (Principles) and in the proposed Bill, clause 25 and further.

(viii) Household activity

3.3.108 In the discussion papers it was stated that the legislation will not cover personal information kept by a natural person in the course of a purely personal or household activity.

3.3.109 Mixed reaction was received on this question. Some respondents agreed with the Commission's preliminary view.[186] The Commission was, however, requested to explain, by way of examples, the exact meaning of information kept "in the course of a purely personal or household activity" since the phrase seems superficially to require exclusion, but it was felt that it is rather vague.[187]

3.3.110 It was pointed out that all types of information have a conceivable commercial value. For instance, names and postal addresses can be valuable for direct marketing. In modern

---

establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority.
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

186 LOA.

187 Financial Services Board.

society, even the number of socks a person has, their colours, sizes, and so on, is potentially of economic value.[188]

3.3.111 Although this may be true, it is, however, important to note that some confusion can be prevented if one takes into account that it is not the nature of the information that is at stake here, but rather the use to which it is put by the collector. A directory of telephone numbers and addresses of friends or acquaintances kept for personal use at home, should therefore not be considered to be processing of personal information and need not be regulated by an information protection law.[189]

3.3.112 However, household information is growing exponentially in the modern world, and it is, of course, not always easy to determine when such information is purely for private use, or when there is economic potential, or potential for abuse.[190] This will, however, be a factual question.[191]

3.3.113 It is therefore the Commission's view that the proposed Bill should not cover personal information kept and used by a person in the course of a purely personal or household activity. See clause 3 at 138 below.

(ix) Anonymised/de-identified information

3.3.114 For the purposes of this discussion the term de-identify has been defined as follows:

> **"de-identify"** in relation to personal information of a data subject, means to delete any information that -
>
> a) identifies the data subject;

188 LOA.

189 Roos 1998 ***THRHR*** at 523.

190 LOA.

191 See also the processing of manual information not being stored in a filing system, para (i) above.

b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

c) can be linked by a reasonably foreseeable method to other information that identifies the data subject or that can be [used or] manipulated by a reasonably foreseeable method to identify the data subject; [192]

3.3.115 The ability to identify a person - or reasonably ascertain a person's identity - from a piece of information is the key component that makes the information personal information.

3.3.116 Possible abuses of ineffective protection of personal information, also in genomic research, range from embarrassment, blackmail, fraud, group stigmatisation, to negative discrimination for health or life insurance, employment, promotion, mortgages, or loans. Another possible abuse may be uncontested parentage testing. [193]

3.3.117 Existing legislation and guidelines in use in South Africa do not adequately address the distinction between identifiable and non-identifiable information about individuals. Since the legislation makes no specific reference to de-identified information, it tends to treat all information about individuals as identifiable information, with corresponding tight restrictions on access to and processing of the information. Examples are:

* Section 16 of the National Health Act, 2003[194] which makes limited reference to circumstances where patient records used contain 'no information as to the identity of the user concerned', but does not provide a description of what this means in practice.
* The definition of 'personal information' used in the Promotion of Access to Information Act and other legislation, and

192 Clause 1 of the Bill.

193 Lowrance WW "Privacy, Confidentiality, and Identifiability in Genomic Research" Paper delivered at the 29th International Conference of Data Protection and Privacy Commissioners September 2007 (hereafter referred to as "Lowrance paper") at 32.

194 National Health Act 61 of 2003.

* the definition of 'personal health information' in a recent report by the Council for Medical Schemes that is so wide that it could be very difficult to de-identify information.[195]

3.3.118 It was pointed out[196] that the proposed legislation would address the issue of the differences in requirements for dealing with identifiable and de-identified information about individuals more effectively than has been the case up to now in South Africa legislation and guidelines.

3.3.119 This issue is of particular concern in public health research, which typically requires access to de-identified information from multiple patients. In the absence of guidelines in the legislation, there is a tendency to assume that access to all information on individuals requires specific consent, which is virtually impossible, especially in the case of large studies. Moreover, where information is de-identified, an argument could be made that the potential benefits of obtaining access to information for public health research far outweigh the small potential risk to individuals of using their information for such studies, but the current state of legislation makes it difficult to sustain such an argument. The collection and use of profiles and statistical information that are valuable for the purposes of monitoring issues of public health and safety, the conduct of medical research, epidemiological research and professional quality assurance programs, all of which contribute to an effective and accountable commercial environment, should not be undermined.

3.3.120 The view was posed that "anonymised/de-identified information" should be exempt from the privacy legislation if it has been audited and proved to be unable to be re-identified. This is key to ensuring that compliance costs for business are kept to a minimum by business.[197]

---

195 It was argued that the definitions of anonymised and de-identified data used in Issue Paper 24, reflect an important improvement on other legislation and guidelines, which do not provide any such definitions. These definitions will be very useful in addressing issues related to de-identified and anonymised data even before the proposed Act comes into force, including the problem of definitions referred to above. The proposed Act will be even more helpful in this regard if the issues highlighted above are addressed in a way which can also be applied in the interpretation of related legislation.

196 Medical Research Council.

197 IMS; Law Society of South Africa.

3.3.121 However, the Commission was referred[198] to the work done by Sweeney and Samarati that shows that information can indeed be used in non-obvious ways to identify (some) individuals about whom 'anonymous' information has been recorded. The question was therefore posed whether such non-obvious techniques are 'reasonably foreseeable', given the fact that they have been reported in the scientific literature.[199] It was therefore argued that information about which there is any doubt in respect of the ability to re-identify a person, should be subject to the proposed legislation.[200]

3.3.122 The success rate for re-identification has been found to be quite high under certain circumstances.[201] Understanding how re-identification can be performed and what the risks of successful re-identification are can assist the development of more effective techniques for de-identification.[202] It would, however, not be possible to exclude every possible risk completely.

3.3.123 Sizing up risks of any kind involves two activities. First,"risk assessment" estimates the probability of undesired events compounded by the severity of the likely consequences. Then "risk appraisal" weighs the risks in perspective of personal or societal values. The risks are then weighed against benefits gained and one considers whether the risks are acceptable.[203] The same balancing act is necessary where de-identification is concerned. The challenge is to protect privacy and foster research at the same time.[204]

3.3.124 In practical and technical terms one would, furthermore, have to ensure that the definition of "processing" must not be interpreted so broadly as to capture the process of de-

198 Prof Martin Olivier.

199 Cell C furthermore posed the question at what stage and by whom the information is de-identified?

200 South African Medical Research Council.

201 El Amam, K "Anonymization and Health Research" Paper delivered at the Health Information Privacy Day, Toronto, September 24, 2007 where it was described how Canadians can be re-identified through record linkage, in particular using publicly available registers.

202 El Emam, K, Jonker, E, Sams, S, Neri, E, Neisa, A, Gao, T & Chowdry, S "Pan-Canadian De-Identification Guidelines for Personal Health Information" April 2007 Paper delivered at the 29th International Conference of Data Protection and Privacy Commissioners Montreal 26 September 2007 at 7-8.

203 Lowrance paper at 31.

204 Lowrance paper at 12.

identifying information.[205] It was argued[206] that since "removal" may be interpreted as being interchangeable with "deletion", a very strong case exists on the surface for the action of "de-identification" to be captured by the definition of "data processing". This is obviously "at odds" with "protecting" personal information, given that the intention of the proposed legislation is to protect the privacy of the individual - not to hamper processes that enhance that right to individual privacy. Anonymisation enhances privacy of the individual and this goal should be actively pursued by organisations that may collect personal information.

3.3.125 The question is therefore whether consent must be given for the de-identification of personal information to occur (i.e. consent to remove identifying details). It was suggested that the process of de-identifying information be handled in terms of the provisions for exemptions in terms of this Bill, eg by a health research ethics committee.[207]

3.3.126 In the USA the rules made under the Health Insurance Portability and Accountability Act of 1996 (the "HIPAA") are in force[208]. The HIPAA will apply to "individually identifiable health information". The definition of "health information" excludes professional provider information, as it applies only to information about the individual receiving health care. Once information has been de-identified – anonymised – it is deemed no longer to be identifiable health information and may be disclosed without restriction. However, if codes or other record identification methods are disclosed and allow subsequent re-identification of the information, or if the information is in fact re-identified, the previous restrictions apply. HIPAA is noteworthy amongst privacy statutes for setting out (at some length) standards and methods of how de-identification is to be undertaken.

3.3.127 After evaluating the arguments set out above as well as the comments received, the Commission recommends that anonymised/de-identified information be excluded from the proposed legislation on condition that it cannot be re-identified. See clause 3 at 138 below.

---

205 Borking Consultancy, Data Protection and Privacy Commissioners Conference in Sydney, September 2003.

206 IMS.

207 South African Medical Research Council.

208 Notwithstanding industry opposition, the rules came into effect on April 14, 2001, entities had two years in which to comply. See U.S. Department of Health and Human Services "Protecting the Privacy of Patients' Health Information" ***HHS Fact Sheet***, 9 May 2001.

(x) Professional information (including provider information)[209]

3.3.128 A submission was received on Issue Paper 24[210] proposing that "professional information" should be excluded from the proposed privacy legislation and that "provider information" should be recognised as a part of professional information.

3.3.129 "Professional information" was defined as:

> (a) the name, title, contact information, identifying code and professional designation of an identifiable individual , and
> (b) information describing the activities and transactions the individual has engaged in carrying out those responsibilities, including a description of those responsibilities when it is used for the purpose of describing the professional or official responsibilities of the individual".[211]

3.3.130 The importance of this interpretation is that a distinction is drawn between information relating to the performance of the individual in their professional, official or business capacity where the information has the potential to influence public interest, national security and public health and safety and the same individual in their personal or private capacities.

3.3.131 The definition of "professional information" should also exclude from the ambit of the Bill information that all types of businesses utilise about individuals with whom they interact in their business or professional capacity.[212]

---

209 See also the discussion on natural v juristic persons in para 3.3(b)(iv) above.

210 IMS.

211 Innovative Medicines SA (IMSA) requested that commercial data should also protected on par with the protection offered to personal data. However, this falls outside the ambit of this Bill.

212 For example, when a business negotiates a contract with a supplier, the business' staff and those of the supplier will prepare notes on the progress of the negotiations, setting out, amongst other matters, the position of the respective parties to the contract, comments on the negotiations etc. All of this information is provided in the individuals" professional capacity as a representative of the business. It is a business-to-business transaction. Any recorded information about the individual's views, or perspective on the proposed business arrangement is created and used solely because the individual represents a potential business partner – it bears no relation to the individual as an individual person. Rather it is important to business as it reflects the corporate position of the company they represent.

3.3.132 It was furthermore proposed that in the health sector the definition of personal health information should be drafted to ensure that information about the employment and business responsibilities, activities and transactions of individual health service providers is not included. This type of information may be used to objectively assess the quality of provider services and should be considered professional in nature rather than personal health information.

3.3.133 It is certainly difficult to discern how an individual prescription can constitute personal information about the physician who wrote it. While it can be revealing with regard to the patient – the nature of an illness or condition, for instance, and perhaps its severity – it discloses little or nothing about the physician as an individual. The prescription is not, in any meaningful sense, "about" the physician.[213] It does not tell us how he goes about his activities. Indeed, a prescription is not normally treated as personal information about himself or herself by the prescribing physician. The patient is not enjoined to secrecy, remaining entirely free to show it to anyone at will, or to leave it unattended in a public place.[214]

3.3.134 It was argued that with the exclusion of "professional information" from the definition of "personal information" in information protection legislation, an individual's rightful expectation of personal privacy is met whilst ensuring that the individual remains accountable to society in their capacity as an employee, worker, public officer, government official or professional.

3.3.135 It was furthermore argued that provider information forms part of professional information. IMS Health Canada and USA use prescription sales information and various statistical methods to produce provider information in the form of estimates of normative prescribing patterns of physicians, as well as estimates respecting individual physicians' prescribing patterns. After tracking prescription trends, IMS Health Canada and USA then make the information available under strict contractual arrangements to pharmaceutical companies, health professional bodies, government, medical researchers and patient advocacy groups for

---

213 However, a collection of all the prescriptions of a doctor may reveal that he is incompetent or favours the medicine of one supplier over the other, etc.

214 See Jones C, Rankin TM and Rowan J "A Comparative Analysis of Law and Policy on Access to Health Care Provider Data: Do Physicians have a Privacy Right over the Prescriptions they Write?" ***Canadian Journal of Administrative Law and Practice*** 2001.

a variety of purposes. These purposes provide a multitude of benefits to the health sector which enable the sector to provide more efficient, effective and transparent services.[215]

3.3.136 IMS Health Canada only discloses estimates respecting an individual physician's prescribing patterns with the express consent of the individual prescriber; otherwise, provider information is disclosed only in aggregate form. In the aggregate format, actual prescribing activity of individual prescribers is not identified – rather, prescribers are assigned a number that depicts the average prescribing activity of members of the entire group

3.3.137 The public benefits that flow from access to provider information, including improving the efficiency of the health care system, clearly militate in favour of allowing wide access to this information.

3.3.138 Medical research, quality assurance of government health programs, efficient monitoring of healthcare funding requirements and fraud prevention all require that some health information be accessible. Prescription records, which neither identify a patient nor reveal the medical history (that is, personal health information) of any person, should be the most widely used source of information for these purposes.

3.3.139 The Commission has already proposed that de-identified information be excluded from the ambit of the Bill.[216] This exemption will most probably provide the necessary relief sought in so far as provider information is concerned. It is, however, the Commission's recommendation that professional information should be included in the definition of personal information in so far as it would be applicable. See also the discussion on juristic persons above. It is furthermore of importance to note that the Commissioner may authorise the processing of personal information under specified circumstances. See Chapter 4 below for a discussion of exemptions from the information principles.

(xi) Processing of information for journalistic, artistic or literary purposes

215 A document outlining these benefits is included as "Benefit of IMS data Canada.pdf" in "Issue Paper Ancillary Docs.zip".

216 See para 3.3(b) (ix) above.

3.3.140 The Commission's preliminary proposal in the Discussion Paper was that no specific provision should be made for exemptions regarding the processing of personal information for journalistic, artistic or literary expression.[217]

3.3.141 It was argued that, at a time when disseminating information to the public can be done by anyone or any group through simple web sites, without the need for elaborate media infrastructure, the scope - and indeed validity of such exceptions - becomes extremely questionable. It is also very difficult to draw the line between purely factual information (such as directories) and journalistic information as the two are often linked or combined, for instance from one web page to another page, where the user can find an interview on a second page with the person listed on the first page.[218]

3.3.142 However, in the submissions received, the following points were, inter alia, made:[219]

a) The definition of "processing" appears to be broad enough to target the day-to-day activities of the media in gathering news, processing personal information in relation to that news, and publishing that news to the public. Furthermore, whenever a person, such as an editor of a newspaper, is responsible for the publication of hard copies that reproduce information that has previously been processed, this may itself constitute "processing" and accordingly be hit by the draft legislation.[220]

b) The speed with which the day-to-day tasks, involving the use of electronic equipment, such as the laptop and the modern printing press, in translating information into the printed newspaper, have to be carried out if a newspaper is to publish news, renders it impractical to comply with many of the data processing principles. The Commission was specifically referred to the *Campbell*

---

217 See para 4.4.25 (e) of the Discussion Paper and the preceding discussion in this regard. This argument was supported by various commentators eg Law Society of SA; Vodacom (Pty) Ltd.

218 Korff ***Comparative Study*** at 137.

219 Dario Milo, Webber, Wentzel and Bowens Attorneys.

220 ***Campbell v MGN Limited*** [2002]EWCA Civ 1371; [2003]QB633 (CA).

case[221] where the English and Wales Court of Appeal (Civil Division) held that, save for the exemption provided for the media in section 32 of the UK Privacy Act, the Data Protection Act would impose restrictions on the media which would radically restrict the freedom of the press.[222]

c) It was therefore proposed that there should be a general exemption in the draft legislation in relation to processing of information where such processing is undertaken with a view to exercising the right of freedom of expression and specifically, in order to publish information of public concern to the public.

3.3.143 It should, at the outset, be noted that the proposed South African privacy legislation can be distinguished from that of the United Kingdom in that the South African proposals make provision for a number of exceptions[223] to the information protection principles that are not found in the United Kingdom Privacy Act. However, a more comprehensive consideration of the position seems appropriate, especially since the EU Directive does make provision for exemptions from its provisions for processing of information carried out for journalistic purposes.[224]

3.3.144 The right to freedom of expression is guaranteed under numerous international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[225] However, the right to privacy is equally protected.[226] There is, therefore, a need to ensure an appropriate balance between the public interest in allowing the free flow of information to the public through the media and the public interest in adequately safeguarding the protection of information.

---

221 Ibid.

222 Supra at para 124.

223 For eg.clause 17(6) (d) and (e) which makes provision for non-compliance of the notification provision where such notification would prejudice a lawful purpose of the collection of the information or where compliance would not be reasonably practicable in the circumstances.

224 See discussion in para 3.3.146 below.

225 For instance, art 19 of the ***United Nations Universal Declaration of Human Rights***, 1948 stresses the right "to receive and impart information and ideas through any media ...." article 9 of the ***African Charter on Human and People's Rights,*** 1981 provides for the "right to receive information". See also art 17 of the ***International Covenant on Civil and Political Rights,*** 1966, art 13 of the ***American Convention on Human Rights*** and section 16(1)(b) of the ***Constitution***. See also art 21(1)(a) of the ***Constitution of the Republic of Ghana*** 1992.

226 See discussion in Chapter 2 above.

3.3.145 The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) do not specifically provide for an exemption relating to journalistic activities. However, they do make provision for exceptions to the privacy principles which should be " limited to those necessary in a democratic society". [227]

3.3.146 The EU Directive states as follows in Art 9:

> Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

3.3.147 However, according to recital 37 no derogations from the rules on security shall be possible and the supervisory authorities responsible for this sector should, at least, be provided with certain ex-post facto powers such as the power to publish regular reports or to refer matters to the judicial authorities.

3.3.148 It should further be noted that the right to freedom of expression as guaranteed in Art 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[228] and Art 11 of the Charter of Fundamental Rights is available to everyone, not just to journalists, artists and writers.[229] It therefore seems as though the journalistic exemption in the Directive should be read broadly so as to encompass all cases in which the responsible party exercises his or her right to freedom of expression. Such considerations will be of particular importance to human rights organisations which collect sensitive information for purposes which are not solely "journalistic" in the narrow sense.[230]

---

227 Guideline 4.

228 Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 1950 establishes that:

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and to impart information and ideas without interference by public authority and regardless of frontiers.[..]
> See, however, also article 8 of the ECHR which guarantees the right to privacy.

229 See also section 16 of the Constitution.

230 Korff ***Comparative Study*** at 130.

3.3.149 The EU has furthermore indicated that the right to reply and the possibility to have false information corrected, the professional obligations of journalists and the special self-regulatory procedures attached to them, together with the law protecting honour (criminal and civil provisions concerning libel) must be taken into consideration when evaluating how privacy is protected in relation to the media.[231]

3.3.150 The laws in different EU countries regarding the processing of personal information for journalistic purposes[232] are widely divergent. They range from stipulating the overall primacy of freedom of expression, through wide exemptions for the press, to a system which imposes restraint on the publication of certain information by the press.[233]

3.3.151 The different national laws currently address the issue by taking one of the following approaches:[234]

a) In some cases information protection legislation does not confer any express exemption from the application of its provisions to the media. This is the current situation in Belgium, Spain, Portugal, and Sweden.

b) In other cases the media are exempted from the application of several provisions of data protection legislation. This is the current situation in the case of Germany, France, The Netherlands, United Kingdom, Austria and Finland. Similar derogations are envisaged by the draft Italian legislation.

c) In other cases the media are exempted from general data protection legislation and regulated by specific data protection provisions. This is the case in Denmark for all media and in Germany in relation to public broadcasters, which are not covered by federal or Länder data protection laws, but are subject to specific data protection provisions in the inter-Länder treaties which regulate them.

---

231 Working Party Recommendation 1/97 at 7.

232 The term "media" refers to all the different means of mass communication including press, radio and television broadcasting.

233 This divergence may raise problems regarding cross-border journalism.

234 European Union Art 29 Working Party ***Data protection law and the media*** Recommendation 1/97 Adopted by the Working Party on 25 February 1997 (hereafter referred to as "WP Recommendation 1/97") at 6; See also ***Personal Information Protection and Electronic Documents Act*** 2000 SC,c 5 (Canada) sections 4(2)(c),7(1)(c); ***Data Protection Act*** 1998 (UK) section 32; ***Privacy Act*** 1993 (NZ) section 2(1); ***Personal Data (Privacy) Ordinance (Hong Kong)*** section 61.

3.3.152 The differences between these three models should not, however, be over-stated. In most cases, independently of any express derogation that may exist, data protection legislation does not apply fully to the media because of the special constitutional status of the rules on freedom of expression and freedom of the press. These rules place a de facto limit on the application of substantive data protection provisions or at least their effective enforcement.

3.3.153 The law in the Netherlands exempts processing for exclusively journalistic, artistic or literary purposes from a limited range of provisions.[235] This is a change from the previous Act which gave full exemption. Such processing is not subject to the duty to inform data subjects, to the exercise of data subject rights or to notification and prior checks. The section does not, however, exempt such processing from the information protection principles and criteria.

3.3.154 The UK law, in section 32, also contains a qualified exemption for processing for journalistic, artistic and literary purposes.[236] Subject to certain substantive and procedural

---

235 Article 3 of the ***Dutch Personal Data Protection Act,*** 2000 reads as follows:
1. This Act does not apply to the processing of personal data for exclusively journalistic, artistic or literary purposes, except where otherwise provided in this Chapter and in Articles 6 to 11, 13, 15, 25 and 49.
2. The prohibition on processing personal data referred to in Article 16 does not apply where this is necessary for the purposes referred to under (1).
(Section 16 deals with the processing of special personal data.)

236 **Journalism, literature and art.**
32. - (1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if-

(a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,

(b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and

(c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

(2) Subsection (1) relates to the provisions of-

(a) the data protection principles except the seventh data protection principle,

(b) section 7,

(c) section 10,

(d) section 12, and

(e) section 14(1) to (3).

(3) In considering for the purposes of subsection (1)(b) whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which-

(a) is relevant to the publication in question, and

(b) is designated by the Secretary of State by order for the purposes of this subsection.

(4) Where at any time ("the relevant time") in any proceedings against a data controller under section 7(9), 10(4), 12(8) or 14 or by virtue of section 13 the data controller claims, or it appears to the court, that any personal data to which the proceedings relate are being processed-

(a) only for the special purposes, and

(b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time twenty-four hours immediately before the relevant time, had not previously been published by the data controller, the court shall stay the proceedings until either of the conditions in subsection (5) is met.

conditions, personal information which is processed for any of these purposes solely with a view to publication of any "journalistic, literary or artistic material" and which the responsible party (data controller) "reasonably believes" to be "in the public interest" is exempt from the information protection principles and from the exercise of data subject rights. The conditions are somewhat complex, but were designed to ensure that in practice the emphasis would remain on the self-regulatory control of the press under the press code of practice.[237]

3.3.155 In Australia, under section 7B(4) of the Privacy Act 1988 acts and practices of a "media organisation" in the course of journalism are exempt from the operation of the Act if the organisation is publicly committed to observe privacy standards that have been published in writing, either by the organisation, or by a person or body representing a class of media organisations.[238] The Australian Press Council developed a code entitled " Privacy Standards for the Print Media" in 2001[239] and has had a positive experience with administering the standards. It is the Council's view that the exemption is working effectively and that no changes are needed. The majority of complaints are settled by conciliation, early in the process, and those settled by adjudication do not demonstrate any egregious abuse of citizen's private rights.[240] The Australian Law Reform Commission has, however, highlighted the problem (also raised by other stakeholders) that the terms of the exemption are silent on the adequacy of media privacy standards. Their preliminary proposal is therefore that criteria should be established in consultation with all the stakeholders and published by the Office of the Privacy Commission in the form of guidelines. The exclusion should be amended in order to ensure that organisations will deal "adequately" with privacy in the context of their activities.

---

(5) Those conditions are-

(a) that a determination of the Commissioner under section 45 with respect to the data in question takes effect, or

(b) in a case where the proceedings were stayed on the making of a claim, that the claim is withdrawn.

(6) For the purposes of this Act "publish", in relation to journalistic, literary or artistic material, means make available to the public or any section of the public.

237 Korff ***Comparative Study*** at 136.

238 ***ALRC Discussion Paper*** at 1081.

239 To be distinguished from the broadcasting media where a co-regulatory system (as opposed to a self-regulatory system for the printed media) is in place.

240 Australian Press Council "Australian Press Council Submissions to the Australian Law Reform Commission in response to its inquiry into the Privacy Act 1988" 8 August 2006.

3.3.156 In South Africa the different competing constitutional rights most relevant to this matter, as entrenched in the Bill of Rights, are the right to privacy (section 14), the right to human section 16). These rights are interactive, and need to be balanced. The Constitution does not accord hierarchical precedence to any particular right entrenched in the Bill of Rights over other rights referred to therein.[241]

3.3.157 Section 16 of the Constitution protects the right to freedom of expression.[242] It protects free expression generally, but also specifically includes freedom of the press and the media.[243] Information on this subject in our common law is limited since it is only recently that the mass media have started to play a significant role.

3.3.158 The right to freedom of speech and expression, like the other fundamental rights and freedoms entrenched in the Bill of Rights, is not absolute.[244] Boundaries are set by the rights of others and by the legitimate needs of society. Section 36 of the South African Constitution is a general limitation clause and sets out specific criteria for the limitation of the fundamental rights in the Bill of Rights.[245]

3.3.159 It is the delicate balance between freedom of the press and the protection of individual privacy, reputation and dignity which has to be determined. In determining the current modes of thought and values of the community, the boni mores or convictions of the community regarding right and wrong are of particular importance. This is a test analogous to that of the unlawfulness inquiry under the common-law actio iniuriarum.[246]

---

241 ***Johncom Media Investments Limited v Mandel ao*** Case CCT 08/08 [2009] ZACC 5 at para [19].

242 Section 16 of the **Constitution** provides:

Freedom of expression
16. (1) Everyone has the right to freedom of expression, which includes -
(a) freedom of the press and other media;
(b) freedom to receive or impart information or ideas;
(c) freedom of artistic creativity; and
(d) academic freedom and freedom of scientific research.

243 The importance of the right to freedom of expression has been acknowledged in ***Islamic Unity Convention v Independent Broadcasting Authority and Others*** 2002 (4) SA 294 (CC); 2002 (5) BCLR 433 (CC).

244 See discussion in Chapter 2 above; See also ***Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International*** 2006 (1) SA 144 (CC);2005(8) BCLR 743 (CC) at para 47 where Moseneke J said the right to free expession in our Constitution is neither paramount over other guaranteed rights nor limitless..

245 See discussion in Chapter 2 above; ***Tshabalala-Msimang ao v Makhanya ao*** Witwatersrand High Court Case Number 18656/07 30 August 2007 at para [43] referring to ***Midi Television (Pty) Ltd v Director of Public Prosecutions,Western Cape*** 2007 (5) SA 540(SCA); 2007 (9) BCLR 958 (SCA) at para [9]-[11]**:** "In other words, one has to weigh the extent of the limitation against the purpose, importance and effect of the intrusion and this entails weighing the benefit that flows from allowing the intrusion against the loss that that intrusion will entail."

246 Burchell at 416.

3.3.160 The list of values that underpins freedom of expression is not closed, but three main justifications for freedom of expression have been advanced:[247]

(a) That the free exchange of ideas is the best way of attaining the truth (the marketplace of ideas theory);[248]

(b) Freedom of expression is a vital part of the democratic process; [249] and

(c) It is a manifestation of individual autonomy and self-fulfilment.

3.3.161 Burchell[250] refers to the fact that the general principle of media freedom was dealt damaging blows by both the legislature and the judiciary during the years of apartheid.[251] This position changed only recently when the Supreme Court of Appeal in **National Media Ltd v Bogoshi,**[252] reaffirmed its commitment to freedom of expression, including media freedom, holding that it was an essential foundation of a democratic society.[253]

3.3.162 The Supreme Court of Appeal in **National Media v Bogoshi**[254] furthermore acknowledged that the standard defences excluding unlawfulness do not necessarily cover all

---

247 Marcus G & Spitz D "Expression " in Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D & Woolman,S (eds) ***Constitutional Law of South Africa*** Juta Kenwyn 1996 (Revision Service 5 1999) (hereinafter referred to as "Chaskalson et al") at 20C6; Burchell 1-2. The three main justifications for freedom of expression can be subdivided further into two broad types -- those that stress that the freedom in question will produce desirable consequences for society (the instrumental, utilitarian or consequentialist theory) and those that stress responsibility, individual autonomy or human dignity rather than the consequences for society (the constitutive, intrinsic or non-consequentialist theory). A further subdivision can be made between those who regard freedom of expression as absolute and those who openly acknowledge that freedom of expression is relative, that is, who acknowledge that it must be balanced against the exercise of other rights.

248 ***Gardener v Whitaker*** 1995 (2) SA 672 (E) at 687 I-J; 1994 (5) BCLR 19(E) at 34A. See also ***R v Keegstra*** [1990] 3 SCR 697 at 729, 3 CRR (ZA) 193, where it was stated that freedom of expression extends to all expression, however unpopular, distasteful or contrary to the mainstream.

249 The democratic process is furthered by the formation of an informed citizenry.

250 Burchell ***SALJ*** at 1.

251 In ***Pakendorf v De Flamingh*** 1982 (3) SA 146 (A) the Appellate Division interpreted the common law to impose strict (no-fault) liability on the mass media for defamation, not including the individual in this strict regimen. A further judicial blow to freedom of expression was delivered when in ***Neethling v Du Preez: Neethling v The Weekly Mail*** 1994 (1) SA 708 (A) the Appellate Division saddled the defendant (including the media) with the burden of proving the set defences to a defamation action on a preponderance of probabilities.

252 Supra; It held that the approach in ***Pakendorf*** was clearly wrong and must be overruled. The strict liability rule for defamation was replaced with the rule that the crucial test was whether the publication was reasonable; See also ***Mthembi - Mahanyele v Mail and Guardian Ltd*** 2004 (6) SA 329 (SCA).

253 Burchell at 4; See especially Cameron J in ***Holomisa v Argus Newspapers Ltd*** 1996 (2) SA 588 (W);1996 (6) BCLR 836 (W). Joffe J in ***Government of the Republic of South Africa v Sunday Times Newspaper*** 1995 (2) SA 221 (T) at 227-8, cited with approval by Hefer JA in ***National Media Ltd v Bogoshi*** supra.

254 Supra.

possible policy issues, and so the distinction between constitutional justification in terms of the limitation clause and common-law justifications, in terms of a broad reasonableness criterion, is becoming increasingly blurred.[255] It was stated that the test for the reasonableness of the publication demands a high degree of circumspection on the part of editors. [256]

3.3.163 In a discussion of the **Bogoshi** case in **Tshabalala-Msimang v Makhanya**[257] the Court noted with approval that the **Bogoshi** approach resulted in the creation of clearly identifiable and operational norms, and the fostering in the media of a value of care and responsibility. [258]

3.3.164 However, in **Holomisa v Argus Newspapers,**[259] Cameron J recognised the special role of the press in a constitutional democracy but stated that this does not mean that the journalists must enjoy special constitutional immunity beyond that accorded to ordinary citizens.[260] Cameron J described the idea of "press exceptionalism" not only as unconvincing but also as dangerous. The right of the media to communicate information and comment, while obviously crucial in a modern democracy, should be no greater than that of an ordinary citizen

---

255 Burchell at 388.

256 ***Bogoshi*** supra at 1212G -1213C; In this case, which deals with defamation, it was indicated that this test includes factors such as: (a) the time and manner of the publication; (b) the status or degree of public concern in the information; (c) its political importance; (d) the tone of the publication; (e) reliability of the source; (f) the steps taken to verify the information, whether the person referred to has been given an opportunity to verify, comment on or reply to the allegation. In Burchell JM "Media Freedom of Expression Scores as Strict Liability Receives the Red Card: ***National Media Ltd v Bogoshi"*** 1999 **SALJ** 1 (hereinafter referred to as "Burchell ***SALJ***") Burchell adds two further factors for determining the bounds of unlawfulness, namely (a) the nature of the publication; and (b) ethical responsibilities laid down for the media in codes of conduct assumed voluntarily or required by statute. On the other hand, in so far as the infringement of privacy is concerned, ***Neethling's Law of Personality*** at 271-272 and Burchell at 416 hold that the common law recognises a number of limited exceptions to the general rule. Although one is dependent on the general legal convictions of the community *(boni mores*) in all cases, there are certain factors, especially apparent in foreign legal sources, which can assist in the application of this criterion: (a) the fact that the plaintiff is a public figure; (b) the fact that the plaintiff is involved in a newsworthy event; (c) the extent or intensity of the violating conduct; (d) the fact that the holder of the right exposes his or her privacy to the risk of violation; (e) the motive, disposition or purpose with which the defendant acts; (f) the fact that the private facts were obtained by a wrongful act of intrusion; (g) the importance of the person involved and his or her status in society; (h) the time-span between the occurrence of a newsworthy event and the publication thereof; (i) the degree of identifiability of the person whose privacy is disclosed; and (j) the fact that the publication of private facts was contrary to a court order or statutory provision. It is submitted that such a provision reflects the *boni mores* and is consequently in the public interest.

257 Supra.

258 ***Tshabalala-Msimang v Makhanya*** supra at para [49] referring to ***Bogoshi*** at para [203] and [204].

259 Supra.

260 Ibid 855-6. Cameron J referred to the following argument of Ronald Dworkin in a ***Matter of Principle*** 1985 386-7: "But if free speech is justified on principle, then it would be outrageous to suppose that journalists should have special protection not available to others, because that would claim that they are, as individuals, more important or worthier of more concern than others."

to communicate.[261] Media freedom should therefore not constitute a plea for privileged status but rather a recognition of the right of the public to be informed.[262]

3.3.165 It is therefore a vital function of the media to inform the public about every aspect of public, political, social and economic activity and thus to contribute to the formation of public opinion.[263]

3.3.166 One should, however, also take note of the capacity of the media, and in particular the tabloid press, to sensationalise[264] and to trivialise sensitive issues and matters of great emotional importance to the individual concerned .[265]

3.3.167 It may, therefore, be necessary for the state , by virtue of its greater power, to lay down conditions restricting the rights and freedoms of its subordinates in the public interest.[266] It stands to reason, especially in light of the entrenchment of freedom of speech in the Constitution, that the public interest in information should not be narrowly construed.[267] On the other hand, this does not imply that the protection thereof is unlimited. It is for instance limited by the right to privacy of persons.

---

261 Burchell states at 17 that while freedom of expression is a vital component of both the democratic process and individual self-fulfilment, it is nevertheless merely a facet of human dignity. To elevate freedom of expression to an absolute right or even to a position of pre-eminence in a hierarchy of rights is to distract attention from the true origin of the right freely to express one's views or opinions through words or conduct. It is part of the dignity that is accorded to thinking and sentient human beings. See, furthermore, the minority judgement of Langa J in ***NM ao v Smith* ao** at para [94] where he stated that the media should be held to a higher standard than the average person. in so far as liability for any disclosures which they should reasonably have foreseen would cause harm.

262 Chaskalson at 20C20; Burchell at 5 and the references made there. In ***Neethling v Du Preez : Neethling v The Weekly Mail*** supra at 777G-H Hoexter JA stated : "At common law there is no general "newspaper privilege". In ***Argus Printing and Publishing Co Ltd v Inkatha Freedom Party*** 1993 (3) SA 579 (A) Grosskopf JA notes that "...freedom of speech can never be an absolute". For the opposite view see Chaskalson at 20.20.

263 ***National Media Ltd v Bogoshi*** supra at 1209H-J; ***Tshabalala-Msimang v Makhanya*** supra at para [38].

264 Mr G J Van Zyl on behalf of the Head of the Office of the Family Advocate, Pretoria in a letter to the Commission dated 20 December 1999 in response to the Discussion Paper on the publication of divorce proceedings.

265 Wall at 137.

266 ***Neethling's Law Of Personality*** at 266.

267 ***Neethling's Law of Personality*** at 268. However, "public interest" was defined narrowly in ***Financial Mail (Pty) Ltd v Sage Holdings Ltd*** 1993 (2) SA 451 (A).

3.3.168 In **Tshabala-Msimang ao v Makhanya ao**[268] the High Court noted that "public interest" is a mysterious concept and that there is little, if any, consensus on what exactly constitutes the public interest.[269] However, it was further stated that public interest will naturally depend on the nature of the information conveyed and on the situation of the parties involved. It is, furthermore, not merely the interests of those associated with the publication that need to be brought to account but, more important, the interests of every person having access to information. [270]

3.3.169 The question is therefore to what extent the publication of private facts concerning individuals is justified in the public interest? Two virtually identical tests are being applied in the American and German law.[271]The public has a legitimate right to be informed of -

(a) Newsworthy events; and

(b) The activities or lives of personalities in the public eye.[272]

3.3.170 It is especially the second category that is of interest to this investigation. Public figures are persons who, by virtue of their status, office, occupation, conduct and crimes, grant the public a legitimate interest in information regarding not only their public life and activities, but also, to a certain extent, their private lives.[273] They include statesmen, sporting heroes, business magnates, artists, etc.[274]

3.3.171 Even public figures who have voluntarily sought the public gaze and have, to some extent, forfeited their right to privacy, have a residual realm of solitude where they have

---

268 Supra at par [37] and [43].

269 Para [37]: "Like a battered piece of string charged with elastic, impossible to measure or weigh. ..."

270 ***Tshabalala-Msimang v Makhanya*** supra at para [43].

271 ***Neethling's Law of Personality*** at 268 and the references made therein.

272 Burchell at 416.

273 ***Neethling's Law of Personality*** states at 269 that the term "public figure" should be restricted to persons who have become known in public to such an extent that they arouse public interest without necessarily being connected to a newsworthy event. In other words these people are newsworthy in themselves. See also Bell, Dewar & Hall at 79; See also McQuoid-Mason D "Invasion of Privacy?" 1973 90 ***SALJ*** 23 at [29] as referred to in ***Tshabalala-Msimang v Makhanya*** at para [39]: "... the test whether a person is a public figure should be: has he by his personality, status or conduct exposed himself to such a degree of publicity as to justify intrusion into, or a public discourse on, certain aspects of his private life?..."

274 ***Neethling's Law of Personality*** at 269; Burchell at 416.

a right to be let alone.[275] However, public figures, by the very nature of their public life and duty, often find it necessary to use the press to communicate on public issues.[276]

3.3.172 A distinction should be made between the public and private lives of these people.[277] It cannot simply be accepted that a legitimate interest in information exists also with regard to the private life of public figures and that only their most intimate life is protected against publicity.[278] In principle the private life of these persons should also be protected against publicity.[279] On the other hand it is quite conceivable that the public may in certain circumstances have a legitimate interest in information concerning even the sordid intimate life of, for example, a politician.[280] Thus it may be concluded that all the circumstances surrounding the publication of the statement invading the plaintiff's privacy must be considered in determining whether the statement is being made for the public benefit.

3.3.173 In **Tshabalala-Msimang v Makhanya** it was held that even where the information sought for publication is obtained by unlawful means,[281] there may well be overriding considerations of public interest which would permit its publication. However, any such interference must be both reasonable and necessary.[282] In this case the Court held that the publication of the unlawfully obtained controversial information was capable of contributing to the debate in democratic society relating to a politician in the exercise of her functions.[283] It further stated that ".. The revelations made are relevant to the first applicant's performance of her

---

275 Burchell at 416.

276 Mostert F "Public figures and privacy" ***De Rebus*** November 1997 (hereinafter referred to as "Mostert") at 726.

277 As far as people holding public office are concerned, their private lives must reflect their fitness to hold such office. A person's behaviour at home can be a guide to his or her standard of morality in public life. ***Hansard*** Thursday, 3 May 1979 at 5587.

278 ***Neethling's Law of Personality*** at 269; Burchell at 416.

279 Ibid.

280 One example was noted in a newspaper article by Ken Vernon, "Boesak and the Blond" ***Sunday Times*** 21 March 1999, where he states: "Ironically, one of the first people to blow the whistle on Boesak's extravagant lifestyle was Elna." Documents revealed in Boesak's fraud trial show that when she filed for divorce from Boesak in 1992, Elna gave a detailed explanation of Boesak's lifestyle and how money was spent. He was subsequently found guilty on fraud charges and served a jail sentence. The public furthermore has an interest in the fact that political figures should uphold high moral standards in accordance with their callings even where their conduct is not criminal.

281 See also ***Neethling's Law of Personality*** 246 ftnt 238 and the references made therein.

282 ***Tshabalala-Msimang v Makhanya*** at paras [34] and [40].

283 ***Tshabalala-Msimang v Makhanya*** at para [46].

constitutional and ministerial duties and are therefore ..... in the public interest".[284] The Court did, however, emphasise that the unlawful acquiring of the information could result in criminal charges being brought against the perpetrators and action by the South African Press ombudsman.[285]

3.3.174 Where a person is not a public figure, as a general rule, disclosures should not be made concerning his or her private way of life, standard of living, place of dwelling and the like.[286] There may, however, be a compelling public interest to disclose this kind of information.[287] This principle was confirmed by the Constitutional Court in the case of **NM ao v Smith ao (Freedom of Expression Institute as amicus curiae)**[288] where the respondents deliberately chose to use the names of the applicants instead of pseudonyms in order to give a book that they were writing, authenticity. The Court held that the public's interest in authenticity does not outweigh the public's interest in maintaining the confidentiality of private medical facts as well as the right to privacy and dignity that everybody should enjoy.

3.3.175 Disclosures concerning a person's family (eg his or her spouse or children) would seem prima facie to constitute an invasion of the privacy of members of the family directly concerned. Such disclosures, however, will once again not be actionable if they are in the public interest, and can be considered as being a valid news item.[289]

3.3.176 Mostert argues that one could furthermore expect of the media themselves to live up to the standards of professional integrity which they rightly demand of others. Voyeuristic journalism, which profits from prurient interest in lurid details, is out of keeping with a society that honors common decency, civility and respect.[290]

---

284 At para [44].

285 At para [55].

286 McQuoid-Mason D J ***The Law of Privacy in South Africa*** Juta & Company Ltd Johannesburg 1978 (hereinafter referred to as McQuoid Mason) at 177.

287 See ***Neethling Law of Personality*** 248 ftnt 242; ***NM v Smith*** at para [45].

288 2007(7) BCLR 751 (CC) at para [61].

289 McQuoid-Mason at 180.

290 Mostert at 726; See also Recommendation 1/97 at 8 where the WP said: "In evaluating whether exemptions or derogations are proportionate, attention must be paid to the existing ethics and professional obligations of journalists as well as to the self-regulatory forums of supervision provided by the profession."

3.3.177 In evaluating the arguments set out above, the Commission is of the opinion that the most appropriate way of balancing the competing principles of privacy and freedom of expression in the proposed Bill will be to grant media organisations a limited exclusion from the operation of the Bill.

3.3.178 In this regard it is important to note the current regulatory framework in place for the media. The Independent Communications Authority of South Africa is a product of statute.[291] It was established in July 2000 as a merger of the telecoms regulator and the broadcasting regulator.[292] It regulates the telecommunications and broadcasting industries in the public interest. Its key functions are to -[293]

a) make regulations and policies that govern broadcasting and telecommunications;
b) issue licences to providers of telecommunication services and broadcasters;
c) monitor the environment and enforce compliance with rules, regulations and policies;
d) hear and decide on disputes and complaints brought by industry or members of the public against licensees;
e) plan, control and manage the frequency spectrum; and
f) protect consumers from unfair business practices, poor quality services and harmful or inferior products.

In regulating the industry ICASA aligns its actions, policies and regulations with the framework set by international and regional bodies to which it is affiliated.

3.3.179 The Press Council of South Africa, the Press Ombudsman and the Press Appeals Panel form a self-regulatory mechanism set up by the print media to provide impartial, expeditious and cost-effective adjudication to settle disputes between newspapers and magazines, on the one hand, and members of the public, on the other, over the editorial content of publications. The Council has adopted the South African Press Code to guide journalists in their daily practice of gathering and distributing news and opinion and to guide the Ombudsman and the Appeals Panel; to reach decisions on complaints from the public. More than 640 publications, mainly members of Print Media South Africa, subscribe to the Code. The Council

---

291 The Independent Communication Authority of South Africa Amendment Act of 2000 (amended in 2005).

292 It also incorporates the postal regulator.

293 ICASA website accessed on 2 July 2008 at http://www.icasa.org.za/content/.

is the custodian of the Code and may amend it from time to time, depending on needs. The industry believes in self-regulation because it is the only way that rights of freedom of expression and freedom of the press and other media guaranteed in the Constitution can be truly expressed.[294]

3.3.180 Para 38 of the ICASA Code of Conduct[295] reads as follows:

> 38. Privacy
>
> Insofar as both news and comment are concerned, broadcasting licensees shall exercise exceptional care and consideration in matters involving the private lives and private concerns of individuals, bearing in mind that the right to privacy may be overridden by a legitimate public interest.

3.3.181 Similarly, para 1.10 of the South African Press Code reads as follows:

> 1.10 In both news and comment the press shall exercise exceptional care and consideration in matters involving the private lives and concerns of individuals, bearing in mind that any right to privacy may be overridden only by a legitimate public interest.

3.3.182 Although the codes of ethics referred to above both seem to embody the spirit of POPIA, neither currently makes specific provision for compliance with the information protection principles. Both codes do, however, cover the handling of complaints from the public dignity (section 10) and the right to freedom of ex pre ssion (.

3.3.183 The Commission recommends that the proposal in the Discussion Paper be confirmed that no specific provision be made for the exclusion from the Bill of processing of personal information for artistic and literary purposes. However, the processing of personal information for exclusively journalistic purposes should be excluded from the ambit of the Bill, subject to the condition that a responsible party will only be excluded if it is subject to a code of ethics, by virtue of office, employment or profession, that

---

294 Official web site of the Press Council of South Africa accessed on 2 July 2008 at http://www.presscouncil.org.za.

295 The "Code of Conduct for Broadcasters" published in accordance with section 78(1) of the Independent Broadcasting Authority Act 153 of 1993 with effect from 4 February 2003 applicable to all licenced broadcasters regardless of their mode of delivery.

adequately observes the privacy standards set out in the information protection principles. The effect of this exclusion is as follows:

a) The Bill will, in general, be applicable to the processing of personal information for journalistic purposes.

b) The exclusion makes provision for a form of self-regulation where responsible parties -

(i) are subject to a code of ethics by virtue of office, employment or profession; and

(ii) the code of ethics referred to in subpara (i) adequately observes the privacy standards set out in the information protection principles.

c) The proposal does not envisage that the Information Regulator will, in general,[296] be required to assess media privacy standards developed by a media organisation in its code of ethics in the absence of a complaint. However, if a complaint is made to the Regulator about the activities of a responsible party, the Regulator would be able to determine whether the privacy standards were adequate and therefore whether the media exemption applies in that instance.

d) The adequacy of enforcement mechanisms would also be a consideration when determining whether media standards are adequate. If the enforcement mechanisms are inadequate, the exemption will not apply.

e) The proposal does not preclude media institutions from making use, should they so prefer, of the provisions set out in Chapter 7 of POPIA in terms of which sector specific codes of conduct may be developed and issued.

(xii) Information in the public domain/public registers

3.3.184 The issue of public registers was not discussed in any detail in the discussion papers. It was accepted that the information protection principles would also apply to public registers except where specific exceptions in the principles made provision for their exclusion.[297]

296 See, however, clause 87 of the Bill.

297 See Principles 2 and 4 of the Bill.

3.3.185 The Commission, however, received a request from the Deeds Office[298] to exclude the operations of the Office from the ambit of the Bill completely, since it contains public records and it is in the public interest that deeds office records should be open to public scrutiny and such interest should take precedence over the right to privacy of the individual.

3.3.186 In another submission[299] it was submitted that the phrase "information in the public domain" should be used rather than the term "public record" (which was used but not defined in the draft Bill) and that the phrase "information in the public domain" should be properly defined as "information accessible to the public". It was further argued that, in light of the fact that the information is already in the public domain, the data subject should be aware of the fact that the public has access to certain personal information belonging to the data subject. There should therefore be a limited application of the information protection principles to information in the public domain. Only principles making provision for information quality, security safeguards, retention periods and access to or correction of information must apply to this kind of information. There should therefore be explicit exceptions from principles dealing with the consent of the data subject, making the data subject aware of the purposes of the collection and intended recipients, giving the data subject information regarding the details of the responsible party and collecting information directly from the data subject.

3.3.187 In so far as public sector information is concerned the European Union Working Party makes a distinction between information that must be made public by law, information which is accessible by law, and situations where the issue of publication of, or access to, public sector information is not regulated by law but is raised following a request from individuals or businesses.[300]

3.3.188 The question of public sector information has been discussed in the international sphere in various documents.[301] The European Commission submitted a Green Paper for

---

298 Submission from the Chief Registrar of Deeds, Pretoria.

299 Credit Bureau Association.

300 See discussion in para 3.3.185-186 above.

301 Volman Y "Public sector Information: A Key Resource for Europe" Presentation made at Bristol Conference 2 March 2005; Stewart B "Five Strategies for Addressing Public Register Privacy Problems" Office of the Privacy Commissioner New Zealand 30Septemebr 1999.

comment in 1998 entitled "Public Sector Information : A Key Resource for Europe".[302] This paper deals with the question how public sector information can be made more accessible to citizens and business and was produced in a response to the demands of public players who wanted low-cost access to public sector information and who disputed the continuing public sector monopoly in this area.

3.3.189 The EU Working Party published an Opinion in response to the Green Paper in 1998.[303] The Opinion explicitly states that public access to information does not mean unfettered access. When personal information is made public, either by virtue of a regulation or because the data subject himself authorises it, the data subject is not deprived of protection, ipso facto and forever.[304] He is guaranteed such protection by law in accordance with the EU Directive setting out fundamental principles of the right to privacy.

3.3.190 It was further noted that the computerisation of information and the possibility of carrying out full-text searches create an unlimited number of ways of querying and sorting information, with Internet dissemination increasing the risk of collection for improper purposes. Furthermore, computerisation has made it much easier to combine publicly available data from different sources, so that a profile of the situation or behaviour of individuals can be ascertained. Making information available to the public, futhermore, serves to fuel the techniques of data warehousing and data mining.[305]

3.3.191 In order to strike a balance between the right to privacy and the protection of personal information on the one hand and the right of the general public to access public sector information on the other, account should be taken of the following factors and issues:[306]

* a case by case assessment of whether personal information can be published or should be accessible or not and under what conditions;

---

302 Com (1998) 585 available at http://www.echo.lu/legal/en/access.html.

303 European Union Art 29 Working Party ***Opinion No 3/99 on Public Sector Information and the Protection of Personal Data*** Contribution to the consultation initiated by the European Commission in its Green Paper entitled "Public Sector Information: A Key Resource for Europe" COM (1998) 585, adopted 3 May 1999. (hereafter referred to as ***WP Opinion*** 3/99) at 4.

304 ***WP Opinion*** 3/99 at 11.

305 ***WP Opinion*** 3/99 at 6.

306 ***WP Opinion*** 3/99 at 12.

* the principles of purpose and legitimacy;[307]
* the obligation to inform the data subject;
* the data subject's right to object;
* the use of new technologies to help protect the right to privacy.

3.3.192 In 2003 the EU adopted a Directive on the re-use of public sector information.[308] It states that wider possibilities of re-using public sector information should, inter alia, allow European companies to exploit its potential and contribute to economic growth and job creation.[309] Public sector bodies should be encouraged to make available for re-use any documents held by them.[310] However, the Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC.[311]

3.3.193 It is interesting to note that the definition of "re-use" is stated as the use of persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced. Exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute re-use.[312]

3.3.194 Outside of the EU it is interesting to note the example of New Zealand where the Privacy Act[313] provides very wide exceptions to the Information Protection Principles for public records.[314] However, when the Act was enacted very few public registers were completely computerised. The Act therefore stipulated that the definition of public records do not include computerised records. By 2008 it is rare for registers to be maintained otherwise than in electronic form. The New Zealand Law Reform Commission was therefore instructed to consider

---

307 The principle of purpose requires that personal information is collected for specific, explicit and legitimate purposes and is not subsequently processed in a manner which is incompatible with these purposes. See article 6 (1)(b) of Directive 95/46/EC and discussion below in Chapter 4. See clause 11 of the Bill.

308 EU Directive 2003/98/EC dated 17 November 2003.

309 EU Directive 2003/98/EC, Recital 5.

310 EU Directive 2003/98/EC Recital 9.

311 EU Directive 2003/98/EC, Recital 21; Article 1(4).

312 EU Directive 2003/98/EC, Article 2 (4).

313 Privacy Act,1993.

314 Information Protection Principles 10 and 11.

whether the law relating to public registers requires amendment as a result of emerging technologies and their impact on access to personal information in public registers. [315]

3.3.195 In its submission on the original Issues Paper of the New Zealand Law Commission, the Privacy Commission[316] identified four matters which should be addressed by any public register reform: bulk release of register information, direct marketing, risk to safety and accountability of government for handling of information. It was noted that the release of personal information compulsorily acquired by the State for uses which are not required in the public interest and which are unwelcome to the individuals concerned must be an issue worth addressing and if possible solving.[317] The question was also posed why government should be bound where it discloses one item of information but unaccountable for disclosing 7 million off a register.[318]

3.3.196 In its final report the Law Commission has recommended that public registers should be more strictly regulated through their establishing statutes with references to the Privacy Act. In each case a dedicated review team will inter alia, determine the purpose for which the register was set up, the purpose for which people should be able to access the register, which privacy principles should apply, whether bulk access should be allowed, etc. Provision was also made for accreditation for bulk access to and use of public register information for specific registers.[319]

3.3.197 It is therefore clear that public registers should be properly regulated and that the proposals for South African public registers in the Discussion Papers are in line with international prescripts. The Commission, however, acknowledges the need for the inclusion in the Bill of a definition of "public record". "Public record" is therefore defined

---

315 NZ Law Commission ***Public Registers: Review of the Law of Privacy Stage 2*** Report 101 January 2008 (hereafter referred to as "NZ Law Commission ***Public Registers***") at 11.

316 Blair Stewart Assistant Privacy Commissioner New Zealand Privacy Commission "Submission on Law Commission Issues Paper on Public Registers" 19 November 2007 (hereafter referred to as " NZ Privacy Commission submission" at 3.

317 NZ Privacy Commission submission at 4.

318 NZ Privacy Commission submission at 6.

319 Although many of the concerns of the Privacy Commission were addressed by the recommendations of the Law Commission, the Privacy Commission wanted the reforms to be implemented through amendments to the Privacy Act and not by individual changes to the establishing statutes as was proposed by the Law Commission. See also Stewart B "Drafting Suggestions for Departments Preparing Public Register Provisions" New Zealand Privacy Commission June 2005.

as "a record that is accessible in the public domain and which is in the possession or under the control of a public body, whether or not it was created by that public body".[320]

3.3.198 The Commission furthermore confirms its recommendations as set out in the Discussion Papers which provides for a balance to be struck between the right to privacy and the commercial interests of private institutions. Data subjects have a right to be informed about the processing of information about them and they furthermore have the right to object on reasonable grounds to the processing except if national legislation provides otherwise. These rights are set out in Principles 2 and 3 of the Bill and no exceptions for public registers are provided.[321]

3.3.199 Given the profusion of information dissemination sources and the large number of operators, provision should furthermore be made for a one-stop-shop for information protection in order to make it unnecessary for data subjects to object to each operator individually. The proposed Consumer Protection Bill makes provision for a statutory exclusion list in this regard.[322]

c) Recommendation

3.3.200 The Commission's recommendation is therefore that the scope of the protection of personal information legislation should include:

a) automatic and manual files;
b) existing and future information bases;
c) sound and image information;
d) information pertaining to both natural and juristic persons;
e) information kept by both the public and the private sector;
f) special personal information (sensitive information);

---

320 See clause 1 of the Bill.

321 Other uncontroversial Principles that apply to information kept in public registers are Principles 5,6 7 and 8.

322 See discussion in Chapter 5 below.

g) professional information; and

h) information in the public domain.

3.3.201 Personal information kept in the course of a purely personal or household activity and de-identified information will be excluded. Limited exclusions have been provided for information processed for journalistic purposes as well as for critical information. In accordance with the Promotion of Access to Information Act, 2000 exclusions have also been granted for the processing of personal information by the Cabinet and committees and relating to the judicial functions of a court as referred to in section 166 of the Constitution.

3.3.202 Provision will also be made for responsible parties to approach the Commissioner for exemptions from specific information principles under specified circumstances. See Chapter 4 of the Bill below.

3.3.203 The Commission therefore recommends the legislative enactment to read as follows:

CHAPTER 2

APPLICATION PROVISIONS

Application of this Act

3. This Act applies to the processing of personal information entered in a record, using automated or non-automated means, by or for a responsible party -

(a) domiciled in the Republic of South Africa; or

(b) which is not domiciled in South Africa, using means situated in South Africa, unless those means are used only for forwarding personal information,

provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

Exclusions

4. This Act does not apply to the processing of personal information -

(a) in the course of a purely personal or household activity;

(b) that has been de-identified to the extent that it cannot be re-identified again;

(c) by or on behalf of the State and -

(i) which involves national security, defence or public safety; or

(ii) the purpose of which is the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures,

to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;

(d) for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;

(e) by the Cabinet and its committees, the Executive Council of a Province and a Municipal Council of a municipality ;

(f) relating to the judicial functions of a court referred to in section 166 of the Constitution; or

(g) that has been exempted from the application of the information protection principles in terms of section 34.

Saving

5.(1) This Act does not affect the operation of any other legislation that regulates the processing of personal information and is capable of operating concurrently with this Act.

(2) If any other legislation provides for safeguards for the protection of personal information that are more extensive than those set out in the information protection principles, the more extensive safeguards will prevail.

This Act binds the State and the private sector

6. This Act binds the State and the private sector.

3.3.204 A final point to note in so far as the scope of the inquiry is concerned is, however, that although the primary focus of this investigation is that of data or information privacy, this area is also closely linked to other privacy concerns such as bodily privacy, territorial privacy, communications privacy and surveillance. [323]

3.3.205 As was stated in the Issue Paper it is clear that information privacy overlaps with all of these other privacy concerns in so far as problems of regulating the processing of the information gained as a result of intrusions (where those intrusions have been lawful) are concerned. One would need a good understanding of all of these areas to ensure that all rights likely to be affected or covered by any information privacy legislation are acknowledged and addressed. Proposed legislation will therefore have to be closely linked to legislation already in place in those areas and may even have to address problems where an area has not been regulated yet.

---

323 The Victorian Law Reform Commission in Australia has published an Information Paper entitled "Privacy Law: Options for Reform***"*** ***Information Paper*** 2001 available at www.lawreform.vic.gov.au. In this paper they briefly explored the meaning of the right to privacy and the challenges of the new technological age and then went on to examine five key dimensions of privacy which are recognised by their existing laws in order to determine which of those areas their Commission's work should focus on. These areas are the following:

(a) bodily privacy: intrusions into a person's body, for example through DNA testing; biometric identification (hand scanning), drug tests, frisking of people, psychological testing of employees, blood tests from people suspected of carrying an infectious disease, and genetic testing (genetic privacy) by for instance insurance agencies. Intrusions are usually to obtain information about an individual.

(b) territorial privacy: intrusions into a person's physical space, for example a home or business premises, using telephones and faxes for unsolicited tele-marketing, listening devices, concealed cameras, sensors, surveillance of e-mail and Internet browsing activity.

(c) information privacy: access to information held by Government or private sector organisations, for example mailing lists, credit bureaux and information contained on public registers such as the electoral roll.

(d) communications privacy: interception of private communications, for example telephone calls and e-mails; and

(e) surveillance: use of surveillance devices, for example video cameras in public (shops, hospitals, streets) and private places.

CHAPTER 4: PRINCIPLES OF INFORMATION PROTECTION

4.1 Origins of the information protection principles

a) Introduction

4.1.1 With the use of electronic computers[1] for storing data in data banks, in particular, integrated data banks, a greater possibility of disclosure ("visibility") of an individual's private life (his so-called computer privacy) has been created than ever before.[2] People leave behind them an electronic trail which gives extraordinary levels of detail of the individual's life.[3]

4.1.2 Public concerns have risen in tandem with the proliferation of personal electronic records kept by government, corporations and employers.[4] The convergence of information and communications technology, combined with new approaches to management and industrial relations, have created increasing risks of privacy infringements.[5] These risks have been exacerbated by the adoption of the Internet over the last decade.

4.1.3 The ease of electronic communication that it has facilitated has spawned novel social and

---

1 This use of the computer has far-reaching consequences. McQuoid-Mason ***Law of Privacy*** at 195-196 refers to the following: computers facilitate the collection, maintenance and retention of extensive records, make data easily and quickly accessible from many distant points, make it possible for data to be transferred quickly from different systems, make it possible to combine data in ways otherwise not practicable, and allow data to be stored, possessed and transmitted in unintelligible form so that few people know what appears in the data records and what is happening to them (see also Du Plessis at 391).

2 See reference in ***Neethling's Law of Personality*** 268 fn 9 to Miller 1972 ***Int So Sci J*** 429 fn 1 who states as follows: "The computer with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn our society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer." However, it is noted that Van der Merwe nevertheless regards the traditional fears in this regard as exaggerated. See further Faul ***Beskerming van die Bankgeheim*** at 8 on so-called "financial privacy".

3 Tilley A "Data Protection in South Africa and the Right to Access to Information: An Inescapable Clash" Submission to the SALRC dated 26/8/2002 (hereafter referred to as "Tilley submission") at 3.

4 Piller C "Privacy in Peril" ***Macworld*** 10 n7 July 1993 124.

5 Victorian Law Reform Commission ***Information Paper*** 2001 at 5.

business practises which have necessitated even those countries who had previously established privacy and information protection legislation to reconsider and revise these laws.

4.1.4 The first privacy laws enacted in order to regulate these practices was in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978).[6]

4.1.5 The emergence of a global market led to an increase in the exchange of information across national boundaries. The flow of information across national borders became the life-blood of the emerging global economy.[7]

4.1.6 Since it was therefore recognised that privacy protection was not only a domestic problem, two crucial international instruments evolved from these laws:

- The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[8] (CoE Convention);and
- the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[9]

4.1.7 These instruments set out specific rules covering the handling of information. The rules describe personal information as data that is afforded protection at every step from collection to storage and dissemination.

4.1.8 These two agreements have had a profound effect on the enactment of laws around the world. Nearly thirty countries have signed the CoE Convention. The OECD guidelines have also been widely used in national legislation, even outside the OECD member countries.

---

6 See analysis of these laws in Flaherty DH ***Protecting Privacy in Surveillance Societies*** University of North Carolina Press 1989.

7 Roos A "Data protection: Explaining the International Backdrop and Evaluating the Current South African Position" 2007 ***SALJ*** Vol124 400 (hereafter referred to as "Roos ***SALJ***")at 403.

8 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 1981.

9 OECD Guidelines.

4.1.9 The policy responses that developed were for the most part driven by a shared understanding about the nature of the information privacy problem they were facing. Hence a set of 'fair information principles" evolved.[10]

4.1.10 All the international data protection documents furthermore have two primary goals, namely the setting of standards at the national level for the protection of personal data, and the reconciliation of this goal with the ideal of allowing the free flow of information across national boundaries.[11]

b) Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention)

4.1.11 The Convention is so far the sole international treaty to deal specifically with data protection. It entered into force on 1 October 1985.[12] The Convention is potentially open for ratification by States that are not members of the CoE;[13] concomitantly it is also envisaged to be potentially more than an agreement between European states. As yet, though, it has not been ratified by any non-member states. [14]

4.1.12 The Convention is not intended to be self-executing. Article 4(10) of the Convention simply

---

10 Bennett Foundation Paper at 10; Roos ***SALJ*** at 405: Despite differences in language, legal tradition and cultural and social values, there has been a broad measure of agreement on the basic content and core rules that should be embodied in data protection legislature.

11 Roos ***SALJ*** at 404.

12 As of 23 May 2002, it had been ratified by 27 CoE Member states.

13 Article 23.

14 Bygrave ***Data Protection*** at 32; Privacy Law and Business (PL&B) International E-news Issue 71 August 1, 2008 reports that the Council of Europe Convention on Data Protection, for the first time since it was opened for signature in 1981, is inviting non-European countries with data protection laws to sign and ratify it. The Convention's Consultative Committee recommended "that non-member states, with data protection legislation in accordance with Convention 108, should be allowed to accede to the Convention", and it "invited the Committee of Ministers to take note of this recommendation and to consider any subsequent accession request accordingly". The Committee of Ministers, on 2 July 2008, "agreed to examine any accession request in the light of this recommendation" and "instructed the Secretariat to disseminate information about the Convention".

obliges contracting States to incorporate the Convention's principles into their domestic legislation; individual rights cannot be derived from it.[15]

4.1.13 The Basic Principles for Data Protection as set out in Chapter II of the Convention deals with:

a) duties of the parties;[16]

b) quality of the data;[17]

c) special categories of data;[18]

d) data security;[19]

e) safeguards for the data subject;[20]

---

15 Bygrave ***Data Protection*** at 34.

16 Article 4
Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter. 2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

17 Article 5
Quality of data

Personal data undergoing automatic processing shall be: a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are stored; d. accurate and, where necessary, kept up to date e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

18 Article 6
Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

19 Article 7
Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

20 Article 8
Additional safeguards for the data subject

Any person shall be enabled: a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention; d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

f) sanctions and remedies;[21] and

g) extended protection.[22]

4.1.14 An additional Protocol to the Convention was adopted on 23 May 2001[23] by the CoE Committee of Ministers. It makes specific provision for the institution of regulating agencies and sets provisions for crossborder transfers (bringing the Convention in line with the EU Directive).

c) Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)

4.1.15 In late 1980, the Organisation for Economic Cooperation and Development (OECD) issued a set of Guidelines concerning the privacy of personal records. Although broad, the OECD guidelines set up important standards for future governmental privacy rules. These guidelines underpin most current international agreements, national laws, and self-regulatory policies. Although the guidelines were voluntary, roughly half of OECD member-nations had already passed or proposed privacy-protecting legislation by 1980. By 1983, 182 American companies claimed to have adopted the guidelines, although very few ever implemented practices that directly matched the standards.

4.1.16 The OECD Guidelines have been highly influential on the enactment and content of information protection legislation in non-European jurisdictions, particularly Japan, Australia, New Zealand and Hong Kong. In North America the Guidelines have been formally endorsed by

---

21 Article 10
Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

22 Article 11
Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects of wider measure of protection than that stipulated in this convention.

23 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) regarding the supervisory authorities and trans border data flows, ETS No 179, open for signature 8.11.2001.

numerous companies and trade associations. They have additionally constituted the basis for the first comprehensive set of information protection standards to be developed by a national standards association: the Model Code for the Protection of Personal Information, adopted by the Canadian Standards Association (CSA) in March 1996.[24]

4.1.17 The OECD Guidelines incorporate eight principles relating to the collection, purpose, use, quality, security and accountability of organisations in relation to personal information. However, the OECD Guidelines do not set out requirements as to how these principles are to be enforced by member nations. As a result, OECD member countries have chosen a range of differing measures to implement the information privacy principles.[25]

4.1.18 Although the CoE and the OECD instruments cover the same basic areas of activity, they represent differing philosophies as to the nature of the problem and as to the appropriate legal response. In particular, whilst the European model sees the establishment of a specialised supervisory agency as critical, the OECD Guidelines have been strongly influenced by the United States which has tended to rely upon the courts as the primary mechanism of enforcement of legal rights.[26]

4.1.19 The OECD Guidelines are set out in the following principles:

- Collection Limitation Principle [27]
- Data Quality Principle[28]

---

24 Bygrave ***Data Protection*** at 33 and references therein.

25 Victorian Law Reform Commission ***Information Paper*** 2001 at 23.

26 As referred to in Strathclyde LLM "Notes for Information Security Theme Two: Data protection" at 4. See para 9.2.14 in Chapter 9 below for the developments in the APEC countries.

27 There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

28 Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- Purpose Specification Principle [29]
- Use Limitation Principle[30]
- Security Safeguards Principle [31]
- Openness Principle[32]
- Individual Participation Principle[33]
- Accountability Principle[34]

---

29 The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

30 Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or
b) by the authority of law.

31 Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

32 There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

33 An individual should have the right:
a) to obtain from a data controller, or otherwise,confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

34 A data controller should be accountable for complying with measures which give effect to the principles stated above. The United States endorsed the OECD Guidelines.

d) Other OECD Guidelines

- **OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999):**

4.1.20 The Guidelines provide that business-to-consumer electronic commerce should be conducted in accordance with the recognised privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980), and taking into account the OECD Ministerial Declaration on the protection of privacy on Global Networks (1998), to provide appropriate and effective protection for consumers.

- **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (OECD Security Guidelines)**

4.1.21 The OECD Security Guidelines were adopted on 25 July 2002 and replaced the existing guidelines due to the dramatic change in the information technology environment during the nineties. The Security Guidelines contain nine information systems security principles. See discussion under Principle 7 below.

e) European Union Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (EU Directive)[35]

4.1.22 In 1995 the European Union enacted the EU Directive in order to harmonise member states' laws in providing consistent levels of protections for citizens, on the one hand, and ensuring the free flow of personal data within the European Union, on the other. Formally adopted on 24 October 1995, the Directive arose from the sense that European citizens were losing control over

35 A copy of the EU Directive is included in this report as Annexure D.

their personal information and that they had a fundamental right to privacy.[36] The Commission of the EC had also become concerned at the effect which discrepancies in the member states' laws and regulations might have on inter-community trade. [37]

4.1.23 The Directive proved controversial throughout its passage through the EU's law-making process, so much so that five years elapsed between publication of the first proposal and adoption of the final text.[38] Criticism came from both ends of the data protection spectrum.[39]

4.1.24 The EU Directive was adopted with member states being required to implement its provisions by October 24, 1998. [40] Member states are therefore compelled to adopt legislation that conforms to the standards set in the Directive. This time-table has proven difficult for member states to adhere to.

4.1.25 The directive sets a baseline common level of data privacy protection that not only reinforces current data protection law, but also establishes a range of new rights. It applies to the processing of personal information in electronic and manual files.[41] The Directive provides only a basic framework which will require to be developed in national laws.[42]

4.1.26 The principles of the protection of the rights and freedoms of individuals which are

---

36 The EU Directive entered into force from the date of publication in the official journal. After that time member states had fifteen months to implement its provisions.

37 Roos ***SALJ*** at 406.

38 As referred to in Strathclyde LLM at 5.

39 The UK objected to the measure as extending the scope and cost of legislation and ultimately abstained from the final vote in the Council of Ministers. Germany was concerned that the protection afforded its citizens by its national Act, may be weakened. The Unites States thought the transborder data flows were being driven by considerations of economic protectionism and constituting a thinly veiled attack on the US data processing industry.

40 Article 32 of the EU Directive.

41 Article 3 of the EU Directive.

42 As referred to in Strathclyde LLM at 4. A good example is the Directive's requirement that member states shall appoint an independent supervisory agency. The particular form of the agency is not specified.

contained in the Directive, notably the right to privacy, give substance to and amplify those contained in the CoE Convention.[43]

4.1.27 A key concept in the European data protection model is "enforceability." Data subjects have rights established in explicit rules. Every European Union country has a data protection commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will need to provide a similar level of oversight.

4.1.28 The EU Directive furthermore contains strengthened protections over the use of sensitive personal data relating, for example, to health, sex life or religious or philosophical beliefs. In future, the commercial and government use of such information will generally require "explicit and unambiguous" consent of the data subject.

4.1.29 The scope of the rights and obligations under the Directive may be restricted when such a restriction constitutes a necessary measure to protect the data subject, or the interests of others, or to safeguard certain public interests.[44]

4.1.30 The Directive encourages the drawing up of sector specific codes of conduct with a view to contributing to the proper implementation of the privacy principles.[45]

4.1.31 The basic principles established by the EU Directive are as follows:[46]

- The EU Directive regulates the processing of personal data of data subjects by or

---

43 Recital 11 of the EU Directive.

44 Roos ***SALJ*** at 411.The public interests that justify these exemptions are (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);(g) the protection of the data subject or of the rights and freedoms of others.

45 Roos ***SALJ*** at 411.

46 Fisher R Excerpt from ***Privacy of Personal Information and the National Information Infrastructure.*** See especially paras (a) -(e) of Article 6 of the EU Directive.

on behalf of a data controller . A data controller determines the purposes for which and the means by which the data is processed, and can be a natural or juristic person, a public authority, agency or any other body.[47]

- The EU Directive establishes an obligation to collect data only for specified, explicit and legitimate purposes and to maintain that information only if it is relevant, accurate and up-to-date.
- The EU Directive establishes a principle of fairness regarding the collection of data under which each individual is given the option of whether to provide the information requested or not, through a type of notice and opt-out procedure.
- Individuals must also be provided with an opportunity to learn the identity of organisations intending to process data about them and the main purpose for which that information is being collected or will be used.
- The Data Protection Directive also requires all data processing to have a proper legal basis and identifies the following legal grounds for the collection and use of data:
    - consent;
    - contract;
    - legal obligations;
    - vital interests of the data subject; and
    - the balance between the legitimate interest of the people collecting or using the data and the people to whom the data relates.[48]
- The Data Protection Directive also provides data subjects with a number of important rights, including:
    - the right of access to data;
    - the right to know where the data originated;
    - the right to have inaccurate data rectified;

---

47 Roos ***SALJ*** at 407.

48 See eg the discussion in Chapter 3 above on the balancing of the right to freedom of expression with the right to privacy insofar as the processing of personal information for journalistic purposes is concerned.

- the right of recourse in the event of unlawful processing of data;[49] and
- the right to withhold permission to use their data in certain circumstances.[50]

- Where data is transferred from a European Union country to a non-European Union country, the Data Protection Directive establishes a basic rule that the non-EU country receiving the data must provide an "adequate level" of data protection.[51]

4.1.32 This requirement has resulted in growing pressure outside Europe for the passage of information privacy laws. Those countries that refuse to adopt adequate data privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data. [52]

4.1.33 Another possible way to protect the privacy of information transferred to countries that do not provide "adequate protection" is to rely on a private contract containing standard information protection clauses. This kind of contract would bind the responsible party and data processor to respect fair information practices such as the right to notice, consent, access and legal remedies. In the case of information transferred from the European Union, the contract would have to meet the standard "adequacy" test in order to satisfy the Data Protection Directive.[53]

4.1.34 The provisions of the EU Directive will be discussed in detail, where appropriate, in the rest

---

49 Article 22 of the EU Directive requires that data subjects should have a judicial remedy, apart from an administrative remedy, for any breach of their rights.

50 Article 14 (a) of the EU Directive provides data subjects with the right to object to the processing of their personal information in specific circumstances on compelling legitimate grounds.

51 Article 25 of the EU Directive.

52 See the discussion on crossborder transfers in Chapter 6.

53 EPIC and Privacy International ***Privacy and Human Rights Report* 2002** at 16. A number of model clauses that could be included in such a contract were outlined in a 1992 joint study by the Council of Europe, the European Commission and the International Chamber of Commerce. In a June 2000 report (see below), the European Parliament accused the European Commission of a "serious omission" in failing to draft standard contractual clauses that European citizens could invoke in the courts of third countries before the Data Directive came into force. It recommended that they do so before September 30, 2000. In July 2001, the Commission issued a final decision approving the standard contractual clauses.

of the report.

f) Other relevant EU Directives

*** EU Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (ISDN Directive)**

4.1.35 In 1997 the European Union supplemented the 1995 directive by introducing the Telecommunications Privacy Directive.[54] This directive established specific protections covering telephone, digital television, mobile networks and other telecommunications systems.[55] It was repealed and replaced by EU Directive 2002/58/EC. See discussion of this Directive below.

*** EU Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services**

4.1.36 Recital 5 provides that the convergence of the telecommunications, media and information technology sectors means all transmission networks and services should be covered by a single regulatory framework. That regulatory framework consists of this Directive and four specific Directives (2002/20/EC, 2002/19/EC, 2002/22/EC and 2002/58/EC.)

4.1.37 The importance of this Directive for our discussion is the fact that the definitions set out in this Directive - together with those in Directive 95/46/EC - are applied everywhere else. See for instance in this regard the definition of “communication” and “electronic mail”.

---

54 EU Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (ISDN Directive). Replaced by 2002/58/EC dated 12 July 2002 which in turn was amended by Directive 2006/24/EC.

55 European Union member countries were required to enact implementing legislation by October 1998.

* **EU Directive 2000/31/EC on electronic commerce**

4.1.38 Provision was also made for opt-out registers in Directive 2000/31/EC :

a) Service providers undertaking unsolicited commercial communications are obligated to consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

b) This provision was made applicable to legal persons as well by Directive 2002/58/EC.

4.1.39 Between May and October 2000, a comprehensive survey of European industry federations was undertaken in order to identify all the private sector initiatives which had been or were being undertaken in member states. It was found that opt-out lists were being set up in the UK, Germany, the Netherlands, Spain, Norway, Sweden, Finland and Italy. The UK's direct marketing association has joined with the American DMA to build a joint register. [56]

* **EU Directive 2002/58/EC on privacy protection in the electronic communications sector[57]**

4.1.40 The purpose of this Directive is to reflect continuing technological developments in telecommunications and other electronic services and to provide an equal level of privacy protection to personal information regardless of the technologies used to provide the services. It repeals and

---

56 Commission of the European Communities (authors Serge Gauthronet and Etienne Drouard) **Unsolicited Commercial Communications and Data Protection** Internal Market DG -Contract no ETD/99/B5-3000/E/96 January 2001 (hereafter referred to as "***Unsolicited Commercial Communications and Data Protection***") at 21.

57 On 21 February 2006 the Council adopted Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or network services and amending Directive 2002/58/EC.

replaces Directive 97/66/EC of 15 December 1997. It translates the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector.

4.1.41 Specific provision has been made for public directories and unsolicited electronic communications for direct marketing. See the discussion in this regard in Chapter 5 below.

g) United Nations Guidelines

4.1.42 The United Nations' (UN) Guidelines Concerning Computerised Personal Data Files (hereinafter termed UN Guidelines) were adopted by the UN General Assembly on 14 December 1990.[58] The Guidelines are intended to encourage those UN Member States without information protection legislation in place to take steps to enact such legislation based on the Guidelines. The Guidelines are also aimed at encouraging governmental and non-governmental international organisations to process personal data in a responsible, fair and privacy-friendly manner. The Guidelines are not legally binding and seem to have had much less influence on information regimes than the other instruments.[59]

h) Commonwealth Guidelines

4.1.43 At their meeting in 1999 in Trinidad and Tobago the Commonwealth Law Ministers endorsed the Commonwealth Freedom of Information Principles. Believing that the obverse side of the freedom of information coin is the protection of personal privacy, the Secretariat proposed for consideration by Senior Officials at their meeting in November 2002 that model legislation to implement the Commonwealth commitment to freedom of information should be a model Bill on privacy.

4 .1.44 The intent of the proposed model legislation is to ensure that governments accord personal

58 Doc E/CN.4/1990/72, 20.2.1990.

59 Bygrave ***Data Protection*** at 33.

information an appropriate measure of protection, and also that such information is collected only for appropriate purposes and by appropriate means. The model deals only with information privacy. Other aspects of privacy such as privacy of communications, bodily privacy and territorial privacy were not dealt with in the model Bill.

4.1.45 The draft model Privacy Bill prepared for consideration of Senior Officials sought to give effect to the OECD principles set out above. It also sought to create a legal regime which could be administered by small and developing countries without the need to create significant new structures.

4.1.46 Concern was also expressed regarding the possible economic implications of the 1995 European Union (EU) Directive on the protection of privacy in member countries, and the need to develop national legislation to address the issue.

4.1.47 Two draft model privacy Bills were considered, one for the private sector and one for the public sector. They are modelled largely on the Canadian legislation, although account was also taken of the United Kingdom legislation (which is based on the EU Directive and therefore places emphasis on different elements of protection) and the OECD Guidelines.

4.1.48 The model Bills give effect to some core principles of this type of protection: setting limits to the collection of personal information or data; restrictions on the usage of personal information or data to conform with openly specified purposes; giving an individual the right to access personal information relating to that individual and the right to have it corrected, if necessary; and the identification of the parties who are responsible for compliance with the relevant privacy protection principles.

4.1.49 In evaluating the proposed Model Laws the Law Ministers' meeting commended the proposed Model Law for the public sector as a useful tool which should be adopted to meet the particular constitutional and legal positions in member countries. They decided, however, that the Model Bill on the Protection of Personal Information for the private sector needed more reflection.

They asked the Commonwealth Secretariat to prepare an amended draft to be considered at the next planning meeting of Secretariat officials.

i) Asia Pacific Economic Cooperation (APEC) framework

4.1.50 APEC is the premier forum for facilitating economic growth, cooperation, trade and investment in the Asia Pacific region.[60]

4.1.51 Thirteen APEC members agreed to develop a framework for accountable flows of personal data across the region, focussing on the use of Cross Border Privacy Rules (CBPR) by business. The aim of a fully operational system is to protect the personal information of an individual no matter where in the region that personal information is transferred or accessed.

4.1.52 This will promote consumer trust and business confidence in cross border data flows. It will support business needs, reduce compliance costs, provide customers with effective remedies, allow regulators to operate efficiently, and minimise regulatory burdens.

4.1.53 A Data Privacy Pathfinder initiative[61] was subsequently developed[62] and adopted in September 2007 to enable member countries to work together on the implementation of the APEC Privacy Framework. This approach recognises that economies are at differing levels of

---

60 List of participating economies: Australia, Canada, Chile, Hong Kong China, Japan, Republic of Korea, Mexico, New Zealand, Peru, Chinese Taipei, Thailand, United States, Viet Nam.

61 The Data Privacy Pathfinder's main objectives are -
* Promoting a conceptual framework of principles of how cross-border rules should work across economies, in consultation with the various stakeholders;
* Promoting the development of consultative processes on how best to include stakeholders;
* Promoting the development of practical documents and procedures that under-pin cross-border privacy rules;
* Exploring ways in which various documents and procedures may be implemented in practice; and
* Promoting education and outreach.

62 Asia-Pacific Economic Cooperation "APEC Data Privacy Pathfinder: Proposed Work Plan" Electronic Communications Steering Group (ECSG) Meeting Cairns Australia 29June 2007.

development and implementation of privacy frameworks within their economies. [63]

4.2 Discussion of Information Protection Principles

A) Introduction

4.2.1 It is common for privacy or information protection Acts worldwide to contain sets of principles. Many jurisdictions regulate privacy by using broad principles, rather than the more conventional method of rules-based regulation. The information protection principles lie at the heart of any Information Privacy Act. It has been found to be an appropriate means of translating the concepts of information privacy into a legally effective form.[64]

4.2.2 Only those legal instruments embracing all or most of the principles set out below are commonly considered to be information protection laws. The principles can however be found in all types of policy and legal instruments.[65]

4.2.3 Professor Julia Black[66] has provided a very useful discussion on the nature of principles-based regulation. She distinguishes between three broad categories of regulatory method: bright

---

63 Reference will be made to specific APEC proposals where applicable in the discussions to follow.

64 Office of the Privacy Commissioner, New Zealand ***Privacy Act Review 1998*** Discussion Paper No 2: Information Privacy Principles (hereafter referred to as "New Zealand Discussion Paper") at 1.

65 Bygrave ***Data Protection*** at 3.

66 Black J "Principles Based Regulation: Risks, Challenges and Opportunities" 2007 London School of Economics and Political Science as referred to by the Law Reform Commission of Australia in the ***ALRC Discussion Paper*** at 549 and further.

line rules;[67] principles[68] and complex or detailed rules.[69]

4.2.4 Principle-based regulation is described as expressing the fundamental obligations that should be observed by everyone. Therefore, principle-based regulation seeks to provide an overarching framework that guides and assists regulated entities to develop an appreciation of the core goals of the regulatory scheme. The regulatory focus is shifted from process to outcomes.[70] It emphasises a "do the right thing" approach and promotes compliance with the spirit of the law.[71] It, furthermore, provides flexibility through the statement of general principles that can be applied to new and changing circumstances.[72]

4.2.5 Principles-based regulation also makes use of qualitative and often evaluative terms such as "fair", "reasonable" and "suitable". This approach facilitates compliance as it is possible to develop policies that comply with the law while also meeting the responsible party's needs. In contrast, rules-based regulation is not always appropriate for all entities regulated.

4.2.6 The disadvantages of a principles-based system centre on problems of ambiguity. It has been argued that it may create an unpredictable regulatory regime which can undermine the system's intended protections and accountability. [73]

---

67 Rules containing a single criterion of applicability. Such rules are clear and straightforward to apply but can fail to achieve their goal because there is considerable scope for manipulation. It may be possible to comply with the letter, but not the spirit of the law.

68 A "principle" articulates substantive objectives. See further discussion in para 4.2.5.and further below. Problems may arise in practice as reasonable minds may differ over what is necessary, in a particular context, for an organisation's functions or activities.

69 Complex rules expressly list the relevant conditions to be taken into account. A list of rules will, however, inevitably leave gaps resulting in scope for manipulation.

70 Ibid at 3.

71 Arjoon S "Striking a Balance Between Rules and Principled-Based Approaches for Effective Governance: A Risk-Based Approach (2006) 68 Journal of Business Ethics 53, 69 as referred to by the Australian Law Reform Commission in the ***ALRC Discussion Paper*** at 550.

72 ***ALRC Discussion Paper*** at 551: This purposive approach expresses both the rationale for the rule and provides overarching requirements that can be applied flexibly to a rapidly changing industry. This is especially important in the information industry where technology is consistently changing.

73 ***ALRC Discussion Paper*** at 552 referring to Black at 2.

4.2.7 Although rules-based and principles-based regulation are very different in their approach, the two systems can also operate as a hybrid system, providing regulated entities with the benefits of both systems.[74] This is also, in principle, the position in respect of the regulatory system set out in the Commission's Discussion Papers. See the discussion below.

4.2.8 Except to the extent that any data controller/ responsible party is able to claim an exemption from any of the principles (whether on a transitional or outright basis) the principles apply to all personal information processed by responsible parties.

4.2.9 The formulation of a code of fair information practices is usually derived from several sources, including codes developed by the OECD(1980), the Council of Europe(1981) and EU (1995) as discussed in para 4.1 above. In this discussion paper the principles will also be compared with other modern sets of privacy principles recently developed in other jurisdictions.

4.2.10 One should remember that these codes are guidelines only which ought to be interpreted by countries to suit their own position. Article 5 of the Directive states for example that:

> Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

4.2.11 For example, in the UK the data principles were originally derived from the CoE Convention which in turn were given substance and amplification by recital 11 of the EU Directive. In New Zealand the information privacy principles follows, but do not directly repeat, the OECD principles, are designed to suit New Zealand law and circumstances and are somewhat more precise. They owe much to the principles in the Australian Privacy Act 1988 although there are significant differences.[75] In Canada the federal Privacy Act of 1982, which applies to the public sector, is based on the OECD Guidelines whereas the Personal Information Protection and Electronic Documents Act (PIPEDA) adopted the CSA International Privacy Code (a national standard developed in conjunction with the private sector - also based on the OECD principles) into law for

---

74 ***ALRC Discussion Paper*** at 553.

75 New Zealand Discussion Paper at 1.

the private sector.[76]

4.2.12 The introduction to Para 7 of the OECD Guidelines emphasises an important point, namely that all the principles set out in the guidelines are interrelated and partly overlapping. Thus, the distinctions between the different activities and stages involved in the processing of information which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole.

B) Principles of Information Protection

4.2.13 What follows is a discussion of the different information principles (sometimes called "good information handling") which information agencies are required to comply with. As stated above, the categories are not always hard and fast, considerable overlap exists between them. Further, each of them is in reality a constellation of multiple principles. Some principles have been incorporated in certain information protection laws as fully fledged legal rules. In other instances the principles function as guiding standards during interest-balancing processes carried out by, for instance, information protection authorities in the exercise of their discretionary powers. The principles may also help to shape the drafting of new information protection laws,[77] and have accordingly been implemented to find the principles to be embodied in a South African Act.

4.2.14 The information protection principles that will be discussed are the following:

- Principle 1: Accountability
- Principle 2: Processing Limitation (fair and lawful processing)
- Principle 3: Purpose Specification
- Principle 4: Further Processing Limitation

---

76 See discussion in Chapter 9 below.

77 Bygrave ***Data Protection*** at 57.

- Principle 5: Information Quality
- Principle 6: Openness
- Principle 7: Security Safeguards
- Principle 8: Data subject participation

It is to be noted that additional principles are set out for sensitive information. See discussion below.

4.2.15 Respondents to the discussion papers were in general supportive of the incorporation of these principles in legislation [78] and indicated that the principles should apply to all personal information kept by a responsible party, who should be obliged to comply with them.[79]

4.2.16 Over and above the importance of protecting the constitutional right to privacy, another reason stated for introducing these principles in legislation was that various commercial opportunities exist for information outsourcing, both domestically and internationally, and that if South Africa's national standards do not conform to international requirements, specifically the EU's directive, this will inhibit full exploitation of those commercial opportunities. [80]

4.2.17 It was, however, emphasised that the real test will lie in the implementation of the principles and that the degree to which these principles are adopted will depend on the cost and feasibility of implementing them.[81] Concern was raised that the application of these principles may have an adverse impact on the cost of information technology, which can be ill afforded in South Africa.[82]

---

78 Eg. Vodacom (Pty) Ltd; The Banking Council; Gerhard Loedoff Eskom; ENF for Nedbank Ltd; ISPA.

79 The Credit Bureau Association indicated that these principles when given effect to within the credit information system, would place certain obligations upon the credit granting industry (subscribers of the bureaux) and the credit bureau industry. See discussion in Chapter 5 below.

80 The Internet Service Providers Association.

81 LOA; Liberty.

82 LOA.

4.2.18 Careful definition will be required to ensure that a balance is maintained between individual rights and the public good, and that the cost and effort to meet the defined requirements are not so onerous as to be unreasonable in relation to the potential risks to individuals of the information collection.[83]

4.2.19 It should, furthermore, be possible to exempt certain organisations from specific principles. It has, for instance, been argued that some of these principles, such as principle 8: data subject participation and principle 6: openness, should not apply to law enforcement agencies. Criminal suspects cannot be informed by the police that specific information about them is being kept in a police information base or be allowed access and correction of personal information that is being gathered about them by the State.[84]

4.2.20 One point of criticism was that the obligation in terms of the principles are too vague. Vagueness may lead to questions of interpretation and ambiguity, it would be preferable to be more specific in relation to prohibitions and legal obligations in order o prevent confusion in the application and enforcement of the principles.[85]

4.2.21 The Commission evaluated the above comments and decided to confirm its original proposal that a framework for information protection has to be set out in legislation, based on internationally accepted principles of information protection.[86]

4.2.22 The flexible principle-based approach will make it possible to regulate the processing of information in all the widely divergent sectors where personal information needs protection. It will, furthermore, make the Bill resilient to the rapid and consistent technological developments taking place in the information field.

---

83 Medical Research Council.

84 SAPS; See Chapter 3 above dealing with the scope of the legislation and specifically “critical data”.

85 NSO Telecommunications (Pty) Ltd.

86 LOA.

4.2.23 These high-level principles, which promote a best-practice approach, have, however, been complemented with a number of detailed rules in the Bill itself, and also by making provision for codes of conduct and official guidelines for specific industries, issued by the Information Regulator. The possible lack of clarity and certainty of the broad-based principles have therefore been tempered by this hybrid approach.

4.2.24 The Information Protection Principles set out in the draft Bill have furthermore been developed over a period of four years in consultation with stakeholders, including business and consumer groups. The principles are generally held to be an acceptable compromise between the protection of personal information on the one hand and on the other hand, the use of personal information for private sector business purposes and to give effect to the responsibilities of the public sector to promote the public interest. technological developments taking place in the information field.

a) Principle 1: Accountability

i) Proposals in Discussion Paper

4.2.26 Principle 8 of the OECD Guidelines reads as follows:[87]

> Accountability Principle
>
> A data controller should be accountable for complying with measures which give effect to the principles stated above.

4.2.27 Article 6 (2) of the EU Directive states:

> It shall be for the controller to ensure that paragraph 1 is complied with.

87 CDT's Guide; See discussion in Roos thesis at 519.

4.2.28 Principle 9 of the APEC Privacy Framework[88] states:

> A personal information controller should be accountable for complying with measures that give effect to the Principles. When personal information is to be transferred to another person or organisation, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organisation will protect the information consistently with these Principles.

4.2.29 The UK Data Protection Act is an example of national legislation in this regard.[89] Section 4(4) provides as follows:

> (4) Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.

4.2.30 In the Discussion Paper Bill accountability was set out as Principle 8 and reads as follows:

> **PRINCIPLE 8**
>
> **Accountability**
>
> **Responsible party to give effect to principles**
>
> 23. The responsible party must ensure that the measures that give effect to the Principles set out in this Chapter are complied with.

4.2.31 The term “responsible party” is defined in the Discussion Paper Bill as follows:

> “responsible party” means 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.

(ii) Evaluation

---

88 Asia-Pacific Economic Cooperation (APEC) ***Privacy Framework*** (2005).

89 See also Part I of the Federal Data Protection Act 1990 (Germany) which directly implements the Accountability Principle in the OECD Guidelines and article 15 of the Wet Bescherming Persoonsgegevens of the Netherlands.

4.2.32 Respondents to the Discussion papers were in favour of this principle.[90] It was furthermore proposed that legislation should provide guidelines and that self-regulation, in the form of individual codes of conduct, may address specific detail should it be required.

4.2.33 It was explained that in a complex environment, eg. the insurance industry, where persons operate phones in call centres when communicating with clients, while other insurer employees deal with clients via email or by post, complex management, control and information systems are necessary. This means that the accountability can shift between computer hardware, software and network employees, their supervisors, their managers, and so on. It is for this reason that legal accountability should lie with the head of a body, or with a "chief information officer".

4.2.34 However, according to the OECD Guidelines Explanatory Memorandum,[91] since the data processing activities are carried out for the benefit of the responsible parties (data controllers) the controllers should be accountable under domestic law for complying with privacy protection rules and should not be relieved of this accountability merely because data processors are carrying out the data processing activities on their behalf.[92]

4.2.35 Some commentators[93] were of the opinion that the provisions of this clause were too vague and need clarification. However, others[94] felt the draft Bill sets out the responsibilities of a data controller adequately.

4.2.36 For a discussion of remedies, liabilities and sanctions see Chapter 6 below.[95]

---

90 The Banking Council. The OECD guidelines are subscribed to by the Banking Council in this respect; LOA; Credit Bureau Association.

91 OECD Guidelines Explanatory Memorandum at 32.

92 Roos thesis at 519.

93 Department of Communication.

94 Law Society of South Africa.

95 It has been submitted that data subjects must be entitled to a judicial remedy, in addition to any administrative remedy, for compensation for damage suffered and that the law must lay down sanctions to be imposed in the event of any infringement of the provisions. See Roos thesis at 522.

(iii) Recommendation

4.2.37 Principle 8 in the Discussion Paper Bill has been included in the new proposed Bill as Principle 1. It is therefore clear, at the outset, that the responsible party is responsible for compliance, not only of all the other Principles set out in the Bill, but also of all the measures, described in the rest of the Bill, that give effect to the Principles. The Commission therefore recommends that the legislative enactment of Principle 1 should read as follows:

PRINCIPLE 1

Accountability

Responsible party to give effect to principles

7. The responsible party must ensure that the Principles set out in this Chapter, and all the measures that give effect to the Principles, are complied with.

b) Principle 2: Processing Limitation (Fair[96] and lawful processing)

(i) Proposals in the Discussion Paper

Fair and lawful[97]

4.2.38 It is sometimes argued that the primary principle of information protection laws is that the personal information must be processed fairly and lawfully.[98] This principle is primary because it embraces and generates the other core principles of information protection laws presented below.

---

96 See, however, Roos thesis at 483 who notes that it is sufficient, in the South African context, to require that processing should be done lawfully, since fairness is part and parcel of the concept of lawfulness. See also the discussion in Chapter 2 above in this regard.

97 **The Commission's proposal for Principle 1 in the Discussion Paper Bill (now Principle 2) reads as follows:**

PRINCIPLE 1
Processing limitation

Lawfulness of processing

7. Personal information must be processed -
(a) in accordance with the law; and
(b) in a proper and careful manner in order not to intrude upon the privacy of the data subject to an unreasonable extent.

98 See Bygrave ***Data Protection*** at 58 and the references made there-in; Roos thesis at 481.

Art 5(a) of the CoE Convention states:
Personal data undergoing automatic processing shall be:
a) obtained and processed fairly and lawfully;...

Article 6 (1)(a) of the EU Directive stipulates that Member States shall provide that personal data must be processed fairly and lawfully.

Principle 1 in the UK's Data Protection Act of 1998 provides:
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive data, at least one of the conditions in Schedule 3 is also met.
Schedule 2 is based on Art 7 of the EU Directive and follows the Directive fairly closely. The conditions deal with the consent to processing as well as other lawful reasons why the data controller needs to process data of the subject. Schedule 3 derives from Art 8 of the EU Directive which allows the processing of sensitive data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs etc, only in specific cases. See also OECD par 7; CoE art 5; New Zealand (NZ) Principle 4; The Netherlands(NL) art 76; Roos thesis ftnt 51 at 482 and 483.

The twin criteria of fairness and lawfulness are manifest in all these principles even if, in some instruments, they are expressly linked only to the means of collection of personal information[99] or not specifically mentioned at all.[100]

4.2.39 The notion of "lawfulness" is relatively self-explanatory. The bulk of information protection instruments comprehend legitimacy prima facie in terms of procedural norms hinging on a criterion of lawfulness (eg that the purposes for which personal information are processed should be compatible with the ordinary, lawful ambit of the particular responsible party's activities).[101] The determination what is fair may be a more difficult task.[102]

4.2.40 At a general level the notion of fairness[103] undoubtedly means that, in striving to achieve their information-processing goals, responsible parties must take account of the interests and reasonable expectations of data subjects. The notion of fairness therefore brings with it requirements of balance and proportionality.[104]

4.2.41 Fairness/reasonableness implies that the processing of information be transparent to the data subject.[105] It militates against secretive collection and processing and also against deception of the data subject as to the nature of, and purposes for, the information processing. See Principle

---

99 The Collection limitation principle in the OECD Guidelines (Principle 1) states as follows:
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

100 Bygrave ***Data Protection*** at 58 and the reference therein to the Norwegian PDA.

101 Section 4 of Canada's federal Privacy Act 1982; IPP1(a) of Australia's federal Privacy Act 1988; Data Protection Principle 1 of the UK Data Protection Act, 1998.

102 Strathclyde LLM at 16.

103 "Fairness" may be regarded as the American equivalent of the South African term "reasonableness". See discussion in Ch 2 on the criterion of reasonableness or boni mores.

104 Bygrave ***Data Protection*** at 58.

105 Bainbridge D ***Data Protection*** CLT Professional Publishing Welwyn Garden City 2000 (hereafter referred to as "Bainbridge ***Data Protection***") at 59.

6 below. Another requirement that may flow from this argument is that information should be collected from the data subject, not from third parties. [106] This requirement is expressly laid down in some, but not the majority of information protection instruments.[107]

4.2.42 Since fairness implies that responsible parties must take some account of the reasonable expectations of data subjects, this has direct consequences for the purposes for which information may be processed.[108] It helps to ground rules embracing the purpose specification principle. It sets limits on the secondary purposes to which personal information may be put. When personal information obtained for one purpose are subsequently used for another purpose, which the data subject would not reasonably anticipate, the responsible party may have to obtain the data subject's consent to the new use.[109] Where a person was deceived or misled as to the purposes of the processing the processing will be unreasonable. The subject should also be informed as to the non-obvious uses to which the controller intends to put the information.[110] See Principle 4 below.

4.2.43 Even though a responsible party may be able to show that information was obtained and personal information processed fairly and lawfully in general and on most occasions, if it has been obtained unfairly in relation to one individual there will have been a contravention of this processing

---

106 Principle 2 and 4 of New Zealand Privacy Act. See below.

107 Bygrave ***Data Protection*** at 59 and the references made therein.

108 Commonwealth Secretariat ***Draft Model Law on the Protection of Personal Information*** LMM(02)08 October 2002 (hereafter referred to as " Commonwealth Bill for private users"). Section 7 reads as follows:

Appropriate purpose

7. An organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

109 Bygrave ***Data Protection*** at 59.

110 Bainbridge ***Data Protection*** at 58; Commonwealth Secretariat ***Model Privacy Bill for Public Sector*** LMM(02)7 November 2002 (hereafter referred to as "Commonwealth Bill for public users"); See Part II of the proposed Commonwealth Privacy Bill dealing with the collection, use, disclosure and retention of personal information by public agencies.

principle. [111]

4.2.44 Where a responsible party holds an item of information on all individuals which will be used or useful only in relation to some of them, the information is likely to be excessive and irrelevant in relation to those individuals in respect of whom it will not be used or useful and should not be held in those cases.[112]

4.2.45 Where personal information contains a general identifier, additional conditions should be laid down to protect the security of the information collected, otherwise the processing will be treated as unreasonable.

4.2.46 There should furthermore be limits to the collection of information. "Fishing expeditions" should not be allowed, and personal information should be collected for a clearly specified purpose only.[113][114] The principle is prominent in all the main international information protection instruments as well as in national legislation.[115] See Principle 3 below.

---

111 Information Commissioner ***Chapter 3: The Data Protection Principles of the IC's Legal Guidance*** Version 1 Nov 2001 (hereafter referred to as "Information Commissioner ***Data Protection Principles***") at 12.

112 Information Commissioner ***Data Protection Principles*** at 18.

113 Roos 1998 ***THRHR*** at 499 and the references made therein. See discussion below on Principle 3.

114 Pretexting is the practice of collecting information about a person using false pretenses. Typically, investigators pretext by calling family members or co-workers of the victim under the pretense of some official purpose. The family members are deceived by the pretexter and provide personal information on the victim.

115 Section 5(3) of Canada's Personal Information Protection and Electronic Documents Act 2000 states as follows:

"An organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances;

Principle 1 of the New Zealand Privacy Act 1993 stipulates as follows:

Purpose of collection of personal information

Personal information shall not be collected by any agency unless -

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and
(b) The collection of the information is necessary for that purpose.

The second Data Protection Principle in the UK Data Protection Act 1998 stipulates as follows:

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in

Minimality[116]

4.2.47 Article 6(1)(c) of the EU Directive furthermore stipulates that EU member states shall provide that personal information must be:

> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; [117]

4.2.48 The minimality principle is also manifested in Arts 7 and 8 of the Directive [118] which deal with

---

any manner incompatible with that purpose or those purposes.

116 Discussion Paper Bill Principle 1 reads as follows:

Minimality

8. Personal information may only be processed where, given the purpose(s) for which it is collected or subsequently processed, it is adequate, relevant, and not excessive (can also be included under Principle 2: Purpose specification and Principle 4:Data quality).

117 Article 5(b) and (c) of the CoE Convention contains an almost identical requirement except that it relates to the purposes for which data are "stored". See also Principle 3 of the UN Guidelines.

118 Article 7 of the EU Directive reads as follows:

Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Article 8 of the EU Directive reads as follows:
The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shalll not apply where:

a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

this question extensively, by setting out circumstances in which processing will be reasonable, and when it will not be reasonable. Clarification has been provided in the Explanatory Memorandum to the Dutch law which mentions as matters to be taken into account to determine the reasonableness of the processing: the *nature of the information*; the *nature of the processing*; whether the processing is carried out in the *private sector* or the *public sector* (with the latter being subject to a stricter assessment); and the *measures* which the controller has taken to protect the *interests of the data subject*. Also relevant is whether the processing is in accordance with a relevant *code of conduct* (in particular, of course, if the code has been positively assessed by the Information Protection Authority).[119]

4.2.49 Of crucial importance for the extent to which information processing may occur, is the interpretation of the criterion "necessary" in paras (b)-(f) of Art 7 and paras (b), (c) and (e) of Art 8(2) of the EU Directive.

4.2.50 The necessity criterion should probably be construed as embracing two overlapping requirements :[120]

a) that the processing corresponds to a pressing (and legitimate) social, political or

---

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
4.....
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to erogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.
6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

119 Korff ***EC Study*** at 80.

120 This interpretation is inspired by, and partly builds upon, the way the ECHR has construed the term "necessary" in Art 8(2) of the ECHR. Requirement (b) also follows from the criterion "not excessive" in Art icle 6(1)(c) of the Directive.

commercial need;[121]

b) that the processing is proportionate to the aim involved.

The stringency of the above two requirements will undoubtedly vary from case to case depending, inter alia, on the sensitivity of the information involved and the context in which the processing occurs.[122]

4.2.51 The amount of personal information collected should be limited to what is necessary to achieve the purpose for which the information is gathered.[123] The principle is once again summed up in terms of "minimality", though it could also be summed up using a variety of other terms such as "necessity", "non-excessiveness, "proportionality" or "frugality".[124]

4.2.52 In determining whether processing is fair/reasonable, regard is furthermore to be had to the method by which the information was obtained. [125] Fairness implies that a person is not unduly pressured into supplying information on him/herself to a responsible party. From this it arguably follows that fairness implies a certain protection from abuse by responsible parties of their monopoly position. While very few information protection instruments expressly address the latter issue, some protection from abuse of monopoly can be read into the relatively common provisions on data subject consent, particularly the requirement that such consent be "freely given."[126]

4.2.53 In order to give effect to the principle, two sets of rules can be identified:

---

121 The processing of data by credit bureaux, for instance, corresponds to a legitimate commercial and social need and it is necessary that the information collected be comprehensive so as to facilitate correct lending decisions.

122 Bygrave ***Data Protection*** at 343.

123 Section 7(1)b) of the Commonwealth Bill for private users states that the collection of the information must be necessary for, or directly related to, that purpose.

124 The term "proportionality" is used by the CoE in several of its data protection instruments. See also section 3a of Germany's Federal Data Protection Act for the term "frugality".

125 Bainbridge ***Data Protection*** at 58.

126 Bygrave ***Data Protection*** at 59.

a) rules prohibiting the processing of personal information without the consent of the data subject;

b) rules requiring responsible parties to collect information directly from data subjects in certain circumstances.

Consent[127]

4.2.54 Some privacy instruments have grappled with the consent issue. The EU Directive provides that personal information may only be processed, inter alia, if the individual concerned has "unambiguously given his consent".[128]

---

127 *Discussion Paper Bill Principle1 reads as follows:*

Consent and necessity conditions

9. (1) Personal information may only be processed where the:

(a) data subject has given consent for the processing; or
(b) processing is necessary for the performance of a contract or agreement to which the data subject is party, or for actions to be carried out at the request of the data subject and which are necessary for the conclusion or implementation of a contract; or
(c) processing is necessary in order to comply with a legal obligation to which the responsible party is subject; or
(d) processing is necessary in order to protect an interest of the data subject; or
(e) processing is necessary for the proper performance of a public law duty by the administrative body concerned or by the administrative body to which the information are provided, or
(f) processing is necessary for upholding the legitimate interests of the responsible party or of a third party to whom the information is supplied.

(2) The processing of personal information in terms of subsection (1)(e) or (f) is subject to the data subject's rights set out in sections 14, 52 and 93.

This section is furthermore to be read with the other information principles; See also ss 10, 11 and 12 of the UK Data Protection Act; arts 14 and 15 of the EU Directive; See also section 45 of the ECT Act for the opt-out option regarding unsolicited commercial communications.

128 Article 7 of the EU Directive reads as follows:

Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; ...

The Quebec Act respecting the Protection Of Personal Information in the Private Sector 1993 states as follows in section 14 :

Consent to the communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.

Consent given otherwise than in accordance with the first paragraph is without effect.

4.2.55 Other instruments make no mention of a consent requirement[129] while yet others often stipulate consent in fairly narrow contexts eg as a precondition for disclosure of information to third parties.[130]

4.2.56 It is important to note that consent is rarely laid down as the sole precondition for the particular type of processing in question; consent tends to be one of several alternative prerequisites. This is also the case with the EU Directive. [131] The alternative prerequisites are often formulated broadly, thereby reducing significantly the extent to which responsible parties are hostage to the consent requirement in practice.[132] With regard to Art 7 of the EU Directive, for example, most instances of processing will be able to be justified under the criteria in paras (b) - (f) of the provision.[133][134]

4.2.57 In the UK law, the provision allowing for processing of (non-sensitive) personal information mentions consent as one condition for processing - which contrasts with the condition for

---

129 For eg the CoE Convention.

130 Para 10 of the OECD Guidelines.

131 Art 7, see above.

132 Eg UK Data Protection Act's First Data Protection Principle states that personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met,..... Schedule 2 is based on Article 7 of the EU Directive and follows the Directive fairly closely. Six conditions are set out in the Schedule of which the first is that the data subject must have given his consent to the processing. Bainbridge ***Data Protection*** at 85 is of the opinion that in terms of the first condition it would seem that acquiescence may be sufficient such as where an individual completing a form fails to tick the ubiquitous box to declare lack of consent. Implicit consent is therefore acceptable for the purposes of condition 1 of Schedule 2.

133 Bygrave ***Data Protection*** at 66.

134 Examples of exemptions to the request of consent:

a) The responsible party may be required by law to process the data. A South African example would be where banks are required to supply the Department of Trade and Industry with statistics in relation to their lending patterns in order to prevent red lining.

b) The processing may be necessary to protect the vital interests of the data subject. Information about notifiable diseases is one such example.

c) There is also the legitimate interest exemption, where the data processor has some legitimate interest in processing data; or third parties in receiving the data (eg customers of credit bureaux). Local authority processing the data of its electricity users in order to establish what the year on year increase in electricity use is going to be would be one such example.

processing of sensitive information which refers to "explicit consent.[135]

4.2.58 In countries in which information protection is based on a constitutional principle, consent is, however, seen as either the main criterion, in the sense that all processing based on any other criterion is construed as an exception to the primary criterion of consent (France, Greece, Portugal, Italy); or as one of two main criteria, with the other one being authorisation by law (Austria, Germany). It follows from this that the other criteria must be restrictively interpreted.[136]

4.2.59 The laws in Germany and Italy stipulate that consent should (in principle) be in writing (while allowing for the giving of consent on the Internet by means of a "mouse-click").[137]

4.2.60 On this subject, the Australian Privacy Charter (1994) states:

> Individual consent justifies exceptions to some privacy principles. However, 'consent' is meaningless if people are not given full information or have no option but to consent in order to obtain a benefit or service. People have the right to withdraw their consent.

4.2.61 Even where a positive action is taken to give authorisation there sometimes remains a problem of specificity. Some organisations ask customers to sign authorisations, unlimited in time and subject matter, essentially purporting to authorise the responsible party to collect anything from anyone at any time and to use and disclose the information for any purpose to any person. One might see this as attempting to contract out of some of the limitations imposed by the information privacy principles. Such a broad consent will probably also be unreasonable (unfair and contra bonos mores).[138]

---

135 Douwe Korff ***EC Study*** at 74.

136 Ibid.

137 Ibid.

138 ***Neethling's Law of Personality*** 251; See ***ALRC Discussion Paper*** at 572 for a discussion on "bundled consent". Bundled consent is defined as the practice of an agency organisation "bundling together", or consolidating, multiple requests for individuals' consent to a wide range of uses and disclosures of personal information, without giving individuals the option of selecting to which uses and disclosures they agree. Bundled consent is often sought as part of the terms and conditions of a product or service. The ALRC at 579 expresses the view that bundling consent can often be contrary to the spirit of the privacy principles and in any event may not be good business practice. Nevertheless, in certain circumstances, particularly where the personal information in question does not fall within the definition of sensitive information, it may be appropriate for an agency organisation to use bundled consent, since it may for instance,

4.2.62 It is clear that the Directive is to ensure that the data subject agrees to whatever use the information is put. This consent may be explicit, as when the data subject expressly consents to the use of his or her information as part of the information which is processed. The consent may also be implicit, such as where a contract entered into requires the automatic processing of the data subject's information.[139]

4.2.63 Consent for the processing of nonsensitive information will therefore be regarded as valid if it amounts to a freely given, specific and informed indication of the wishes (volunté) of the data subject - but that this volunté can be expressed in a variety of ways and that (other than with regard to sensitive information, for which it needs to be express, as discussed below) it does not necessarily need to be put in writing. Thus, for instance, if a person was informed of an intention on the part of a responsible party to use his (non-sensitive) information for a specific purpose, and was offered an opportunity to object to this use (e.g., by means of a negative tick-box on a form), yet did not use this opportunity (i.e. by returning the form without the box being ticked), his consent to the use of his information can be inferred from this (in)action.[140]

4.2.64 In South Africa, section 51 (1) of the Electronic Communications and Transactions Act[141] suggests a regime, whereby the consent of the data subject is needed, unless the data controller (responsible party) is required or permitted by law to process the information. [142]

---

obviate the need to contact a customer repeatedly about minor issues.

139 The LOA argued that clients should be afforded the right to consent, or not, to the collection of information. Consent can often be inferred from the behaviour of the data subject. For example, where a data subject adds their name to a distribution list. Consent should therefore be permissible both expressly and impliedly and egislation should accommodate the various types of consent.

140 Douwe Korff ***EC Study*** at 76.

141 **Principles for electronically collecting personal information**
51. (1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

142 The privacy provisions contained in the ECT Act should be seen as an interim arrangement until POPIA is enacted.

4.2.65 See the discussion in Chapter 5 below on the consent requirements in respect of unsolicited electronic communications for direct marketing.

4.2.66 It should be noted that the laws in several EU member states - Greece, the Netherlands, Spain - stress that consent which does not meet the requirements of the law (and the Directive) must be regarded as null and void (i.e. not just as voidable). The laws in Austria, Denmark, the Netherlands, Spain and Sweden add that consent to processing may be revoked at any time (albeit without retrospective effect, as most make clear). The UK data protection authority has said, somewhat more ambiguously:[143]

> Even when consent has been given it will not necessarily endure forever. While in most cases consent will endure for as long as the processing to which it relates continues, data controllers should recognise that the individual may be able to withdraw their consent.

Collection directly from data subject[144]

---

143 Douwe Korff ***EC Study*** at 77.

144 Discussion Paper Bill Principle 1 reads as follows:

Collection directly from data subject

10. (1) Personal information must be collected directly from the data subject.

(2)It is not necessary to comply with subsection (1) of this principle if -
(a) the information is contained in a public record; or
(b) the data subject authorises collection of the information from someone else; or
(c) non-compliance would not prejudice the interests of the data subject; or
(d) non-compliance is necessary –
(i) To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) For the enforcement of a law imposing a pecuniary penalty; or
(iii) For the protection of the public revenue; or
(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(v) In the interests of national security; or
(vi) for upholding the lawful interests of the responsible party or of a third party to whom the information are supplied;

(e) compliance would prejudice a purpose of the collection; or

(f) compliance is not reasonably practicable in the circumstances of the particular case; or

(g) the information -
(i) will not be used in a form in which the individual concerned is identified; or
(ii) will be used for statistical or research purposes and will not be published in a form that could identify the individual concerned; or
(h) the collection of the information is in accordance with an authority granted under section 33 (exemptions) of this Act.

4.2.67 Rules requiring that information may only be collected from the subject directly, are found only in a minority of information protection instruments,[145] though such rules could and should be read into the more common and general requirement that personal information be processed fairly. In New Zealand the principle is set out in Principle 2 of their Act.[146]

(ii) Evaluation

4.2.68 In general it was stated [147] that the principles of limitation of the processing of personal information as set out in sections 7 to 10 of the draft Bill are in accordance with the EU Directive and other international laws. These sections are therefore acceptable in that only specifically

---

145 Section 5(1) of Canada's Federal Privacy Act of 1982, IPP 2 of the New Zealand Privacy Act and NPP 1.4 in Schedule 3 to Australia's federal Privacy Act.

146 **PRINCIPLE 2**

Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.
(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds -

(a) That the information is publicly available information; or
(b) That the individual concerned authorises collection of the information from someone else; or
(c) That non-compliance would not prejudice the interests of the individual concerned; or
(d) That non-compliance is necessary -

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) For the enforcement of a law imposing a pecuniary penalty; or
(iii) For the protection of the public revenue; or
(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(e) That compliance would prejudice the purposes of the collection; or
(f) That compliance is not reasonably practicable in the circumstances of the particular case; or
(g) That the information -

(i) Will not be used in a form in which the individual concerned is identified; or
(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

147 Law Society of South Africa.

applicable data can be processed in particular circumstances and nothing superfluous is to be stored or collected.

Lawfulness (section 7)

4.2.69 The question was posed[148] when an intrusion would be deemed unreasonable. Would holding a name, address and telephone number, which is generally public information, and contacting the prospect during office hours be an intrusion to an unreasonable extent? Or would it only be unreasonable, if the prospect did not have the option to ask not to be contacted, or if the contact were to be made at 10pm? [149]

4.2.70 It was argued that this section raises the issue of the balancing of the protection of privacy rights with the commercial requirements for use and processing of personal information. Until such time as clear precedents are established, it will be difficult to clearly determine what this standard would allow and disallow. The Commission was urged to require of the regulatory authority to issue directives or guidelines or for regulations to be implemented as soon after the Act is promulgated as possible, setting forth guidelines for various industries, including the financial services industry, as to what would be acceptable processing in accordance with this section and what would fall foul of these provisions. The codes of conduct may also be used to clarify these requirements from an industry-specific perspective.[150]

Minimality (section 8)

4.2.71 Clarity was requested[151] regarding the terms "adequate", "relevant" and "not excessive". Will these terms be more clearly described by the Commissioner in Regulations or is it intended that

148 NIA; Nedbank; SAIA.

149 SAIA; See discussion on direct marketing in Chapter 5 below.

150 Nedbank.

151 SAFPS; NIA; SAIA; LOA.

the terms will be left open to interpretation by the judiciary at some later stage?

4.2.72 It was suggested[152] that the Principle of Minimality should remain as a separate clause and should not be incorporated under Principle 2. By including Minimality as a discreet clause, its importance will be emphasised.

4.2.73 Medical schemes have to ensure that members are provided with appropriate, cost effective medical interventions. In order to achieve this, schemes need to maintain significant amounts of data some of which may have little immediate relevance or value but could be highly significant at a later stage. With this in mind, it was submitted that allowance had to be made for the retention of data by medical schemes and that, in this instance, principle of "minimality" should not pertain.[153]

Consent, justification and objection (section 9)

4.2.74 One commentator[154] agreed that processing should only be allowed to the extent to which the data subject have consented. However, another[155] stated that the process of requiring consent is too vague. The procedure should be spelt out.

4.2.75 It was submitted[156] that the word *"pursuing"* in clause 9(1)(f) in the Discussion Paper Bill should be substituted for the word *"upholding"* and by the addition of a semi-colon and the word ***"or"*** at the end of the subsection such that the amended section reads:

(f) processing is necessary for pursuing the legitimate interests of the responsible party or

---

152 Provincial Administration of Western Cape.

153 Board of Health Care Funders; Momentum Health.

154 MTN (Pty) Ltd.

155 Department of Public Works.

156 Foschini's; SA Insurance Association; Michaelson's Attorneys.

of a third party to whom the information is supplied.[157]

4.2.76 It was argued that the use of the word *"pursue"* encompasses a broader range of legitimate commercial and marketing activities than the word *"upholding"* as presently used in the draft Bill.

4.2.77 It was furthermore suggested[158] that a further sub-section be included that reads:

> (g) where the processing relates only to the title, name, identity number, telephone numbers, contact email addresses, physical and postal addresses of the data subject; "

4.2.78 Commentators[159] understood that it would be advisable for medical schemes to obtain specific member consent for the processing of information but argued that such consent is not strictly necessary in order to process such member's personal information. They based this contention on the fact processing may also be necessary for the performance of a contract or agreement to which the data subject is party and the fact that the Bill is not consent driven.[160]

4.2.79 In Issue Paper 24 the question was posed whether the opt-out approach would constitute valid consent. Responses were varied.

4.2.80 It was argued that the "opt-out" approach implies implicit consent;[161] and would constitute valid consent, provided it meets all the criteria of implied consent required by the common law and

---

157 In this regard, it was noted that the UK Data Protection Act of 1998 stipulates that one of the grounds for the lawful processing of personal data is where:
6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
The UK approach has also been followed in an identical manner by both Guernsey and the Isle of Man, whose data privacy laws, like Argentina's were determined to be "adequate" in terms of the EU Data Protection Directive by the decisions of the EU Council issued on 21 November 2003 and 28 April 2004 respectively.

158 Foschini's.

159 Board of Health Care Funders; Momentum Health.

160 Sovereign Health.

161 SABC.

set out in the privacy instruments.[162]

4.2.81 It was suggested that the following requirements be met by responsible parties when the "opt-out" approach is being used:-[163]

a) the information about the individual must only be used within defined legal limits and for the purposes for which it was collected, unless otherwise expressly agreed between the parties, in which case the use of such information should not be contrary to public policy; and

b) before it can be said an individual has impliedly consented to his or her information being disclosed, he or she must in the circumstances have exercised an informed choice. In this regard the onus should be on the responsible party to point out any fine printing to the individual and, accordingly, the safety mechanism must be so that were litigation to ensue, the onus must be on the responsible party to prove that the individual's failure to respond was a positive decision.[164]

---

162 Vodacom.

163 SABC.

164 This requirement (informed consent) was re-iterated by the Banking Council.

4.2.82 The banking industry explained that it has adopted the opt-out approach[165] since there is no clear guidance in South African legislation as to how the 'consent' issue should be addressed and also because of the prohibitive costs and administration should consent have to be sought for each and every application of personal information.[166]

4.2.83 It was argued that a clear distinction is necessary between the use of personal information for marketing of services and products, and the use for processing product applications, verification of personal details, credit assessment, fraud prevention and statutory reporting obligations (FICA for instance). In order to make the distinction clear, the Banking Council has, for instance, treated marketing of products and other uses of personal information separately in the new Code of

---

165 In the new Code of Banking Practice, effective from June 2004, the consent issue is dealt with as follows:

"4.7.1 Information about your personal debts and/or the manner in which you conduct your accounts may, in appropriate circumstances, be disclosed to credit risk management services where:

- you have fallen behind with your payments or you are in default with the terms of a product or service, and you have not made satisfactory proposals to us for repayment of your debt following formal demand and you have been given at least 28 calendar days' notice of our intention to disclose; or
- you have given us written, electronic or in the case of telephone banking, verbal consent; or
- your cheque is referred to drawer, in which case the information may be placed on a cheque verification service.

4.7.2 In respect of the marketing of services or products if you are:

- a new client, we will obtain your consent at the beginning of your relationship with us;
- an existing client we will inform you that you may withhold or withdraw your consent and how to exercise that choice. If you do not withhold your consent, we will presume that you agree to us continuing to market the services or products

With your consent we may:

- bring to your attention details of our services and products, which may be of interest to you;
- give certain information about you to other subsidiaries within our group for marketing purposes;
- inform you about another company's services or products and, if you respond positively, you may be contacted directly by that company.

We will not pressurise you by suggesting that access to any of our services and products is conditional upon your consent".

166 The Banking Council.

Banking Practice.[167]

4.2.84 It was, however, also reiterated[168] that any opt-out abilities should be kept in check (see especially the discussion on direct marketing below) and that the notion of "informed consent" should be supported. As an example, a consumer should be aware of the fact that he is agreeing to allowing a bank to share his or her information with its insurance business and financial planning affiliated companies, and not for the benefit of a whole range of unrelated services, for example, travel services, IT services or for the sale of household products. It was noted that many of the problems that could be seen as consent issues would, however, be addressed by the purpose specification and further processing principles.

4.2.85 Practically, the concern may be that a bank has common databases which house client information across group companies and that accordingly, the Act will require the bank and all the

---

167 **4.6 Confidentiality and privacy**

We will treat all your information as private and confidential (even when you are no longer a client). Except as set out in 4.7.1 below, we will not disclose any information about your accounts or your personal details to anyone, including other companies in our group, other than in four exceptional cases permitted by law. These are:

- where we are legally compelled to do so;
- where it is in the public interest to disclose;
- where our interests require disclosure (This will not be used as a reason for disclosing information about you or your accounts [including your name and address] to anyone else including other companies in our group for marketing purposes);
- where disclosure is made at your request or with your written or verbal consent. If you make use of electronic banking facilities like telephone banking, and the telephone calls are recorded, consent to disclosure might be recorded verbally.

5.1 Provision of credit

5.1.1 We will market and approve credit responsibly (based on the information you supply to us), to match your borrowing requirements and capabilities and supply you with suitable products, in an attempt to ensure that you are not extended beyond your financial means. However, our ability to do so depends on your compliance with our expectations of you set out in 5.11.4 regarding your financial affairs.

5.1.2 All lending will be subject to an assessment of your ability to afford and willingness to repay. This assessment may include:

- taking into account your income and expenses, including the dependability of your income;
- how you handled your financial affairs in the past;
- information obtained from credit risk management services and related services, and other appropriate parties, for example, employers, other lenders and landlords;
- how you have conducted your previous and existing accounts with us;
- information supplied by you, including verification of your identity and the purpose of the borrowing;
- credit assessment techniques, for example, credit scoring;"

168 Nedbank.

group companies who share common databases to obtain consents which are drafted in such a way so as to allow this practice to continue and at the same time to ensure that they meet the purpose specification and further processing requirements. Having multiple and separate databases is not always cost effective or practical, because practically, the obligation to then keep such information updated becomes a much more complex task.[169]

4.2.86 The Commission was referred to the fact that organisations may have large client databases, which have been generated over decades. The question was posed wether these organisations will still be able to make use of these existing databases in order to up-sell or cross-sell to existing policyholders, as they do not have the consent of the policyholder to process this information, if it is not being used for its initial purpose, which was to purchase the policy. Even the internal sharing of information between the business units of the same Insurer will be impacted.[170]

Directly from data subject: (section 10)

4.2.87 Some commentators [171] were of the opinion that the provisions of 10(2)(d)(iii), (e) and (f) are too wide and that the phrase "not reasonably practicable" should be clarified.[172]

4.2.88 The Commission was referred[173] to the fact that the Financial Intelligence Centre Act, and the Prevention of Organised Crime Act, the Protection of Constitutional Democracies against Terrorist Activities Act also impose duties on private bodies (including individuals) to prevent and detect (and in some cases investigate) certain criminal activities or offences. It was therefore recommended that this obligation be acknowledged in the subsection dealing with the requirements for collection of information.

---

169 Nedbank.

170 See discussion on "grandfathering" in Chapter 3 above.

171 Department of Communications; Nedbank.

172 See discussion above on purposive interpretation of principles-based legislation.

173 Banking Association.

4.2.89 It was suggested that the "legitimate interests" of the responsible party or third party when the information is supplied as referred to in subclause 10(2)(d)(vi) of the Discussion Paper Bill should be evaluated against the confidentiality provisions of the FAIS Codes and Code of Banking Practice as well.

4.2.90 It was furthermore stated[174] that section 10(2)(e) of the Discussion Paper Bill had to refer to the "lawful" purpose to read as follows:

(e) compliance would prejudice a lawful purpose of the collection;

4.2.91 See the discussion on public records in Chapter 3 above.

(iii) Recommendation

4.2.92 Principle 2 sets out a framework for the processing of personal information by requiring that the information must be processed by lawful means and, where appropriate, with the knowledge or consent of the data subject. Responsible parties must, furthermore, collect personal information directly from the subject of the information, where possible, or alternatively, inform the subject of the collection of the information where it is obtained through a third party.

4.2.93 A consent requirement is included as set out below as one of the lawful ways in which personal information may be processed.[175] The legislation is, however, not consent-driven. This means that there are also other alternatives available for responsible parties to ensure lawful processing. Processing of sensitive information and processing in respect of unsolicited electronic communications for the purpose of direct marketing are

---

174 Nedbank.

175 See the definition of consent in clause 2 of the Bill: 'consent" means any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal information relating to them.

notable exceptions to this rule. In these instances the general rule requires the explicit consent of the data subject. [176] **It should, furthermore, be noted that consent is often sought by responsible parties, in any event.**

4.2.94 However, processing will, for instance, be justified where it is necessary for pursuing the legitimate interests of the responsible party, even where consent has not been obtained. However, the data subject will in certain cases where consent has not been obtained, have a right to object to the processing on reasonable grounds. Where the data subject objects, the processing will have to be ceased.

4.2.95 It stands to reason, that in order to be able to object, the data subjects need to have knowledge of the fact that their personal information is being collected. Provision is therefore made in the other Principles for the elements of "openness" and "purpose specification". [177] **It is therefore clear that the different principles relate closely to each other and that all the principles should always be read together.** [178]

4.2.96 The concept of informing data subjects that processing is taking place and providing them with the option to object against the processing, is sometimes referred to as implied consent or so-called "opt-out consent". The Bill can therefore, in general, be regarded as opt-out legislation.

4.2.97 Finally, where possible, responsible parties are required to collect personal information directly from the person concerned. Guidance should be provided in codes of

---

176 See discussion in Chapter 5 (unsolicited electronic communications) and in para 4.3 (sensitive information) below.

177 See Principle 3, clause 13 (purpose specification) and Principle 6,clause 17(2)(openness).

178 In the ***ALRC Discussion Paper*** at 584 it was argued that consent is already a critical element of a number of other privacy principles- especially those dealing with use and disclosure, transborder flows and the collection of sensitive information and that it may therefore not be necessary to make provision for a discreet principle dealing specifically with consent.

conduct and guidelines[179] as to what exactly terms such as "legitimate interest" and "reasonably practicable"[180] should mean in a specific context or sector.

4.2.98 The Commission's recommendation for the legislative enactment of Principle 2 is as follows:

PRINCIPLE 2

Processing limitation

Lawfulness of processing

8. Personal information must be processed -

(a) lawfully; and

(b) in a reasonable manner in order not to infringe the privacy of the data subject.

Minimality

9. Personal information may only be processed if, given the purpose(s) for which it is processed, it is adequate, relevant, and not excessive.

Consent, justification and objection

10.(1) Personal information may only be processed if -

(a) the data subject has consented to the processing;

---

179 See discussion on codes of conduct and the duties of the Information Regulator.

180 Clause 11(2) (d)(v) and 11(2) (f).

(b) processing is necessary for the conclusion or performance of a contract to which the data subject is party, or to carry out actions that are necessary for the conclusion or performance of such a contract;

(c) processing is necessary to comply with an obligation imposed by law on the responsible party;

(d) processing is necessary to protect a legitimate interest of the data subject;

(e) processing is necessary for the proper performance of a public law duty by a public body; or

(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

(2) A data subject may object, at any time, on reasonable grounds relating to his, her or its particular situation, in the prescribed manner, to the processing of personal information, in terms of subsection (1)(d) to (f), unless otherwise provided for in national legislation.

(3) If a data subject has objected to the processing of personal information in terms of subsection (2) the responsible party may no longer process the personal information.

Collection directly from data subject

11.(1) Personal information must be collected directly from the data subject, except as otherwise provided in this section.

(2) It is not necessary to comply with subsection (1) of this section if -

(a) the information is contained in a public record or has deliberately been made public by the data subject;

(b) the data subject has consented to the collection of the information from another source;

(c) collection of the information from another source would not prejudice a legitimate interest of the data subject;

(d) collection of the information from another source is necessary --

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) to enforce a law imposing a pecuniary penalty;

(iii) to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997;

(iv) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

(v) in the legitimate interests of national security; or

(vi) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

(e) compliance would prejudice a lawful purpose of the collection; or

(f) compliance is not reasonably practicable in the circumstances of the particular case.

(c) Principle 3: Purpose specification

(i) Proposals in Discussion Paper

4.2.99 The OECD "purpose specification principle" (Principle 3) reads as follows:

> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4.2.100 This principle is furthermore set out in Article 6(1)(b) of the EU Directive.[181] See also the basic regulatory premise - embodied in arts 7 and 8 of the EU Directive - which is that the processing of data is prohibited unless it is necessary for the achievement of specific goals. [182]

Purpose specified at time of collection[183]

---

181 Article 6(1)(b) of the EU Directive stipulates that Member States shall provide that personal data must be:
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

182 See discussion in Roos thesis at 483; Clause 11 of Principle 2 in the Discussion Paper Bill reads as follows:

PRINCIPLE 2

Collection for specific purpose

11. Personal information must be collected for a specific, explicitly defined and legitimate purpose.

See also Dutch Privacy law, art 7 and New Zealand Privacy Act, Principle 3.

183 Clause 12 of Principle 2 in the Discussion Paper Bill reads as follows:

Data subject aware of purpose of collection and intended recipients

12.(1) Where personal information is collected, such steps must be taken as are, in the circumstances, reasonably practicable to ensure that the data subject is aware of -
(a) a purpose for which the information is being collected; and
(b) the intended recipients of the information.

(2) The steps referred to in subsection (1) of this section must be taken before the information is collected or, if that is not reasonably practicable, as soon as reasonably practicable after the information is collected.

(3) The steps referred to in subsection (1) of this section in relation to the collection of information from the data subject need not be taken if those steps have been taken previously in relation to the collection from that data subject, of the same information or information of the same kind and the purpose of collection and intended recipients of the information are unchanged.

(4) It is not necessary to comply with subsection (1) of this section where -
(a) non-compliance is authorised by the data subject; or
(b) non-compliance will not prejudice the interests of the data subject; or
(c) non-compliance is necessary -
(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) for the enforcement of a law imposing a pecuniary penalty; or
(iii) for the protection of the public revenue; or
(iv) for the conduct of proceedings before any court or tribunal being proceedingsthat have been commenced or are reasonably in contemplation; or
(v) in the interests of national security; or
(d) compliance would prejudice a lawful purpose of the collection; or
(e) compliance is not reasonably practicable in the circumstances of the particular case; or
(f) the information will -
(i) not be used in a form in which the data subject is identified; or
(ii) be used for statistical or research purposes and will not be published to any third party in a form that could identify the data subject.

4.2.101 It may be open to responsible parties to proclaim their functions or activities on a very broad basis. It may be relatively easy for a responsible party to claim that it had broader purposes in mind than were fully understood by the individual from whom information was collected. The problem is how to be sure as to what a responsible party's function or activities were at the time of collection. Explaining the purpose of collection is, furthermore, seen as of greatest importance, but should any other explanations be required, such as an indication as to whether collection is mandatory or voluntary?[184]

4.2.102 This task is theoretically more straightforward in jurisdictions having a registration/notification process. In those jurisdictions agencies are required to register a list of their functions or activities and the purposes for which they collect information.[185] They are therefore not permitted to use the information for an unregistered purpose. [186] (It is proposed that the South African legislation will make provision for a process of notification. See Principle 6 below as well as the discussion in Chapter 7 below.)

4.2.103 Where no registration or notification takes place, it might be possible for responsible parties/data processors to have a statement of their functions and activities and their purposes for collecting information on their own file. The suggestion is that this could be verified in some way, such as by having a dated copy open for inspection at the responsible party/data processor or published from time to time, for example in a responsible party's annual report.

4.2.104 Another approach might place an onus on the responsible party to prove these matters in the event of a complaint. Naturally, a responsible party would have a defence when it

---

184 New Zealand Discussion Paper at 3.

185 New Zealand, Australia and Canada have rejected a registration process as being too bureaucratic, imposing unreasonable compliance costs on business and government, and as being ineffective in enhancing privacy. See discussion below dealing with the notification process.

186 Part II of Schedule I of the UK Data Protection Act indicates that there are two means by which a data user may specify the purpose for which the personal data are obtained namely, in a notice given by the data controller to the data subject and in a notification given to the Commissioner under the notification provisions of the Act.

has actually taken steps to communicate its purposes to the individual concerned. Where this has not been done the responsible party would be obliged to make out a case where there are doubts as to the matter.

4.2.105 A third suggestion would be to oblige bodies to give notice to the regulatory authority in certain exceptional cases where a high degree of sensitivity exists in respect of the purpose of the information. [187]

4.2.106 For example, because of competition, credit bureaux are not inclined to register a list of their functions or activities but may be prepared to compile an internal statement of their functions, activities and purposes for processing information, which statement can be open for inspection by the regulatory authority.[188]

4.2.107 The UK law stipulates that the purpose of any processing may be specified in particular, in the information given to the data subject or in the particulars notified to the information protection authority in the context of notification. In the UK (as elsewhere) the notified purposes are, however, often expressed in broad terms - which means that responsible parties can claim some considerable leeway with regard to both the primary and any secondary purposes.[189]

4.2.108 For the purpose of this principle the point is that the determining specification is the one provided to the data subjects when the information is obtained, and not the one set out in a responsible parties' notification. [190]

---

187 New Zealand Discussion Paper at 2.

188 The CBA submitted that in defining the legitimate purpose/s for which data is processed within the South African credit information system cognizance should be taken of the fact that credit bureaux in South Africa have reached a level of maturity and sophistication comparable with the most mature systems in the world and consequently are able to provide information for the assessments of risks other than credit risks such as insurance risk; and provide information for purposes of fraud prevention .

189 Douwe Korff ***EC Study*** at 63.

190 Douwe Korff ***EC Study*** at 64.

Retention of records[191]

4.2.109 Article 6(1)(e) of the EU Directive stipulates that Member States shall provide that personal data must be:

> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

4.2.110 See also art 5(e) of the CoE Convention.[192] The Commonwealth Model Law for private sector sets out the finality of records in art 20 (2) and (3).[193]

---

191 Clause 13 of Principle 2 set out in the Discussion Paper Bill reads as follows:

Retention of records

13. (1) Subject to subsections (2) and (3), records of personal information must not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless-
(a) another law requires or authorises the responsible party to retain the record;
(b) the responsible party reasonably requires the record for purposes related to its operation;
(c) the record is retained in terms of any contractual rights or obligations of the parties;
(d) the data subject has authorised the responsible party to retain the record.

(2) Records of personal information may be retained for periods in excess of those provided for under (1) only where the retention of these records are for historical, statistical or scientific purposes, and where the responsible party has established appropriate safeguards against the records being used for any other purposes.

(3) A responsible party that has used a record of personal information about an individual to make a decision about the individual must -
a) retain the record for such period of time as may be prescribed by law; or
b) where there is no law prescribing a retention period, for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

(4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after it is no longer authorised to retain the record under subsection (1).

192 Art 5(e) of the CoE Convention reads as follows:

Article 5
Quality of data
Personal data undergoing automatic processing shall be:
a) - d).....

. e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

193 Article 20

Retention of records
(1).....

4.2.111 The OECD Guidelines omit a specific provision on the destruction or anonymisation of personal data after a certain period. However, it may be required pursuant to the principle of "purpose specification". Many, but not all,[194] national laws make specific provision for the erasure etc of personal information once the data are no longer required.[195]

4.2.112 For example in national laws, see Data Protection Principle 5 in the UK Data Protection Act[196] and Principle 9 of the New Zealand Privacy Act. [197] Similar provisions are found in several other jurisdictions. See for example, principle 2(2) of the Hong Kong Personal Data (Privacy) Ordinance[198] and the 1993 Quebec Act respecting the Protection of Personal Information in the Private Sector (section 12).[199]

4.2.113 The principle will always be subject to the requirements of other enactments. There are, for example, laws requiring taxpayers to retain taxation records and health agencies to retain

---

(2) An organisation that has used a record of personal information about an individual to make a decision about the individual shall retain the record for such period of time as may be prescribed after making the decision, to allow the individual a reasonable opportunity to request access to the information.
(3) An organisation shall destroy or delete a record of personal information or de-identify it as soon as it is no longer authorised to retain the record under subsection (1).

194 US federal Privacy Act 1974 being an example.

195 Bygrave ***Data Protection*** at 60.

196 Fifth Principle
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

197 New Zealand Discussion Paper at 6:
Principle 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

198 Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are to be used.

199 Once the object of a file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned, subject to a time limit prescribed by law or by a retention schedule established by government regulations.

medical records. In the public sector the national archives [200] and national[201] and local [202] government require the retention of certain archives.[203]

4.2.114 Concerns have been expressed that over zealous application of this principle might lead to premature destruction of records which may in fact turn out to be useful to the responsible party and able to be used both lawfully and in accordance with the information privacy principles. It may also be possible, for example, for the responsible party to return documents to the data subject or disclose the information to another responsible party that does have a further lawful use for the information.

4.2.115 Of course, personal privacy and autonomy may also be harmed by the premature destruction of information. Examples include:

* destruction by the sole repository of information concerning a person's origins (such as information about a birth parent in an adoption context or about donor of gametes in relation to offspring born through assisted human reproduction);
* destruction of personal information so as to prevent the individual concerned exercising a right of access;
* destruction of information upon which a decision has been based so as to prevent any review of that decision or exercise of any judicial or administrative remedies (for example, information which would have indicated unlawful discrimination in an employment decision).

---

200 National Archives of South Africa Act 43 of 1996.

201 Electoral Act 73 of 1998.

202 Eg the Local Government Municipal Electoral Act 27 of 2000 and the Local Government Municipal Property Act 6 of 2004.

203 New Zealand Discussion Paper at 6; SAHA believes that any adoption of such a principle must explicitly recognise that:

*Categories of “personal” and “public” information are not mutually exclusive.
*The “purpose” of a document may include indefinite retention in a public archive as a document of enduring value.
*Destruction of certain records is legally impermissible under the National Archives Act and provincial archival legislation until such time as an assessment has been made of whether they are records of enduring value.

4.2.116 It was submitted that guidelines should be provided but that self-regulation, in the form of individual codes of conduct, should define the applicable retention periods.[204]

4.2.117 Different laws require different record retention periods. For instance, financial and accounting information is generally retained for a pre-determined time period (approximately 5 years), while long-term insurance contracts can easily have a contractual duration equal to or extending beyond the lifetime of the life assured. Legislation such as the Financial Intelligence Centre Act provides that records should be retained for 5 years after the termination of an insurance contract.[205] It was argued that fraud information should remain in a correctly managed storage system for an indefinite period and should not be restricted to a 3 or 5 year deletion.[206]

4.2.118 The British Columbia Freedom of Information and Protection of Privacy Act has tackled this issue directly. In a section entitled "retention of personal information" (section 31) it states:

> If a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

4.2.119 In the Commonwealth Model Bill for the public sector this principle is set out in art 14.[207] In the Model Law for the private sector it is set out in art 20.[208]

---

204 The Banking Council.

205 LOA.

206 SAFPS.

207 **Retention and disposal of personal information**

14.(1) Where a public authority uses personal information for an administrative purpose, it shall retain the information for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual concerned has a reasonable opportunity to obtain access to the information, if necessary.
(2) Subject to subsection (1) and this Act, the Minister shall prescribe by regulation, guidelines for the retention and disposal of personal information held by a public authority.

208 **Retention of records**

20.(1) Subject to subsection (2), an organisation shall not retain a record of personal information after the purpose for which the organisation collected the information has been fulfilled unless –
(a) another law requires the organisation to retain the record;
(b) the organisation reasonably requires the record for purposes related to its operation; or
(c) the regulations authorise the organisation to retain it.
(2) An organisation that has used a record of personal information about an individual to make a decision about the individual shall retain the record for such period of time as may be prescribed after making the decision, to allow the

(ii) Evaluation

Purpose declared

4.2.120 Respondents to the discussion papers mostly agreed with this principle.[209] Responsible parties should be obliged to identify the minimum amount of information that is required in order to fulfil their purpose properly and this will be a question of fact in each case. If it is necessary to hold additional information about certain individuals, such information should only be collected and recorded in those limited cases. It should not be acceptable to hold information on the basis that it might possibly be useful in future without a view of how it will be used.[210]

4.2.121 Information should, therefore, only be collected for a purpose or purposes specified clearly to the data subject at the time the data is collected .[211] It was submitted that the law should stipulate that such obligations rest with the person or body which is the first original collector of the data and not the subsequent data distributor.[212]

4.2.122 Another commentator[213] reiterated that sections 11 (and 14) of the Discussion

---

individual a reasonable opportunity to request access to the information.
(3) An organisation shall destroy or delete a record of personal information or de-identify it as soon as it is no longer authorised to retain the record under subsection (1).

209 See eg ENF for Nedbank; LOA; Credit Bureau Association.

210 See eg. ENF for Nedbank; LOA; Law Society of South Africa; See also the discussion on minimality under Principle 2 above.

211 Law Society of South Africa.

212 Credit Bureaux Association.

213 Society of Advocates of Kwazulu- Natal.

Paper Bill are fundamental to the proposed Act and should be a cornerstone of the proposed Act. These principles are consistent with principles established internationally. The commentators supported the fact that the Bill makes provision for non-compliance where such non-compliance is necessary, for example, to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences (para 13(3)(c)(I) of the Bill.

4.2.123 One submission,[214] however, cautioned that the whole local and international regime relating to anti-money laundering and combatting the financing of terrorism is a dynamic, constantly evolving arena where additional demands are being legislated, regulated or imposed by regulators. These new demands would have to be processed on personal information outside of the specific, explicitly defined original purposes. A typical example is the Financial Intelligence Centre Act, implemented in 2003, and where the application of the Act was significantly expanded by Guidance Note 3 (for banks) issued in mid 2005. Presumably the various caveats relating to compliance with the law will provide satisfactory protection to affected institutions impacted by these changes.

4.2.124 It was, however, emphasised that it should be clear how the purpose should be determined in terms of the Bill and this determination should be clarified in relevant regulations or directives under the Bill or in terms of the relevant codes of conduct. The normal practice is for most organisations, who are a part of a group of companies, to obtain consent for related services which may be provided by affiliate or sister companies, such as insurance services, as part of the consent for banking services. In addition, consent would be obtained in respect of all banking and financial services offerings across the board and not specific to each specific banking service.[215]

4.2.125 It was noted[216] that clause 12 (4)(c) of the Discussion paper Bill does not contain an equivalent to clause 10 (2)(d)(vi)[217] of the same Bill and suggested that this clause must be included in the context of clause 12.

---

214 Banking Association.

215 Nedbank.

216 SAIA.

217 Non-compliance is necessary for upholding the lawful interests of the responsible party or of a third party to whom the information is supplied.

Retention of records (section 13)

4.2.126 There was agreement that this section is essential.[218] One commentator [219] submitted that the retention periods be aligned with the retention period proposed by the NCA so as to have some uniformity of application. Another[220] suggested that a specific time limit must be determined eg 12 months after the information has been collected. It was also recognised[221] that retention periods could also be regulated in terms of codes of conduct contemplated to be issued in terms of chapter 7 and suggested that this provision be specifically included.

4.2.127 An example was provided of instances where it would be important to address best practices in a specific sector (eg. where retention periods are concerned one may want to clarify what would constitute "purposes related to its operation" in a code of conduct.[222] Where a data subject applies for a credit card and is declined, the information gathered pursuant to the credit card application can no longer be retained as the purpose for which it was originally gathered, has been satisfied. The information is then destroyed or de-identified. If that data subject shortly thereafter makes another application for a credit card, the bank may be completely unaware of this fact. It may be that such concerns are accommodated by section 13(1)(b) of the Discussion Paper Bill, but in circumstances where the Bank may need to keep information for a considerable period of time, namely longer than that required by FICA, it may not provide sufficiently for this scenario.

4.2.128 It was also stated, in general, that the Intelligence Services would not be in a position to conduct its functions effectively if it has to comply with the Bill. The Commission must never be allowed to authorise the processing of personal information of members of the Intelligence Services or categories/groupings of such members per se. It is always the objective of the

---

218 Banking Council.

219 Land and Agriculture Development Bank.

220 Department of Communications.

221 Vodacom (Pty) Ltd.

222 Banking Association.

Intelligence Services to act in the public interest and therefore it is already subject to scrutiny and oversight in terms of national legislation. It will also never be possible to act on conditions as the Commission thinks fit.[223]

(iii) Recommendation

4.2. 129 After evaluating the submissions received, the Commission confirms the proposals set out in the "collection principle" in the Discussion Paper. It is, however, decided to move the notification requirements to Principle 6 (Openness) which is also sometimes referred to as the "notification principle", leaving only a reference to the principle in clause 13. This is another example where the Principles need to be read together.

4.2.130 Information should, therefore, be processed for a specific and lawful purpose related to the functions or activity of the responsible party. At the time it is collected, or as soon as practicable afterwards, the responsible party must take reasonable steps to ensure, inter alia, that data subjects are aware of the purpose of the collection of the information.

4.2.131 It should be noted that Principle 3 underpins every other aspect of the processing of the information, since it determines the scope of the processing of the information. No exceptions are provided to the requirement that collection must be collected for a specific, explicitly defined and lawful purpose. Principle 3 also forms the basis for Principle 4 as the latter Principle states that information may not be distributed for a purpose other than the purpose for which it was collected as set out in Principle 3.

4.2.132 The most effective means of protecting a person's privacy rights is, furthermore, to limit access to the person's information. If the information is destroyed or permanently de-identified, the information self-evidently cannot be accessed or misused.

---

223 NIA.

Information should, therefore, not be kept longer than necessary for the purposes for which it is processed. The only exceptions to this rule would be those necessary in a democratic society on one of the grounds listed in article 13 of the Directive.[224]

4.2.133 No unacceptable tension exists between the retention requirement in the Bill and retention requirements in other legislation since provision is specifically made for retention of a record where this is required or authorised by law.[225]

4.2.134 The Commission recommends that the legislative enactment to give effect to Principle 3 should read as follows:

PRINCIPLE 3

Purpose specification

Collection for specific purpose

12. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

Data subject aware of the purpose of collection of information

13. Steps must be taken in accordance with section 17(2) below to ensure that the data subject is aware of the purpose of the collection of the information as referred to in section 12 above.

Retention of records

14.(1) Subject to subsections (2) and (3), records of personal information must not be retained

---

224 See also Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC adopted on 25 March 2006.

225 Clause 14(1)(a).

any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless -

(a) retention of the record is required or authorised by law;

(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject has consented to the retention of the record.

(2) Records of personal information may be retained for periods in excess of those provided for under subsection (1) for historical, statistical or research purposes, and if the responsible party has established appropriate safeguards against the records being used for any other purposes.

(3) A responsible party that has used a record of personal information about a data subject to make a decision about the data subject must -

a) retain the record for such period as may be required or prescribed by law or a code of conduct; or

b) if there is no law or code of conduct prescribing a retention period, for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

(4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after it is no longer authorised to retain the record in terms of subsection (1) or (2).

(5) The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.

(d) Principle 4: Further Processing Limitation[226]

(i) Proposals in Discussion Paper[227]

4.2.135 The principles of collection limitation, purpose specification and use limitation are closely related and require that, once personal information is collected, there are limits to the internal uses to which a collecting body may put it, or to the external disclosure that may be made. [228]The notion of "relevance" underlies all these principles, since the information may be processed

---

226 The term "further processing" includes both the use and the disclosure of information.

227 Principle 3 of the Discussion Paper Bill reads as follows:

PRINCIPLE 3
Further processing limitation

Further processing not incompatible with purpose of collection

14. (1) Personal information must not be further processed in a way incompatible with a purpose for which it has been collected in terms of principle 2.

(2) For the purposes of assessing whether processing is incompatible, as referred to under subsection (1), the responsible party must take account of the following -

(a) the relationship between the purpose of the intended further processing and the purpose for which the information has been obtained;
(b) the nature of the information concerned;
(c) the consequences of the intended further processing for the data subject;
(d) the manner in which the information has been obtained, and
(e) any contractual rights and obligations existing between the parties.

(3) The further processing of personal information must not be regarded as incompatible as referred to under subsection (1) where -

(a) the processing of the information for that other purpose is authorised by the data subject; or
(b) the source of the information is a publicly available publication; or
(c) non-compliance is necessary -
(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) for the enforcement of a law imposing a pecuniary penalty; or
(iii) for the protection of the public revenue; or
(iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(v) in the interests of national security; or
(d) the processing of the information for that other purpose is necessary to prevent or mitigate a serious and imminent threat to-
(i) public health or public safety; or
(ii) the life or health of the data subject or another individual; or
(e) the information is used for historical, statistical or scientific purposes where the responsible party has made the necessary arrangements to ensure that the further processing is carried out solely for these specific purposes and will not be published in a form from which the identity of the data subject may be established or inferred; or (f) the further processing of the information is in accordance with an authority granted under section 33 (exemptions) of this Act.

228 See discussion in Roos thesis at 496; ***ALRC Discussion Paper*** at 673 states that in a practical sense, use and disclosure will often be dealt with identically; however, a single use and disclosure principle does not preclude use and disclosure being treated differently where appropriate.

only for purposes specified at the time of collection.[229] Information gathered to determine income tax liability, for example, may not be used to evaluate eligibility for social assistance. If information is disclosed for other purposes, the consent of the individual must first be obtained.[230]

4.2.136 In practice, there should, therefore, be limits to the use and disclosure of personal information: personal information should not be (used or) disclosed for other purposes except with the consent of the data subject; or by the authority of law.[231]

Further use of personal information for specified purpose

4.2.137 In New Zealand this principle is set out in Principle 10:Limits on use of personal information[232] and in the UK it is set out in Principle 2.[233]

4.2.138 The idea of limiting use of personal information only for purposes specified at the time of collection (or compatible purposes or those authorised by the individual concerned or by law) lies at the heart of any information protection law.[234]

4.2.139 The Commonwealth Model Law for the Public sector makes provision for this

---

229 See purpose principle above.

230 Roos 1998 ***THRHR*** at 505.

231 Para 10 of the OECD Guidelines; CDT's Guide to Online privacy "Privacy Basics: Generic Principles of Fair Information Practices" found at http://www.cdt.org/privacy/guide/basic/generic.html (hereafter referred to as "CDT Guide").

232 New Zealand Discussion Paper at 7.

233 The second Data Protection Principle in the UK Protection of Data Act stipulates as follows:
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

234 The principle itself is straightforward and runs only to a single sentence. However, the detail is to be found in the list of exceptions.

principle in section 9.[235] The Commonwealth Model Law for the private sector also makes provision for this principle in sections 12, 14 and 15.[236]

---

235 **Limits on use of personal information**

9. Subject to section 12, where a public authority holds personal information that was collected in connection with a particular purpose, it shall not use that information for any other purpose unless –
(a) the individual concerned authorises the use of the information for that other purpose;
(b) use of the information for that other purpose is authorised or required by or under law;
(c) the purpose for which the information is used is directly related to the purpose for which the information was collected;
(d) the information is used -
(i) in a form in which the individual concerned is not identified; or
(ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;
(e) the authority believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety; or
(f) use of the information for that other purpose is necessary -
(i) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law;
(ii) for the enforcement of a law imposing a pecuniary penalty;
(iii) for the protection of public revenue;
(iv) for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
(v) in the interests of national security.

236 **Limits on use of personal information**

12.(1) Where an organisation holds personal information that was collected in connection with a particular purpose, it shall not use that information for any other purpose unless –
(a) the individual concerned authorises the use of the information for that other purpose;
(b) use of the information for that other purpose is authorised or required by or under law;
(c) the purpose for which the information is used is directly related to the purpose for which the information was collected;
(d) the information is used -
(i) in a form in which the individual concerned is not identified; or
(ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;
(e) the organisation believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety; or
(f) use of the information for that other purpose is necessary -
(i) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law; or
(ii) for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.
(2) Where an organisation uses personal information for a new purpose, it shall document that purpose in order to comply with section 21(5)(d).

Condition for use or disclosure of personal information

14. An organisation shall only use or disclose personal information under section 12 or section 13, where such use or disclosure would not amount to an unreasonable invasion of privacy of the individual concerned, taking into account the specific nature of the personal information and the specific purpose for which it is to be so used or disclosed.

Use of personal information outside *[name of country]*

15.(1) An organisation shall not use, outside *[name of country]* personal information collected in *[name of country]* unless the organisation -
(a) would be permitted under this Act to make the same use of that information in *[name of country];* and
(b) takes appropriate steps to preserve the confidentiality of the information and to protect the privacy of individuals.
(2) Nothing in this section affects the use of personal information that is required or authorised to be made under another Act.

4.2.140 Two questions must be distinguished. First of all, what should be regarded as the specified purpose, [237] and secondly, how is the incompatibility of any secondary processing with the primary purpose to be determined.[238]

4.2.141 In Belgium the law stipulates that the compatibility or incompatibility of secondary uses must be assessed in the light of the reasonable expectations of the data subjects. This stipulation derives from a court ruling under a previous law in which it was held, by reference to that test, that a bank could not, without the consent of its customers, use its customers' payment information (which showed how much they paid other companies for certain insurances) to offer them cheaper insurance from its own insurance division. [239]

4.2.142 In Germany, the permissibility or otherwise of secondary processing of personal information for purposes different from the one for which the information was obtained (or disclosed) depends on the application of a variety of (slightly varying) balance tests, without express reference to compatibility. Basically, information may be used for a different purpose if this serves a(manifest) legitimate (or protection-worthy) interest of the responsible party or a third party, provided there are no counter-prevailing legitimate interests of the data subjects. These tests were also developed under a previous law with regard to public-sector processing, and in that context were strictly applied: the interest for which the information could be used had to be manifest, and manifestly stronger than the interests of the data subject against such change of purpose. The extension of these tests to the private sector in principle amounts to a significant tightening of the law in Germany - but it is too early to see how this test will be applied to the private sector in practice. [240]

---

237 Dealt with in Principle 3.

238 Douwe Korff ***EC Study*** at 63. In practice, the two are closely linked, as can be well shown by contrasting law and practice under the UK and Irish laws.

239 Douwe Korff ***EC Study*** at 64.

240 Douwe Korff ***EC Study*** at 64.

4.2.143 The information protection authority in France takes into account, in particular, whether the data subject is under a legal obligation to provide the information (or has little choice in practice, eg. as concerns the supply of essential services), and whether the responsible party bears a special duty of confidentiality (as is the case with information held by financial institutions or medical doctors etc.).[241]

4.2.144 The Dutch law elaborates further on matters to be taken into account in determining whether processing for a secondary purpose is "(in)compatible" with the primary purpose for which the information was obtained. It mentions as examples of such matters: the relationship between the primary and secondary purposes; the nature of the information; the consequences of the(secondary) processing for the data subject; as well as the manner in which the information was obtained and the extent to which "suitable safeguards" have been provided to protect the interests of the data subjects.

4.2.145 In other words, under the Dutch Law the question of"compatibility" is addressed very much like the question of "balance" in the context of the information protection criteria. Indeed, the two tests are closely intertwined. It follows from the compatible use requirement that (eg) insurers may not use medical information obtained in the context of an insurance claim in order to take decisions on requests for a different insurance from the same customer; that information obtained in the context of a sale may not be used (without specific consent) to promote unrelated goods and services offered by the responsible party; that the creation of a personality profile on the basis of such sale information is also incompatible; as is the making of selections in mailings on the basis of sensitive criteria. Thus, for instance, the authorities have suggested that a pharmacist may not send out a mailing to customers who have bought contact lenses, about a new contact-lens-cleaning fluid (unless the customers expressly and consented to this beforehand).[242]

4.2.146 An issue has arisen overseas as to whether "browsing" constitutes a "use" under

---

241 Douwe Korff ***EC Study*** at 65.

242 Douwe Korff ***EC Study*** at 65.

such a principle. In England it was suggested that simply reading personal information, but not employing that information for a purpose, may not constitute "use". In that case it could be shown that a police officer had checked a confidential police information base for details of debtors being investigated by his friend but it could not be proved that the information had been passed on or actually put to a use. The Court treated the accessing of the computer record as a prerequisite to use rather than use itself.

4.2.147 The Commissioner, furthermore, had to form a view on the meaning of the term in a Principle 8 case where a responsible party stored and retrieved information, but nothing else had apparently happened. The Commissioner concluded that in order to show that some usage had occurred, the retrieval would need to have been followed by some act.

4.2.148 Article 6(1)(b) of the Directive[243] in principle allows for the further processing of personal information for research purposes, even if the information had not been collected for those purposes, as long as the appropriate safeguards are provided. However, the processing of sensitive information for such purposes (other than with the consent of the data subjects) is only allowed on the basis of article 8(4)[244], i.e. the Member States may only allow processing (even with suitable safeguards) with regard to research which serves a substantial public interest. [245]

---

243 Art 6(1) (b) reads as follows:

Article 6
1. Member States shall provide that personal data must be:
(a).....
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide apprpriate safeguards;

244 Art 8(4) reads as follows:

Article 8
4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

245 Douwe Korff ***EC Study*** at 66. In the Netherlands and Sweden, processing of non-sensitive data for research purposes is subject to rather limited safeguards only. The Dutch law merely requires safeguards to ensure that any data used for research purposes are only used for those purposes (without otherwise protecting the data subjects).The proviso about research data not being used to take decisions in respect of the data subjects is also set out in the UK law, which adds to this a weighted balance test: data are not [to be] processed [for research purposes] in such a way that substantial damage or substantial distress is, or is likely to be caused to any data subject. Overall, the rules concerning secondary processing of personal information for research purposes without the consent of the data subjects thus vary very considerably: some consist of rather general substantive rules, others of more detailed substantive requirements; some rely on procedural safeguards; and some combine substantive and procedural rules. Some are contained in the data protection law; and

4.2.149 It should be noted that the use of credit information for the purposes of compiling marketing lists is a controversial issue. However, it has been argued that the use of credit information for marketing purposes is not always a negative practice as it is better to ensure that consumers that are over-committed or in difficulties are removed from such lists. Without the use of credit information, marketing will not stop, it will simply become more general, increasing the exposure of those who are vulnerable. Opt-out consent could perhaps provide the necessary protection in this regard. [246]

Disclosure of information to third parties

4.2.150 In so far as the disclosure of information to third parties is concerned this principle is not always consistently expressed in information protection instruments. Moreover, neither the CoE Convention nor the EU Directive specifically addresses the issue of disclosure limitation but treat it as part of the broader issue of the conditions for processing information. Thus, neither of these instruments apparently recognises disclosure limitation as a separate principle but incorporates it within other principles, particularly those of fair and lawful processing and of purpose specification.

4.2.151 The OECD Guidelines incorporate the principle of disclosure limitation within a broader principle termed the "Use Limitation Principle", [247] while the UN Guidelines specifically

---

some in other laws or regulations.

246 Credit Bureau Association. See the discussion on credit bureaux in Chapter 5.

247 Principle 4 of the OECD Guidelines reads as follows: (para 10)

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
a) with the consent of the data subject; or
b) by the authority of law.

address the issue of disclosure under the principle of purpose specification.[248]

4.2.152 Disclosure limitation is, however, sometimes singled out as a separate principle in its own right because it tends to play a distinct and significant role in shaping information protection laws. Concomitantly, numerous national statutes expressly delineate it as a separate principle or set of rules.[249]

4.2.153 In New Zealand this principle is set out in Principle 11[250]: Limits on disclosure of

---

248 Bygrave ***Data Protection*** at 67.

249 Bygrave ***Data Protection*** at 67.

250 **PRINCIPLE 11**

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds -

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
(b) That the source of the information is a publicly available publication; or
(c) That the disclosure is to the individual concerned; or
(d) That the disclosure is authorised by the individual concerned; or
(e) That non-compliance is necessary -

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) For the enforcement of a law imposing a pecuniary penalty; or
(iii) For the protection of the public revenue; or
(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to:

(i) Public health or public safety; or
(ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or
(h) That the information -

(i) Is to be used in a form in which the individual concerned is not identified; or
(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

personal information.[251] The Commonwealth Model Law for the Public sector makes provision for this principle in sections 11 and 12[252] and in the Model Law for the private sector in sections 13 and 16.[253]

---

251 New Zealand Discussion Paper at 7.

252 **Limits on disclosure of personal information**

11.(1) Subject to section 12, where a public authority holds personal information, it shall not disclose the information to a person, body or agency (other than the individual concerned), unless-
(a) the individual concerned has expressly or impliedly consented to the disclosure;
(b) the disclosure of the information is required or authorised by or under law;
(c) the disclosure of the information is one of the purposes in connection with which the information was collected, or is directly connected to that purpose;
(d) the individual concerned is reasonably likely to have been aware or made aware under section 8 (2)(c) that information of that kind is usually passed on to that person, body or agency;
(e) the information is to be disclosed -
(i) in a form in which the individual concerned is not identified; or
(ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(f) the authority believes on reasonable grounds that disclosure of the information is necessary -
(i) to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety;
(ii) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law;
(iii) the enforcement of a law imposing a pecuniary penalty;
(iv) the protection of public revenue;
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
(vi) in the interests of national security.
(2) Any person, body or agency to whom personal information is disclosed under subsection (1) shall not use or disclose the information for a purpose other than the purpose for which the information was given to that person, body or agency.

Condition for use or disclosure of personal information

12. A public authority shall only use or disclose personal information under section 10 or section 11, where such use or disclosure would not amount to an unreasonable invasion of privacy of the individual concerned, taking into account the specific nature of the personal information and the specific purpose for which it is to be so used or disclosed.

253 **Limits on disclosure of personal information**

13.(1) Where an organisation holds personal information, it shall not disclose the information to another person, body or agency (other than the individual concerned), unless –
(a) the individual concerned has expressly or impliedly consented to the disclosure;
(b) the disclosure of the information is required or authorised by or under law;
(c) the disclosure of the information is one of the purposes in connection with which the information was collected, or is directly connected to that purpose;
(d) the individual concerned is reasonably likely to have been aware or made aware under section 10(2)(c) that information of that kind is usually passed on to that person, body or agency;
(e) the information is to be disclosed -
(i) in a form in which the individual concerned is not identified; or
(ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(f) the organisation believes on reasonable grounds that disclosure of the information is necessary –
(i) to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety;
(ii) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law; or
(iii) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

(ii) Evaluation

Further use of personal information

4.2.154 Commentators[254] agreed that information should, in principle, not be used other than agreed or consented to by the data subject. Commentators were, however, concerned with the clarification of detail:

a) One commentator[255] requested that the words " further processing" be defined and requested clarity regarding the definition of "incompatibility".

b) It was also advised[256] that the words ""the necessary arrangements" be deleted.

c) One commentator[257] inquired as to when processing will be in the national interest.

4.2.155 It was furthermore agreed[258] that further processing of health or health-related data could be justifiable under some conditions. However, careful consideration will have to be given

---

(2) Any person, body or agency to whom personal information is disclosed under subsection (1) shall not use or disclose the information for a purpose other than the purpose for which the information was given to that person, body or agency.

Disclosure of personal information outside *[name of country]*

16.(1) An organisation shall not disclose personal information collected in *[name of country]* to an organisation outside *[name of country]* unless –
(a) the organisation receiving the information performs functions comparable to the functions performed by a person to whom this Act would permit disclosure by the organisation disclosing the information in *[name of country];* and
(b) the organisation disclosing the information believes on reasonable grounds that the organisation receiving the information will take appropriate steps to preserve the confidentiality of the information.
(2) Nothing in this section affects a disclosure of personal information that is required or authorised to be made under another Act.

254 MTN (Pty) Ltd; SAFPS.

255 Department of Communications.

256 Cell C. Cell C furthermore indicated that it fully complies with its Licence and that the Cell C licence states in clause 9: The Licensee shall not use any information regarding its past, current or potential customers for purposes other than those for which the information was obtained, unless the customer gives prior written consent to such other use.

257 NIA.

258 SA Medical Research Council.

to the circumstances under which this is to be allowed. Again, health research ethics committees, using this legislation as one of the sets of guiding provisions, have an important role to play in guiding potential data users. Where such 'further processing' is done for other purposes, e.g. for risk management or product development by health care funders, guidelines in terms of this legislation could prove useful.

4.2.156 The Private Health Information Standards Committee (PHISC) has in the past suggested that patient disclaimers be modified to include specific provision for further processing under defined conditions (e.g. that patient data is not identifiable), but no specific activities related to this have been undertaken by PHISC.

4.2.157 See furthermore the discussion regarding profiling in Chapter 5 below.

Disclosure

4.2.158 In the Discussion Papers the question was posed whether institutions should be allowed to share information and, if so, under what circumstances. Submissions were received from the following sectors: insurance, banking, credit bureaux, the fraud prevention service, archives and communications.[259]

4.2.159 An insurance contract is entered into for the payment of a premium to insure against the occurrence of a specific risk. In long-term insurance, this risk relates to death or certain health events. The medical history of the assured is of critical importance to every insurer in determining the risk of the occurrence of the insured event. In addition, fraud is a common element, for example applicants for insurance policies are often not truthful regarding their medical history. For this reason, the long-term insurers in South Africa have arranged for the sharing of information regarding these "notifiable impairments". It is essential that such a system of sharing of information

259 It is imperative that the SABC is allowed access to data stored by other responsible parties to ensure that the SABC is able to collect licence fees from defaulters.

continues, or long-term insurers will not be able to properly assess the risks involved.[260]

4.2.160 Nedbank indicated that an area which will need to be carefully considered is that of the use of information within a company's group to its subsidiaries or affiliates or across brands, divisions or product areas within an organisation and the effect of data protection legislation preventing such cross selling and marketing practices, eg. where a bank passes sales leads to its insurance affiliates or subsidiaries.[261]

4.2.161 The Banking Industry recommended that banks be permitted to share account information on a customer's account behaviour across their financial subsidiaries, for purposes of credit control. [262] However, data sharing amongst or between different institutions should only be allowed for defined purposes, such as the use of credit bureaux, fraud prevention and subject to clients' informed consent.[263]

4.2.162 Data sharing within the context of the South African credit information system prevents over-commitment, bad debt, fraud , money laundering and promotes responsible lending,

---

260 LOA.

261 Where companies within a group share a common IT infrastructure, the cost of creating separate and often, in effect, duplicate databases of client information is not practical. The new, updated draft Code of Banking Practice already provides for an opt-in procedure for banks to share information within their group.

262 The Banking Industry.

263 Data sharing within and amongst organisations in the banking industry is critical for the following purposes (this is not a *numerus clausus*):

* Marketing of services and products;
* Evaluation of applications for products and credit;
* Management of relationships and accounts within the group;
* Application of score cards in lending;
* Development of score cards for risk management;
* Risk management;
* Fraud prevention;
* Supply of bank reports and bank codes amongst banks;

Sanlam Life indicated that there is no neat watertight division in the provision of certain financial services eg an application for a loan from a bank to be secured by an insurance policy. Under these circumstances data shared between institutions is necessary to give effect to contractual provisions.

and accordingly should be allowed.[264][265]

4.2.163 The sharing of data in the fraud prevention arena has led to a reduction in fraud and other economic crime. SAFPS agrees that the sharing of data has to be carried out within the principles of data privacy.[266] It is, however, proposed that there should be a provision similar to section 29 of the UK Data Protection Act in any future legislation.[267]

4.2.164 SAHA indicated that any restriction on data-sharing should explicitly be subject to provision under the National Archives Act for transfer of records of enduring value to the National Archives. The same principle applies to provincial archives legislation and services.[268] [269]

4.2.165 Respondents generally felt that information should be shared (disclosed), but subject to specific conditions. It was held that, although there has been a growth in information sharing,[270] there is currently legal uncertainty as to the legality of such practices as well as the proper ways of handling the information.[271]

---

264 Credit Bureau Association.

265 In so far as credit bureaux are concerned it was suggested that those who wish to access a credit report should obtain the consent of the data subject and the onus to obtain the consent should rest on the entity wishing to access the report. Also the collectors of the information should obtain consent at the time of collection for the uses to which the data will be put. Again, the onus would be on the subscribers or clients of the credit bureaux.

266 SAFPS.

267 In response to the Issue Paper one respondent indicated that this principle should not be rigidly interpreted, should it be incorporated into future legislation. It was argued that article 6(1)(b) and (c) of the EU Directive is draconian and needs to be more flexible to permit data supplied fraudulently to be disseminated within closed user groups. With regard to the dissemination of data supplied fraudulently by a data subject, the only limitation that should be imposed is that the data so provided is only disseminated within a closed user group and would not be available for general use. In addition those organisations contributing to such a closed user group should be restricted in the manner in which they utilise such data.

268 SAHA.

269 Restriction on "data-sharing" under privacy legislation should be subject to explicit provision in the National Archives Act and provincial archives legislation for transferring records of enduring value to these institutions.

270 SALRC ***Issue Paper 24*** at 122.

271 MFSA.

4.2.166 One commentator noted that It seems that the most important pre-condition for the sharing of information is consent. Any information shared must be with the consent of the person (i.e. when giving consent the person must know that the information will be shared in certain circumstances).[272]

4.2.167 Different views were expressed regarding the nature of the consent required. One respondent stated that sharing should only be allowed on written consent of the subject.[273] Another view was that the consent requirements should constitute an 'opt out' option as discussed.

4.2.168 It was also argued that a distinction should be drawn between a legitimate private interest and public interest: sharing for a legitimate private interest should be with the knowledge and consent of the data subject whereas information sharing which is in the public interest such as information sharing within the credit information system should be just with the knowledge of the data subject as it is not advisable to place limitations on information sharing that is in the public interest.[274]

4.2.169 An example of the implementation of this provision was provided by the LOA which indicated that all potential applicants are required to furnish their consent to the disclosure of information to the shared information base maintained by the LOA[275].

---

272 Vodacom.

273 Strata.

274 Credit Bureau Association.

275 The LOA Code on the Life Register provides for the following form of detailed consent (clause 8.2.1 and 8.2.2 of the Code):

An Authorisation shall be obtained from each proposer and life insured to which a proposal for insurance, falling within the business limits set out in paragraph 3.2, relates.

The Authorisation must be in the following form using the wording, and only the wording, set out below:-

Accepting that I am thereby curtailing my right of privacy, but to facilitate the assessment of the risks, and the consideration of any claim for benefits, under a policy related to this or any other proposal for insurance made by me, or in respect of me as life assured, I irrevocably authorise ABC -

(a) to obtain from any person, whom I hereby so authorise and request to give, any

4.2.170 However, it was noted that in the prevention of crime environment, consent of the subject cannot be obtained as such a requirement will result in a miscarriage of justice. Crime cannot be effectively addressed in isolation. If the police investigator is not talking to the prosecutor who will eventually be presenting the State's case there can hardly be any expectation of success. Information sharing is thus a reality which should rather be controlled than outlawed. [276]

4.2.171 In April 2003 the Performance and Innovation Unit (PIU) in the UK, one of Whitehall's most influential bodies, produced a report,[277] the purpose of which was to review problems associated with information sharing and ensure that information lawfully in the possession of any government body can be shared with another government body for any purpose.[278]

4.2.172 It has been argued that the PIU report effectively marginalised information protection to enable information sharing to take place.[279] This is because it breaches the second principle of the UK Data Protection Act of 1998, which states that information gathered for one purpose cannot be used for another purpose.

---

information which ABC deems necessary, and

(b) *to share with other insurers that information and any information contained in this proposal or in any related policy or other document, either directly or through a data base operated by or for insurers as a group,*

at any time (even after my death) and in such detailed, abbreviated or coded form as may from time to time be decided by ABC or by the operators of such database.

SIGNATURE OF EACH PROPOSER AND LIFE ASSURED

(Note: to be signed by the legal guardian in the case of a minor or person under legal disability)"

276 SAPS.

277 Performance and Innovation Unit UK Cabinet Office ***Privacy and Data-sharing, the Way Forward for the Public Services*** (hereafter referred to as PIU report) April 2002 available at http://www.number-10.gov.uk/su/privacy/index.htm**.**

278 Whilst the PIU Report focuses on government bodies, the principles apply equally to companies and other "private bodies"**.**

279 Sarah Williams "Writing in Computers and Law" available at http://www.scl.org/Services/default.asp?p=154&c=-999&ctID=12&cID=1140000634.

4.2.173 Different views were expressed as to who should be responsible for the accuracy and maintenance of the information where it is shared by different entities. Some commentators held that the data processor should be responsible.[280] [281] However, many felt that since the responsible party was ultimately accountable, he or she should also be responsible for shared information (with or without other parties). [282] [283] Some argued that the responsible party should be responsible for supplying accurate information to the data processor, who should then be responsible for the maintenance of the information.[284] See discussion on Principle 1 (accountability) above and Principle 7 (Security) below.

(iii) Recommendation

4.2.174 The Commission confirms its proposal as set out in the Discussion paper that the further processing of personal information must be compatible with the lawful purpose for which it was originally collected. Further processing includes both the use and disclosure of information.

4.2.175 Guidelines are set out in the Bill to assess whether processing will be compatible or not. In general, the further processing should be something that arises in the context of the original purpose. A number of exceptions are, furthermore, included that indicates circumstances in which the further processing will not be regarded as incompatible with the original purpose of collection.

---

280 SAFPS..

281 Liberty Group Ltd indicated that, as regards the quality, the databases are shared 'as is" – whoever uses it has an obligation to ensure that the data are accurate. Once no longer in its possession, the responsibility lies with the subsequent responsible party. SAPS argued that the accuracy and maintenance of data that is shared should be the responsibility of both the gatherer and the user of the data.

282 The Banking Industry.

283 ENF for Nedbank.

284 Credit Bureau Association.

4.2.176 The Commission's recommendation for the legislative enactment of the principle is as follows:

PRINCIPLE 4

Further processing limitation

Further processing to be compatible with purpose of collection

15.(1) Further processing of personal information must be compatible with the purpose for which it was collected in terms of principle 3.

(2) To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of the following -

(a) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

(b) the nature of the information concerned;

(c) the consequences of the intended further processing for the data subject;

(d) the manner in which the information has been collected, and

(e) any contractual rights and obligations between the parties.

(3) The further processing of personal information is not incompatible with the purpose of collection if -

(a) the data subject has consented to the further processing of the information;

(b) the information is available in a public record or has deliberately been made public by the data subject;

(c) further processing is necessary -

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) to enforce a law imposing a pecuniary penalty;

(iii) to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997;

(iv) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

(v) in the legitimate interests of national security;

(d) the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to -

(i) public health or public safety; or

(ii) the life or health of the data subject or another individual;

(e) the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for these specific purposes and will not be published in an identified form; or

(f) the further processing of the information is in accordance with an authority granted under section 34 (exemptions) of this Act.

(e) Principle 5: Information Quality

(i) Proposals in the Discussion Paper[285]

4.2.177 Principle 2 of the OECD Guidelines reads as follows:[286]

> Data Quality Principle
>
> Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

4.2.178 Article 6(1)(d) of the EU Directive stipulates that Member States shall provide that personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. [287]

4.2.179 It was noted that responsible parties should continually monitor compliance with this principle. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate, [288] and use thereof unreasonable.

4.2.180 All information protection laws contain rules directly embodying the principle, but they vary considerably in their wording, scope and stringency. Information protection laws use a variety of

---

285 **PRINCIPLE 4**

Quality of information to be ensured

15. The responsible party must take the reasonably practicable steps, given the purpose for which personal information is collected or subsequently processed, to ensure that the personal information is complete, not misleading, up to date and accurate.

Based on Information quality OECD par 8; CoE art 5; EU Dir art 6(1) (c); Roos thesis at 492.

286 CDT's Guide.

287 See discussion in Roos thesis at 490.

288 Information Commissioner ***Data Protection Principles*** at 18.

terms to describe the stipulated information quality. Article 5(d) of the CoE Convention and Art 6(1)(d) of the EU Directive refers to “accurate” and “up to date” data. See also Data Protection Principle 4 in Part 1 of Schedule 1 to the UK Act.[289] Other laws refer to “accuracy or correctness” or “completeness” (OECD Guidelines).[290]

4.2.181 Variation exists in terms of the stringency with which information protection instruments require checks on the validity of personal information. The standard set by the EU Directive, for example, is in terms of “every reasonable step must be taken” (art 6(1)(d)). By contrast the UN Guidelines emphasizes a duty to carry out “regular checks” (principle 2).[291] In the UK it is not enough for a responsible party to say that, because the information was obtained from either the data subject or a third party, they had done all they could reasonably have done to ensure the accuracy of the information at the time. They have to go further and take reasonable steps to ensure the accuracy of the information themselves and mark the information with any objections. The extent to which such steps are necessary will depend on the (negative) consequences of the inaccuracy for the data subject. [292]

4.2.182 Thus, both the UK law and the (current, pre-implementation) Irish law - which is not to be changed in this respect - stipulate that information shall only be regarded as inaccurate if they are incorrect or misleading as to any matter of fact - which means that opinions or assessments of a person can never be inaccurate (although they could possibly be challenged if they were manifestly based on incorrect factual information). Other States may be less rigid in this regard.[293]

4.2.183 The Irish law also says - again, in a provision in the current law which is to be retained in the new (amended) law - that the principle requiring information to be accurate and, where

---

289 Fourth Principle
Personal data shall be accurate and, where necessary, kept up to date.

290 Bygrave ***Data Protection*** at 62.

291 Bygrave ***Data Protection*** at 63.

292 Information Commissioner ***Data Protection Principles*** at 19.

293 Douwe Korff ***EC Report*** at 62.

necessary, kept up to date does not apply to back-up information. However, it would be better to clarify that if information is archived or retained for back-up, and date-stamped, it can be regarded as accurate as long as it truly reflects the situation at the time of storage; and that it is only necessary to update such information if it is retrieved.[294]

4.2.184 It has also been argued that attention has to be given to securing adequate quality not just of data and information but the *systems* used to process them.[295]

4.2.185 In the Commonwealth Model Law for the public sector the data quality principle is manifested in art 9.[296] In the Model Law for the private sector it can be found in art 17.[297]

4.2.186 In New Zealand the principle manifests itself in Principle 8 stipulating that the accuracy etc of personal information has to be checked before use. [298]

---

294 Douwe Korff ***EC Report*** at 62.

295 Bygrave ***Data Protection*** at 13.

296 **Accuracy etc of personal information to be checked before use**

9. Where a public authority holds personal information, having regard to the purpose for which the information is proposed to be used, it shall not use that information without taking such steps as are, in the circumstances, reasonable to ensure that the information is complete, accurate, up to date, relevant and not misleading.

297 **Accuracy of information**

17.(1) An organisation that collects, uses or discloses personal information about an individual shall –
(a) take all reasonable steps to ensure that whatever record it makes of the information is as accurate, complete and up-to- date as is necessary for the purposes for which it collects, uses or discloses the information, as the case may be;
(b) take all reasonable steps to minimise the possibility that an organisation will use inaccurate personal information to make a decision about the individual.

(2) The organisation shall not update a record of personal information about an individual unless–
(a) doing so is necessary to fulfil the purpose for which the organisation collec ted the information;
(b) the individual consents to the updating; or
(c) this Act or another law permits the updating.

298 New Zealand Discussion Paper at 6.
Principle 8

Accuracy, etc, of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

4.2.187 Even though the finality principle has been included in Principle 3 above, it is sometimes dealt with in the information quality principle and then requires that personal information should be erased or anonymised once it is no longer required for the purpose for which it has been kept.[299]

4.2.188 A privacy risk exists where such personal information is retained since:[300]

* the information may become out of date and therefore should not be used;
* accumulations of personal information create a risk that they will be used regardless of the purpose for which the information was obtained, or the ability to approach the individual directly for the same information;
* the retention of personal information well beyond its "use by date" represents an additional and avoidable security risk as it may inadvertently be disclosed.

4.2.189 To comply with this principle responsible parties will need to review their personal information regularly and to delete the information which is no longer required for their purposes.[301] See Principle 3 (Purpose specification) above.

(ii) Evaluation

4.2.190 Commentators, in general,[302] agreed that the quality of personal information should be maintained and section 15 of the Discussion Paper Bill was supported.

4.2.191 The Commission was referred to certain factors which make the quality of information

---

299 Art 5 of the CoE Convention.

300 Bygrave ***Data Protection*** at 60***.***

301 Information Commissioner ***Data Protection Principles*** at 20.

302 SAFPS.

retention difficult. Information may be saved in a different format and in different mediums,[303] eg. one person may make telephonic contact in providing information, another may write a letter, while a third may use electronic mail. Another problem could be the migration of information from one medium to another. The responsible party should, however, be responsible and accountable for building safeguards to protect against information becoming corrupt or lost because of technology obsolescence.[304]

4.2.192 The impact of the provision on costs to be incurred by responsible parties in order to comply with the Bill was also highlighted.[305]

4.2.193 It was suggested[306] that the phrase "up to date" should be qualified with the words "where necessary", in accordance with article 6 to the EU Directive. A strong view was expressed[307] that where information is being kept for archival or record purposes and will not be re-used, it should be unnecessary to maintain such information by updating it, since it would be very time consuming, costly and would serve no purpose whatsoever.

4.2.194 It was furthermore argued that there should be a reciprocal obligation on the part of the clients of a business to ensure that they notify the business of changes to their personal information. It would be extremely onerous to maintain large numbers of records updated, without assistance or co-operation from the clients themselves, and without the clients being legally mandated to have the obligation to do so. It was proposed that this condition could perhaps be set out in codes of conduct.

---

303 The Banking Council.

304 LOA.

305 CAPES.

306 Nedbank.

307 Nedbank.

(iii) Recommendation

4.2.195 The Commission recommends that a distinct information quality principle be included in the Bill as proposed in the Discussion Paper.

4.2.196 Even though there may be a cost implication for business, it is envisaged that this principle would encourage good record information management, which is an excellent principle to work towards. It reaffirms the idea that the data protection legislation should be seen as the implementation of ordinary, good business practice. A phased implementation period may perhaps be considered.

4.2.197 The Commission recommends that the legislative enactment of the principle should read as follows:

PRINCIPLE 5

Information quality

Quality of information to be ensured

16. The responsible party must take reasonably practicable steps, having regard to the purpose for which personal information is collected or further processed, to ensure that the personal information is complete, not misleading, accurate and updated where necessary.

(f) Principle 6: Openness

(i) Proposals in the Discussion Paper[308]

4.2.198 The principle of openness flows from the notion of fairness and transparency set out above.[309] It is furthermore the first part of the principle giving effect to data subject participation and control. Before an individual can request access to personal information, he or she has to have

---

308 **PRINCIPLE 5**
Openness

Notification to Commission and to data subject

16. (1) Personal information may only be collected by a responsible party that has notified the Commission accordingly in terms of this Act, and which notification has been noted in a register kept by the Commission for this purpose.

(2) Where a responsible party collects personal information about a data subject, the responsible party must take such steps as are, in the circumstances, reasonably practicable to ensure that the data subject is aware of -
(a) the fact that the information is being collected;
(b) the name and address of the responsible party;
(c) whether or not the supply of the information by that data subject is voluntary or mandatory and the consequences of failure to reply; and
(d) where the collection of information is authorised or required under any law, the particular law to which the collection is subject.

(3) The steps referred to in subsection (2) of this section must be taken before the information is collected or, if that is not reasonably practicable, as soon as reasonably practicable after the information is collected.

(4) A responsible party is not required to take the steps referred to in subsection (2) of this section in relation to the collection of information from a data subject if a responsible party has previously taken those steps in relation to the collection, from that data subject, of the same information or information of the same kind.

(5) It is not necessary for a responsible party to comply with subsection (2) of this section if -
(a) non-compliance is authorised by the data subject; or
(b) non-compliance would not prejudice the interests of the data subject; or
(c) non-compliance is necessary -
(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) for the enforcement of a law imposing a pecuniary penalty; or
(iii) for the protection of the public revenue; or
(iv) for the conduct of proceedings before any court or tribunal being proceedings that have been commenced or are reasonably in contemplation; or
(v) in the interests of national security; or
(d) compliance would prejudice a purpose of the collection; or
(e) compliance is not reasonably practicable in the circumstances of the particular case; or
(f) the information will be used for statistical or research purpose and will not be published in a form that could reasonably be expected to identify the data subject.

309 See discussion in Roos thesis at 505.

knowledge of the fact that personal information about him or her is being kept by a specific body.[310]

4.2.199 It is clear that even the most comprehensive measures for protecting information are worthless if the individual does not have such knowledge. Without this knowledge he or she remains completely unaware that his or her privacy is threatened or even actually infringed. Therefore the responsible party should have a legal duty to notify persons concerning whom information is collected of this fact (unless, of course, they are in some other way already aware of it).[311] Obviously, allowance must be made for exceptions to this principle, for example where personal information is processed for the purposes of national security.[312]

4.2.200 The most important of these rules are those which require responsible parties to orient data subjects directly about their information-processing operations. Secondly, there are the category of rules requiring responsible parties to provide basic details of their processing of personal information to information protection authorities, coupled with a requirement that the latter store this information in a publicly accessible register.[313]

4.2.201 Principle 6 of the OECD Guidelines[314] stipulates that there should be a general policy of openness about developments, practices and policies with respect to personal information.[315]

---

310 Roos 1998 ***THRHR*** at 499.

311 ***Neethling's Law of Personality*** at 278 refers to Klopper at 266-267 who comments on the present position in SA regarding credit bureaux: "[O]nder die huidige bestel is persone nie . . . bewus van die inligting wat oor hulle bestaan nie omdat hierdie inligting agter 'n sluier van vertroulikheid verberg word wat hy (*sic*) nie eens die reg het om te lig nie." (see further McQuoid-Mason ***Law of Privacy*** at 198).

312 See in general Neethling ***Huldigingsbundel WA Joubert*** at 125-128 for exceptions.

313 Bygrave ***Data Protection*** at 63.

314 Para 9 Part II Basic Principles of National Application of OECD Guidelines; Roos 1998 ***THRHR*** at 503.

315 Principle 6 of the OECD Guidelines reads as follows:

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Means should be readily available of establishing the existence and nature of personal information, and the main purposes of its use, as well as the identity and usual residence of the responsible party.

4.2.202 Articles 10-11 of the EU Directive[316] require responsible parties (data controllers) to supply data subjects directly with basic information about the parameters of their data-processing operations, independently of the data subjects' use of access rights. The Directive therefore provides detailed guidance on the information that must be provided, and in this distinguishes between the situation in which information is obtained directly from the data subjects, and situations in which information is obtained from other sources than the data subjects.[317]

4.2.203 The laws in the EU member states, however, vary considerably with regard to the kinds of information that must be provided, the form in which it must be provided, and the time at which

---

316 Article 10 of the EU Directive reads as follows:

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11 of the EU Directive

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with at least the following information, except where he already has it:
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) any further information such as
- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.
2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

317 At 98.

it must be provided - both in circumstances in which information is collected directly from data subjects, and in cases in which information on them is otherwise obtained.[318]

4.2.204 Many information privacy laws oblige explanations only when collecting individual information directly from the individual concerned. However, a realisation as to the limitations of that approach has led some modern information privacy laws to vary the approach. The 1992 British Columbia law obliges public bodies to tell *any individual from whom it collects personal information* the purpose and legal authority for collection of personal information.

4.2.205 However, if an obligation were to be imposed on responsible parties to explain the purpose of collection when collecting information from someone other than the individual concerned, there would be a variety of issues to be worked through. For example, should the obligation arise only when collecting information from a natural person, such as a parent, or also when collecting information from another public or private body?

4.2.206 Articles 10 and 11 of the Directive are supplemented by art 21 which requires the Member States to "take measures to ensure that processing operations are publicised (art 21(1)) and to ensure that there is a register of processing operations open to public inspection (art 21(2)).

4.2.207 The UN Guidelines "principle of purpose specification" (principle 3) stipulates that the purpose of a computerised personal data file should "receive a certain amount of publicity or be brought to the attention of the person concerned".

---

318 At 98; Thus, the laws in Austria, Belgium, Denmark, the Netherlands, Portugal and Sweden all again basically follow the Directive by stipulating that the controller must inform the data subject of the identity of the controller and the purposes of the processing, and of further information only to the extent that that is necessary to ensure fair processing in respect of the data subject (or when this is necessary to allow the data subject to exercise his rights, or to safeguard those rights). The law in the UK also basically stipulates these matters - but then again qualifies this by adding that the information only needs to be provided so far as practicable and that the data subject must either be provided with the information, or have it made readily available to him. By contrast, the laws in Finland, Greece, Italy and Spain, and the proposed new (amended) law in France, are more demanding, by requiring that all the information should always be provided. Several of them also require that the information should (in principle) be given in writing (Greece, Italy) or at least explicitly, precisely and unequivocally (Spain).

4.2.208 This means that the following facts should be publicly known:[319]

a) the existence of record-keeping systems, registers and data banks that contain personal data;

b) nature of the data being processed;

c) a description of the main purpose and uses of the data; and

d) identity and usual residence of the data controller.

4.2.209 An example of the principle in national legislation is that of Principle 3 of the New Zealand Privacy Act. [320] Underlying the principle are the idea of openness: that collection of personal information should be done with the knowledge or consent of the individual concerned, that the purposes for which information is collected should be specified and that there should generally be transparency about information collection policy and individual participation in that process.[321]

4.2.210 In South Africa PAIA partly complies with this principle as far as information collected by the public sector is concerned, with the requirements in sections 14 and 15 that an index of

---

319 CDT's Guide.

320 **PRINCIPLE 3**

Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of -

(a) The fact that the information is being collected; and
(b) The purpose for which the information is being collected; and
(c) The intended recipients of the information; and
(d) The name and address of -

(i) The agency that is collecting the information; and
(ii) The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law -

(i) The particular law by or under which the collection of the information is so authorised or required; and
(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and
(g) The rights of access to, and correction of, personal information provided by these principles.

Section 4 makes provision for certain exceptions to section 1.

321 New Zealand Discussion Paper at 3.

records must be kept.[322] A similar provision is found in section 51 which applies to private bodies. PAIA does not, however, specifically deal with the collection of information.

4.2.211 In addition to the right of access to their information records, a data subjects must also have the right to require from the responsible party information as to the identity of all persons who have had access to their information record. This will enable them to ascertain whether or not the information was used for the protection of a legally recognised interest or for the purpose(s) in question. Thus the responsible party must be legally obliged, at the request of the data subject, to give him or her information concerning whom and when the information was made available. Obviously provision must be made for exceptions in situations where it will not be justifiable to disclose such information.[323] See Principle 8 below.

(ii) Evaluation

4.2.212 It was clear from the response to the discussion papers that there is, in general, support for this principle.[324] It is, for instance, accepted as good practice within the credit information industry that credit grantors' give data subjects 28 days notice prior to transferring default information on that data subject to a credit bureau.

4.2.213 Concern was, however, expressed that disclosing the purposes, the use of the information, the identity and address of the responsible party, and so on, may not be cost-effective. The ultimate question should be how much information must be provided in order to ensure that any consent is properly informed.[325]

4.2.214 In general the submissions indicated that commentators were in favour of a strict

---

322 The Act provides that government and private bodies must publish a manual containing inter alia, a description of the subjects on which information is kept, as well as the categories of records held on each subject.

323 ***Neethling's Law of Personality*** at 279.

324 The Banking Council; SAFPS; Society of Advocates of Kwa-zulu Natal.

325 LOA.

regime. Some felt strongly that the notification of the data subject should not take place ex post facto at all.[326] This will ensure that personal information is not disclosed to a party whom the data subject does not wish to have access. [327]

4.2.215 It was also argued that the exception making provision for steps taken previously need not be repeated, should only be applicable to "same" but not "similar" information'.[328] One commentator[329] argued that "authorisation" for non-compliance should be in writing. This will enable corporate entities to prove that authorisation has actually been given by the owner of the service and not someone else. Another commentator[330] was in favour of the word "authorisation" being replaced with "consent of data subject".

4.2.216 In so far as the exception stating that non-compliance would not prejudice the interests of the data subject is concerned the following comments were received: Only the owner of the information can decide whether it is in his/her interest for non-compliance to take place.[331] The Commission was referred to the example of reverse searching. This is a process whereby a caller to directory enquiries, instead of giving a customer's name or address and receiving a telephone number, gives a telephone number, and then receives a name/address in return. This is incompatible with the purpose for which the information has been collected, but a telecommunications company could consider that its customer will not be prejudiced by its implementation of reverse searching. The possible result will be that the customer becomes the victim of a criminal who now easily obtains the customer's address. It was, therefore, argued that the Bill has to specify that the data subject should provide specific authorisation for the use of his/her information.

---

326 Department of Communications; Sovereign Health.

327 Sovereign Health.

328 Department of Communications.

329 Telkom SA Ltd.

330 Department of Communications.

331 Telkom SA Ltd.

4.2.217 Some commentators[332] argued that the word “interest” where it was provided that the data subject’s interests should not be prejudiced by non-compliance with this principle, was too wide and all encompassing since it was not qualified or defined. They felt that it should be replaced by the words “data subject’s rights”. It was also suggested[333] that the words “reasonably praticable” as a prerequisite for informing the data subject should be deleted.

4.2.218 One commentator[334] contended that the present formulation of the draft Bill entails a more onerous obligation to report the processing of personal information to the Commissioner than to the data subjects themselves. Section 16(2) provides for circumstances in which non-compliance is authorised, including where the non-compliance is not reasonably practicable in the circumstances of the particular case. There is no exemption to the requirement to notify the Commissioner on grounds of practicality

(iii) Recommendation

4.2.219 The Commission confirms its view that responsible parties should comply with the general goals of openness and transparency. This means that, subject to the exceptions mentioned in the Bill, collection of personal information should be done with the knowledge of the data subject, the purpose of the collection should be specified and the information collection policy and individual participation process of the responsible party should be known.

4.2.220 The regulatory mechanism therefore requires the responsible party to :

a) provide basic details of their processing to the Information Protection Regulator which keeps a register; and

b) orient data subjects directly about their information-processing operations

---

332 Vodacom (Pty) Ltd; ESKOM Holdings Ltd.

333 Department of Communications.

334 Foschini’s.

(so-called "awareness principle").

Two kinds of notification can therefore be identified, namely, a notification of general practices of the responsible party and secondly notification on how a responsible party will handle the personal information of a specific data subject.

4.2.221 Principles 3 (purpose specification) and 6 (openness) should therefore be read with Chapter 6 of the Bill which sets out the detail regarding the notification requirements.

4.2.222 It should be noted that the Information Protection Regulator will be appointed to oversee both POPIA and PAIA. Provision has, therefore, been made for notification in terms of both acts to be done simultaneously, should the responsible party so prefer.[335] It is also important to realise that notification will only be given once and not each time personal information is received or processed. See the full discussion on Chapter 6 of the Bill, below.

4.2.223 The Commission recommends that the legislative enactment of Principle 6 should read as follows:

PRINCIPLE 6

Openness

Notification to Regulator and to data subject

17.(1) Personal information may only be processed by a responsible party that has notified the Regulator in terms of Chapter 6 of this Act.

(2) If personal information is collected, the responsible party must take reasonably practicable

335 The advantages of this requirement are that it encourages responsible parties to consider how the Information Protection Principles apply to their activities, it provides the data subject with information and it aids the process of auditing to be carried out by the Regulator. See discussion in ***ALRC Discussion Paper*** at 652.

steps to ensure that the data subject is aware of -

(a) the fact that the information is being collected;

(b) the name and address of the responsible party;

(c) the purpose or purposes for which the information is being collected;

(d) whether or not the supply of the information by that data subject is voluntary or mandatory and the consequences of failure to provide the information;

(e) any particular law authorising or requiring the collection of the information; and

(f) any further information such as -

(i) the recipients or categories of recipients of the information; or

(ii) the nature or categories of the information; or

(iii) the existence of the right of access to and the right to rectify the information collected;

which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

(3) The steps referred to in subsection (2) of this section must be taken -

(a) in the case if the information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in subsection 2(a) to (f); or

(b) in any other case, before the information is collected or as soon as reasonably practicable after the information is collected.

(4) A responsible party that compiles or has compiled a manual and made it available in terms of section 14 or section 51 of the Promotion of Access to Information Act 2 of 2000, does not have to comply with subsection (1) of this section, if all the particulars referred to in section 51 of this Act are contained in the manual.

(5) A responsible party that has previously taken the steps referred to in subsection (2) will comply with subsection (2) in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information is unchanged.

(6) It is not necessary for a responsible party to comply with subsection (2) of this section if -

(a) the data subject has provided consent for the non-compliance;

(b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;

(c) non-compliance is necessary -

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) to enforce of a law imposing a pecuniary penalty;

(iii) to protect of the public revenue;

(iv) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

(v) in the legitimate interests of national security;

(d) compliance would prejudice a lawful purpose of the collection;

(e) compliance is not reasonably practicable in the circumstances of the particular case; or

(f) the information will -

(i) not be used in a form in which the data subject may be identified; or

(ii) be used for statistical or research purposes.

(g) Principle 7: Security safeguards

(i) Proposals in the Discussion Paper

4.2.224 This principle implies that personal information should be protected by appropriate security safeguards against risks such as loss, accidental or intentional unauthorised access or disclosure, interference with, amendment of or destruction of information.[336] Further, these safeguards should be aimed at ensuring that authorised users of the information are able to gain access to and process the information in accordance with their authority.

4.2.225 Information exists in many forms: it can be spoken, written, printed, stored physically and electronically, and transmitted by post or electronically, it can be shown on films and broadcasted in all sorts of multimedia. The bottom line remains that in whatever way, manner or form the information might exist; it has to be protected.[337] However, in many instances appropriate business and legal safeguards have yet to be developed.

4.2.226 The advent of information technology has increased interest in the right to privacy.

---

336 CDT's Guide to Online Privacy; See Bygrave ***Data Protection*** at 67; Roos thesis at 515; Principle 6 of the Discussion Paper reads as follows:

PRINCIPLE 6.
Security safeguards

Security measures to ensure integrity of personal information

17. (1) The responsible party must implement appropriate technical and organisational measures to secure -
(a) the integrity of personal information by safeguarding against the risk of loss of, or damage to, or destruction of personal information; and
(b) against the unauthorised or unlawful access to or processing of personal information.

(2) The responsible party must take measures to -
(a) identify all reasonably foreseeable internal and external threats to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risk identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

337 Cameron O ***Information and Systems Management: Balancing Security and Privacy*** Discussion Document for the Department of Justice and Constitutional Development to Establish Security Requirements and Frameworks 2003 (hereafter referred to as "ISM Discussion Document") at 4.

Computers now support critical infrastructures such as energy, transportation and finance and play a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information.[338] The number and nature of infrastructure access devices have accordingly multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections.[339] Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially and has become more difficult to protect.[340]

4.2.227 The speed and accessibility that create the enormous benefits of the computer age may, if not properly controlled, allow individuals and organisations to eavesdrop inexpensively on, or interfere with, these operations from remote locations for mischievous or malicious purposes,[341] including fraud or sabotage.[342]

4.2.228 As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information

---

338 OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002 (hereafter referred to as "OECD Security Guidelines") at 7.

339 SALC ***Computer-related crime*** Discussion Paper at 3; The potential danger if computers performing these functions are interfered with is very serious.

340 OECD Security Guidelines at 7; United States General Accounting Office (GAO) "Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk" Testimony of Robert F Dacey Director, Information Security Issues before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives GAO-03-303T November 19, 2002 (hereafter referred to as "GAO testimony") at 2; The South African Law Commission ***Computer-related Crime: Preliminary Proposals for Reform in Respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects*** Discussion Paper 99 Project 108 June 2001 (hereafter referred to as "SALC ***Computer-related crime*** Discussion Paper") at 3. This dramatic increase in computer interconnectivity, especially in the use of the Internet, have increased the risks to computer systems.

341 OECD Security Guidelines at 7. Government officials in the United States are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.

342 GAO testimony at 3.

technology, the likelihood increases that information attacks will threaten vital national interests.[343]

4.2.229 In addition, the disgruntled organisation insider is a significant threat. [344] As the number of individuals with computer skills has increased, more intrusion or "hacking" tools[345] have become readily available and relatively easy to use.[346]

4.2.230 There is a multitude of methods by means of which information can be obtained from a computer or its functioning be interfered with. Such methods can include the duplication of information on a computer, the removal of information on a computer, the alteration of information stored on a computer and the alteration of the functioning of a computer.[347]

4.2.231 Security specialists have found it useful to place potential security violations in three

---

343 GAO testimony at 4.

344 A 32 year old Johannesburg man, bearing a grudge against Edgars, was recently found guilty of loading a virus on the computer of the company, an act which the company claims cost it R20 million and affected up to 700 stores. Because the ECT Act was not yet in force the man was charged with malicious damage to property. ***Mail and Guardian Online*** Tuesday May 18, 2004.

345 Examples of hacking incidents:

* 5,4 million card numbers were hacked when the security of a US-based card processing company's computer systems were breached, 139 FNB credit and debit card numbers were potentially compromised, but no clients were defrauded. iafrica.com Monday 24 February 2003" FNB clients safe after mass "hack "attack.
* The Sunday Times (http://www.sundaytimes.co.za/2003/07/20/news/news.asp) on 20 July 2003 reported that a perpetrator used "spyware" - an e-mail message that, when opened, sets itself up to record certain keystrokes on the computer and transmit these to a given address - to gain access to the personal computers of victims. ABSA accounts were breached in this way and thousands of rands stolen.
* The Natal Witness (http://www.witness.co.za/content/2003_07/16987.htm) reported that the African Bank Internet site was hacked into by a hacker known as "7up". He continued to hack into more than 52 South African web sites in less than 18 hours.

346 GAO testimony at 4. This form of crime targets a computer system, generally to acquire information stored on that computer system, to control the target system without authorisation or payment (theft of service) or to alter the integrity of data or interfere with the availability of the computer or server. Many of these violations involve gaining unauthorised access to the target system (ie "hacking" into it). Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the US Department of Justice "The Electronic Frontier : the Challenge.... Use of the Internet" March 9,2002 available at http://www.usdoj.gov/criminal/cybercrime/unla (hereafter referred to as " CCIPS United States Department of Justice "Electronic Frontier") at10.

347 SALC ***Computer-related crime*** Discussion Paper at 4; EPIC (Electronic Privacy Information Center) reports in its EPIC Alert Volume 9.23 dated November 19, 2002 available at http://www.epic.org/alert/EPIC_Alert_9.23.html that a new law in California requires state agencies and businesses that own databases to disclose security breaches involving certain personal information. The Bill comes in response to an April 2002 incident in which the records of over 200,000 state employees were accessed by a computer cracker.

categories:[348]

a) Unauthorised information release: An unauthorised person is able to read and take advantage of information stored in the computer.

b) Unauthorised information modification: An unauthorised person is able to make changes in stored information - a form of sabotage which may also include the destruction of information.

c) Unauthorised denial of use: An intruder can prevent an authorised user from referring to or modifying information.

Generally accepted information security practises usually refer to the categories described above as confidentiality, integrity and availability. The primary aim of information security practise is to provide appropriate safeguards to ensure that the status of information, being confidential, having integrity and being available to authorised persons, is maintained.

4.2.232 In all three instances the release, modification or denial of use occurs contrary to the desire of the person who controls the information, possibly even contrary to the constraints supposedly enforced by the system. The biggest complication may be that the intruder may be an otherwise legitimate user of the computer system.[349]

4.2.233 Practical examples of resources that may be at risk are payments and collections that could be lost or stolen and sensitive information, such as taxpayer information, social security records, medical records, and proprietary business information could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime. Targets also include telephone customer records or consumer credit report information. Critical operations, such as

---

348 Problems experienced by agencies have been identified as follows (See GAO testimony at 5):
- Agencies were not fully aware of the information security risks to their operations.
- They had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable.
- They had a false sense of security because they were relying on ineffective controls.
- They could not make informed judgments as to whether they were spending too little or too much of their resources on security.

349 Saltzer ***Basic Principles of Information Protection*** available at http://web.mit.edu/Saltzer/www/publications/protection/Basic.html as referred to in the GAO testimony at 5.

those supporting national defence and emergency services, could be disrupted.[350]

4.2.234 A hacker may furthermore gain access to a hotel reservation system to steal credit card numbers. Other cases may involve a perpetrator who seeks private information about another individual, whether as a means to an end (eg to extort money or to embarrass the victim through public disclosure), to obtain a commercial advantage, or simply to satisfy personal curiosity. [351] Security solutions, products and services typically seek to prevent the introduction of viruses, eliminate network vulnerabilities, limit access by unauthorised users and authenticate information, messages or users. [352] It is also important to note that recent research shows that there has been a marked shift in the motivation for hacking from those who were simply hacking into systems to show that they could do so to hacking being used as a tool to obtain information for criminal activities.[353]

4.2.235 A recent flood of well publicised information security compromises worldwide relating to personal information has highlighted the emerging legal obligation on companies to establish and maintain adequate information security measures.[354]

4.2.236 Problems regarding the security of information have, however, been acknowledged and addressed worldwide since the early eighties. Both the EU Directive and the OECD Guidelines

---

350 The April 2002 annual report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches. In addition, the number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 73,359 for just the first 9 months of 2002.

351 CCIPS United States Department of Justice "Electronic Frontier" at 10.

352 OECD "Inventory of Privacy Enhancing Technologies (PET's)" Report developed by Hall L in co-operation with the Secretariat of the Working Party on Information Security and Privacy of the Directorate for Science, Technology and Industry of the OECD dated 7 January 2002 (hereafter referred to as "OECD Hall Report") at 17.

353 VeriSign Internet Security Intelligence Brief June 2005.

354 In the UK 24 million personal child benefit records went missing after unencrypted CD's containing the information were put in the post, unregistered and unrecorded, by the HM Revenue and Customs. It has been referred to as a "system failure" in government's handling of sensitive information. See The Telegraph "Minister ignored data security warnings" dated 22 November 2007 accessed at http://www.telegraph.co.uk/. On 22 August 2008 it was reported that the Home Office had lost confidential information on every prisoner in the country and more than 40 000 serious criminals. The information was on a computer memory stick that has gone missing. Robert Winnett "Home Office loses confidential data on all UK prisoners" ***Telegraph*** 22 August 2008.

make provision for security issues.[355]

4.2.237 The principle manifests itself in Principle 5 of The OECD Guidelines.[356] Principle 5 of the OECD Guidelines provides that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. A representative provision is also found in article 7 of the CoE Convention.[357]

4.2.238 The relevant provisions of the EU Directive are a little more detailed. Article 17(1) requires data controllers to implement security measures for ensuring that personal data are protected from accidental and unlawful destruction, alteration or disclosure. The measures taken are to be commensurate with the risks involved in the data processing. A controller must also ensure - by way of contract or other legal act (article 17(3)) that data processors engaged by him/her/it provide "sufficient guarantees in respect of the technical security measures and organisational security measures governing the processing to be carried out (article 17(2)). The latter requirements are supplemented in article 16 which provides : "Any person acting under the authority of the controller or .... processor, including the processor himself, which has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law".[358] Further, the measures taken pursuant to article 17(1) and (3) shall be documented. (article 17(4)).

4.2.239 Specific provision has been made in the Discussion Paper Bill for the protection of

---

355 CDT's Guide; See Bygrave ***Data Protection*** at 67.

356 Principle 5 of the OECD Guidelines reads as follows:

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

357 Art 7 of the CoE Convention reads as follows:

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

358 Bygrave ***Data Protection*** at 68.

information processed by a person acting under authority and information processed by a processor (referred to as an "operator" in the current Bill). [359]

4.2.240 In the Commonwealth Model Law for the public sector the security principle is set out in art 13[360] and in the Model Law for the private sector in art 18.[361]

---

359 Clauses 18 and 19 of the Discussion Paper Bill read as follows:

Information processed by person acting under authority

18. (1) Anyone acting under the authority of the responsible party or the processor, as well as the processor himself, where they have access to personal information, must only process such information with the knowledge or consent of the responsible party, except where otherwise required by law.

(2) The persons referred to under subsection (1), who are not subject to an obligation of confidentiality by virtue of office, profession or legal provision, are required to treat as confidential the personal information which comes to their knowledge, except where the communication of such information is required by law or in the proper performance of their duties.

Security measures regarding information processed by processor

19. (1) Where the responsible party has personal information processed for his, her or its purposes by a processor, the responsible party must ensure that the processor establishes and maintains information security safeguards in accordance with the provisions of subsection 17(2) above.

(2) The carrying out of processing by a processor on behalf of the responsible party must be governed by an agreement in writing or in another equivalent form between the processor and the responsible party, which agreement must include an obligation to establish and maintain security safeguards.

(3) The responsible party must satisfy itself that the processor -
(a) processes the personal information in accordance with section 19(1) and
(b) complies with the obligations incumbent upon the responsible party under section 17.

(4) Where the processor is established in another country , the responsible party must make sure that the processor complies with the laws of that other country, notwithstanding the provisions of subsection (3)(b).

360 **Storage and security of personal information**

13. Where a public authority holds personal information, it shall ensure that -
a) the information is protected, by such security safeguards as is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure, and against other misuse; and
b) where it is necessary for the information to be given to a person, body or agency in connection with the provision of a service to the authority, everything reasonably within the power of the authority is done to prevent unauthorised use or disclosure of the information.

361 **Security of information**

18.(1) An organisation shall take reasonable steps to ensure that personal information in its custody or control is protected against unauthorised use or disclosure and to ensure that the records containing the information are protected against unauthorised copying, modification or destruction.
(2) An organisation is responsible for personal information in its custody or control, including information that has been transferred to a third-party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by the third party.
(3) The question of what protection constitutes compliance with subsection (1) shall be determined in light of all the circumstances, including the sensitivity of the information, the amount of information and the format in which it is stored.

4.2.241 In addition to the existing 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data and the 1997 OECD Guidelines for Cryptography Policy, the OECD governments have drawn up new guidelines entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"[362] to deal specifically with cyber terrorism, computer viruses, hacking and other threats.[363] The Security Guidelines should be read in conjunction with the abovementioned Guidelines.

4.2.242 The Guidelines suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".[364]

4.2.243 They urge all users of information technology, including government, business and individual users, to adhere to and implement basic principles covering such areas as security awareness and responsibility and respect for ethical and democratic values.[365] This 2002 guideline

---

(4) Upon request, the organisation shall make available to any person a general description of the safeguards that it uses to protect personal information and to fulfil its obligations under subsection (1).

362 See fn 338 above.

363 OECD "OECD Governments Launch Drive to Improve Security of Onlline Networks" News release dated August 7, 2002 (hereafter referred to as "OECD news release") at 1.

364 OECD Security Guidelines at 7.

365 OECD news release at 1.These Guidelines aim to:

(a) Promote a culture of security among all participants as a means of protecting information systems and networks.

(b) Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.

(c) Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.

(d) Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.

(e) Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.

(f) Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

built on the security safeguards principle in the earlier 1992 OECD guidelines.

4.2.244 The nine principles are complementary and should be read as a whole. [366]The Principles are as follows:

a) Awareness:[367] Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.[368]

(b) Responsibility: [369] All participants are responsible for the security of information systems and networks. [370]

(c) Response:[371] Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents. [372]

---

366 OECD Security Guidelines at 9.

367 OECD Security Guidelines at 10.

368 Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

369 OECD Security Guidelines at 10.

370 Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

371 OECD Security Guidelines at 10.

372 Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

d) Ethics: [373] Participants should respect the legitimate interests of others. [374]

e) Democracy:[375] The security of information systems and networks should be compatible with essential values of a democratic society.[376]

f) Risk assessment:[377] Participants should conduct risk assessments.[378]

g) Security design and implementation:[379] Participants should incorporate security as an essential element of information systems and networks.[380]

h) Security management: [381] Participants should adopt a comprehensive approach to security management. [382]

---

373 OECD Security Guidelines at 11.

374 Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

375 OECD Security Guidelines at 11.

376 Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

377 OECD Security Guidelines at 11.

378 Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

379 OECD Security Guidelines at 12.

380 Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

381 OECD Security Guidelines at 12.

382 Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit.

i) Reassessment:[383] Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. [384]

4.2.245 The OECD recommends that member countries establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the Guidelines by adopting and promoting a culture of security as set out in the Guidelines.[385]

4.2.246 An example of national legislation incorporating the security principle is Data Protection Principle 7 of the UK Data Protection Act[386] and Principle 5 of the New Zealand Act, which is closely modelled on a principle in the Australian Privacy Act. [387]

Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

383 OECD Security Guidelines at 12.

384 New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

385 OECD Security Guidelines at 15.

386 Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

387 **PRINCIPLE 5**
Storage and security of personal information

An agency that holds personal information shall ensure -
(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against -

i) Loss; and
ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

4.2.247 In practice six major areas of security design and management have been identified.[388] These six areas of general controls are:

(a) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented;

(b) access controls, which ensure that only authorised individuals can read, alter, or delete information;

(c) software development and change controls, which ensure that only authorised software programs are implemented;

(d) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection;

(e) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and

(f) service continuity, which ensures that computer-dependent operations experience no significant disruptions.

4.2.248 The security mechanisms of traditional paper-based communications media - envelopes and locked filing cabinets - are therefore being replaced by technological and organisational measures.

4.2.249 Some examples of security technologies[389] are encryption software, proxies and firewalls. Encryption is a powerful tool that can be used to provide both privacy and security to the individual user. Through the use of encryption, communication and information stored and transmitted by computers can be protected against access and interception to a very high degree. See discussion on the OECD Guidelines for Cryptography Policy which included within them a set of principles above.

4.2.250 The UK Financial Services Authority has stated that it may take enforcement action

---

388 GAO testimony at 10.

389 PETs (Privacy Enhancing Technologies) are technological tools that can assist in safeguarding online privacy. They present a range of characteristics. Some filter “cookies” and other tracking technologies; some allow for “anonymous” web-browsing and e-mail; some provide protection by encrypting data; some focus on allowing privacy and security in e-commerce purchases; and some allow for the advanced, automated management of users’ individual data on their behalf. In essence PETs reinforce transparency and choice, which can lead to greater individual control of data protection.

against firms that fail to encrypt customer data offsite. It is not appropriate for customer data to be taken offsite on laptops or other portable devices which are not encrypted. [390]

4.2.251 Proxy servers and firewalls can also greatly enhance security in a network environment. Both can prevent the disclosure of an individual's IP address or other personal information by acting as an intermediary between a website and an individual computer.[391] Many technologies can be used in many different ways. It is therefore crucial to recognise the context in which any given technology is used. [392]

4.2.252 The USA also emphasise the empowerment of individuals to utilise technology to safeguard their own information. One part of the "empowerment principle" states:

> Individuals should be able to safeguard their own privacy by having ... the opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions.

4.2.253 The empowerment principle also implies that the individuals should be able to safeguard their own privacy by having the opportunity to remain anonymous when appropriate. Anonymity is often the basis of the most effective security safeguard that individuals can adopt.

4.2.254 In Europe, the German law has, furthermore, moved away from a specific tick list, in recognition of a different emerging information processing environment. Some new main aspects on which information protection should focus have been identified[393] and a series of Data-protection-friendly Technologies were recommended with reference to the principles of information

---

390 Financial Crime and Intelligence Division of the UK Financial Services Authority ***Report on Data Security in Financial Services - Firms' Controls to Prevent Data Loss by their Employees and Third-party Suppliers*** April 2008 (hereafter referred to as "***FSA report***") at 6.

391 OECD Hall Report at 16 and 23.

392 OECD Hall Report Introduction at 4.

393 Douwe Korff ***EC Study*** at 160; They are authority (the basis for providing access, eg. a contract); identification and ID verification (to ensure access is only granted to authorised users); access-control; logging; and reporting (on use and access of the system).

minimisation and as-soon-as possible anonymisation.[394]

4.2.255 Two matters of particular relevance were emphasised: the need to start thinking about using technology to ensure information protection rather than regarding information protection as a means to counter technological development (Datenschutz durch Technik); and the fact that the means to ensure information protection and information security clearly increasingly involve the use of biometric information, including sound and image information.[395]

4.2.256 The French data protection authority, too, has long promoted the introduction of privacy-enhancing technologies or PETs and works closely with industry and issues its own guidance, eg. in the field of telematics, on-line access to data, encryption, biometrics, etc. While welcoming such technologies, the authority is however also concerned that companies promoting such PETs offer products that afford real protection. In that respect, it is to be noted that the proposed new law in France allows the authority to express an opinion on the compatability of such products with the law. In effect, this means the CNIL will be able to give such products its support (or to withhold such approbation).[396]

---

394 Douwe Korff ***EC Study*** at 161; These are :
* self-generated pseudonyms;
* pseudonyms for which the key is contained in a separate list;
* one-way pseudonyms;
* hash-keys;
* digital signatures;
* electronic certificates;
* blind digital signatures;
* biometric keys;
* the use of trusted third parties (in several ways); and
* identity protectors.

395 Douwe Korff ***EC Study*** at 161.

396 Douwe Korff ***EC Study*** at 161.
.

4.2.257 In South Africa certain offences were created in sections 85 to 89[397] of the Electronic Communications and Transactions Act [398] to deal with unauthorised access to, interception of or interference with data and with computer-related extortion, fraud and forgery**.** Chapter V of the Act furthermore provides for the registration of cryptography providers.[399] These sections deal mainly with the criminalisation of unauthorised interference with data and may act as a deterrent. They do not however, impose any obligation on organisations to implement any of the principles as set out above in the Guidelines.

(ii) Evaluation

4.2.258 In general, commentators felt that the proposed security safeguards as set out in the draft Bill are well thought through and introduce what they believe to be necessary requirements. The safeguards will, however, change the behaviour of many data collecting organizations and individuals as well as provide Government with a coherent, coordinated set of policies.[400]

4.2.259 There has recently been a string of incidents[401] in the US where consumer data has been lost, stolen or exposed affecting Visa, Bank of America and others. It was reported that US laws are fairly lax in this regard and there is no generally applicable statutory penalty for such carelessness with data, though US consumers use class action law suits. There are no similar actions available to wronged persons, especially individuals, in South Africa, so some statutory penalties for intentionally or even negligently breaching the duty of data privacy should be

397 As set out in Chapter XIII (Cyber crime).

398 Act 25 of 2002.

399 The ECT Act only deals with electronic data and transactions.

400 Law Society of South Africa.

401 See ZDNet (www.zdnet.com).

considered. The proposed mechanisms for dealing with violations of personal privacy are therefore necessary, especially in our country.[402]

4.2.260 The question arises whether security issues have been adequately dealt with in the ECT Act or whether additional provision should be made for the security protection of personal data in accordance with the principles set out above. [403]

4.2.261 Respondents to the Discussion Papers were divided in their answer to this question. Most commentators felt that security issues should form part of the new privacy legislation.[404] Some commentators were of the opinion that security issues have been adequately addressed in other legislation.[405]

4.2.262 What was clear, however, is that there is considerable confusion over the roles and responsibilities for Information and Communications Technology (ICT) in the South African government departments. Currently at least seven public service agencies have a role to play in government ICT issues.[406] (See also the discussion on critical data in Chapter 3).[407]

---

402 Law Society of South Africa.

403 See question 15 in SALRC Issue Paper 24.

404 The Banking Council; ISPA; SABC; LOA; Eskom Legal Department; ENF for Nedbank, Gerhard Loedolff, Eskom. Respondents argued that the ECT Act only applies to data obtained through electronic transactions and does not deal with paper and the voluntary nature of Chapter 8 of the Act is one example of the lack of adequate security measures.

405 Vodacom; SAPS; It was submitted that the cyber crime provisions of the Electronic Communications and Transactions Act 25 of 2002, together with the provisions of the Regulation of Interception of Communications and Provisions of the Communication-Related Information Act which provides for the issuing of a decryption direction to monitor communications that consist of encrypted information as well as the SAPS Act are, for the moment, sufficient to regulate security issues.

406
* The Department of Public Service and Administration (DPSA) which has responsibility for developing ICT policies for the public service as a whole;
* The Public Service Commission (PSC) which has the responsibility of monitoring those policies;
* The National Treasury which has the responsibility of supervising the main transversal systems and managing the Central Computer Services (CCS) (now part of SITA);
* The Department of Trade and Industry (the dti) which has a responsibility for promoting the IT industry;
* The Department of Communications (DoC) which has been given the responsibility to act as secretariat for the development of an ICT strategy for the country with the ultimate responsibility for such a strategy being vested in the Deputy-President's Office (ODP);
* The State Information Technology Agency which has as its objective to provide information technology, information systems and related services in a maintained information systems security environment to, or on behalf of, participating departments and organs of state.

4.2.263 It is of utmost importance that the different departments take the appropriate steps to develop co-ordinated, authoritative policy guidelines as to how the various acts and policies[408] in these departments should be interpreted in order to balance security and privacy requirements. This has become especially pertinent with the expected privacy legislation now on the cards. It has, however, been noted that the National Intelligence Agency is currently revising the Protection of Information Act 84 of 1982 and that the Amendment Bill is currently being discussed in Parliament.

4.2.264 It was furthermore argued that any wording included in the legislation to deal with security measures must be technologically neutral. The wording and requirements in the proposed legislation should take account of the fact that information security can never be absolute. The Bill should provide for information security being commensurate with the risk attendant on the compromise of the information.[409]

4.2.265 The Commission was, however, cautioned that the Privacy Act will not be able to deal with the practical aspects of security issues.[410] For instance, identity theft has become a 'hot topic' as far as financial institutions are concerned. [411]This was highlighted in recent reported cases of

---

* The Department of Arts, Culture, Science and Technology which has been charged with developing the technoloy foresight study of ICT in South Africa.

* The Auditor General which has been charged to ensure compliance and certification of these policies and framework.

407 ISM Discussion Document at 2.

408 See Public Service Act, 1994; Electronic Communications and Transactions Act 25 of 2002; Electronic Communications Security Pty (COMSEC) Act 68 of 2002; National Archives of South Africa Act 43 of 1996; Minimum Information Security Standards (MISS); State Information Technology Agency Act 88 of 1998; Protection of Information Act 84 of 1982; Promotion of Access to Information Act 2 of 2000; Information Security Framework and ISO 17799/BS7799.

409 Nedbank.

410 What must be guarded against is information security being glossed over in the legislation. It underpins the jurisprudence which has developed around privacy law and, on the current thinking of the draft legislation, will allow industry sectors to provide codes of conduct which address specific practices desirable or necessary in a particular profession or industry.

411 SAFPS supports this statement as also the notes and footnotes to paras 4.2.174-179 in the Issue Paper and maintains its position regarding the problems surrounding identity theft, which is increasing at an alarming rate both worldwide and in South Africa. The SAFPS filings with regard to identity theft and Impersonation show a marked increase in rand value terms from R5 448 239 in 2004 to R12 646 434 in 2005.

unauthorised electronic transactions.[412] It is also clear that no statute or statutes can entirely control identity theft or plain poor control of databases since better management of these issues also require educated participation by all in the process.[413]

4.2.266 Identity theft happens within a 'paper' environment (over the counter transactions/applications etc.) and within an electronic environment (internet banking).[414] The methods may differ but the results are the same. The banking industry indicated that it is committed to take utmost care in both environments and as such adequate information protection is paramount to the industry.[415][416]

4.2.267 In the South African environment, the country is furthermore plagued with an outdated and inefficient identity document which is easily forged or altered and which has resulted in large numbers of impersonations and identity theft taking place. There is reportedly also elements of corruption within the Department of Home Affairs and taking all these issues into consideration it is submitted that it will be many years before the new identity card system becomes fully effective in South Africa. This behoves the legislature to take steps to combat the problems of identity theft.

---

412 The Banking Council.

413 Law Society of South Africa.

414 There is international recognition that identity theft has become a serious issue with the USA reporting fraud through identity theft in excess of US $ 53 billion during 2003 and the United Kingdom indicating increases of 77% during the same period. The USA has recently enacted the Fair and Accurate Credit Transactions Act of 2003 which provides consumers with identity theft protection. Australia is experiencing massive problems with the influx of immigrants from Asian countries, many of whom have only one name and no official means of identity.

415 One of the ways banks try to prevent identity theft, and/or limit the consequences thereof, is by using the services of the South African Fraud Prevention Services (SAFPS). Where banks become aware of possible identity theft, they load the details against the principal's name on the SAFPS database. This may subsequently cause complications should the genuine principal seek to borrow from a credit grantor where the latter performs a check at the SAFPS database. That is, an alert would be sent back to the credit grantor that would cause inconvenience and possible embarrassment to the (genuine) principal. However, there is no alternative to such loading of "identity fraud" against the principal's name. In defence of the practice, it protects the principal. The (genuine) principal should not be allowed to take legal action against the member of the SAFPS that loaded the identity fraud warning."

416 The SAFPS provides a world first free public service to South African citizens who have had their identity documents lost or stolen or who can prove that they have been impersonated. The service is available on the SAFPS website (www.safps.org.za) or by a fax on demand service.

It must be remembered that such theft does not occur simply through electronic transactions on the Internet but also in normal business and credit application transactions.[417]

4.2.268 However, the most that privacy legislation can do is to impose a duty on responsible parties to exercise sufficient measures to secure the information (as a reasonable person would to secure assets). Identity theft is a crime as well as a delict (wrongful infringement of identity)[418] that is perpetuated technologically and should therefore be dealt with according to the criminal laws of the country. [419]

4.2.269 Reference was furthermore made in one submission to the question whether, in the absence of an undertaking or intention, a negligent disclosure of private information[420] would give rise to liability.[421] The conclusion was that the general delictual remedies do not apply[422] and it was

---

417 SAFPS.
.

418 ***Neethling's Law of Personality*** 258.

419 Liberty Group Ltd; LOA.

420 During July 2001 an on-line financial service provider in South Africa accidentally e-mailed the private financial statements of a number of customers to other subscribers. At least one of the affected customers threatened to sue. The financial service provider maintained that there was no legal basis on which it could be held liable, but the matter was subsequently settled. "Close shave for icanonline" Basheera Khan, ITWeb, 23 July 2001, http://www.itweb.co.za. In several other incidents financial service providers have unintentionally disclosed confidential information of their customers . A South African financial service provider addressed an e-mail to a large number of customers in such a way that the addresses of the several hundred other customers were made available to each customer, see 'FNB reveals clients' e-mail addresses, P Vecchiatto, ITWeb, 25 March 2003, http://www.itweb.co.za/sections/internet/2003/
"Credit bureau Experian accidentally made available on its web site the records on 1.5 million clients in July 1999" "Fears that Website Listed Confidential Bank Data," Africa News, July 12, 1999. First National Bank's (FNB) telephone banking service allowed callers to obtain a balance statement and available credit level for the accounts of any client "FNB Allows Access to Account Balance Data," Business Day, February 21, 2000, who considered this to be a breach of their privacy. While these incidents were reported widely in the press none gave rise to litigation. While there is no case law, it is the very absence of litigation that raises important questions about the protection of privacy.

421 Andrew Rens Wits Law School.

422 See however Petzer N "Opinion: Who Should Carry the Internet Banking Can?" in **De Rebus** November 2003 accessed on 2003/11/01 at http://www.derebus.org.za/current/letters/InternetBanking.htm.

argued that a case exists for development of the common law or a constitutional claim for damages action.[423]

4.2.270 In this regard, it is worth considering the number of laptop computers, PDAs, smart phones, flash memory devices and other digital data holders that often have unprotected and extremely personal information about persons other than the erstwhile owner of the device stored on them and are then stolen or mislaid. Insecure e-mail, instant messaging , SMS and other data communication channels would also need to be dealt with accordingly. Whilst the securing of certain data in such devices and communication channels may be outside the purview of the proposed Bill, stronger control of personal data with some specific penalties for negligent handling of it should concentrate minds on data security, especially on mobile devices. [424]

423 Andrew Rens Wits Law School.

424 Law Society of South Africa.

4.2.271 In so far as notification of security compromises are concerned two options were proposed in the Discussion Paper.[425] Commentators did not agree on this point. One group[426] supported option 1 whereas the other group[427] was in favour of option 2.

---

425 The two options set out in the Discussion Paper read as follows:

Notification of security compromises

Option 1:

20 (1) Where any compromise of information security safeguards has, or may reasonably be believed to have resulted in the personal information of any person being accessed or acquired by an unauthorised person, the responsible party, or any third party processing personal information under the authority of a responsible party, must notify -

(a) the Commission as soon as reasonably possible after the discovery of the compromise; and
(b) the person whose information has been compromised, where the identity of such a person can be established.

(2) The responsible party must make the notification in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the compromise and to restore the reasonable integrity of the responsible party's information system.

(3) The responsible party may only delay notification if the South African Police Services or the Commission determine that notification will impede a criminal investigation.

(4) The responsible party must notify a person whose personal information has been compromised by written notification -

(a) mailed to that person at the person's last known physical address; or
(b) by email addressed to the person's last known eMail address; or
(c) by prominently posting details of the compromise on its website; or
(d) by publication in the news media; or
(e) as may be directed by the Commission.

(5) A notification must provide such information as may be relevant to allow the person to protect himself or herself against the potential consequences of the compromise, including where possible, the identity of the unauthorised person(s) who may have accessed or acquired the personal information.

(6) The Commission may direct a responsible party to publicise, in a manner directed by the Commission, the fact of any compromise to the integrity or confidentiality of personal information, if the Commission has reasonable grounds to believe that such publicity would protect any person who may be affected by the compromise.

Should this option be incorporated in the legislation the following clause will have to be inserted in clause 39 (duties of Commission) :

(aa) To require the responsible party to disclose to any person affected by a compromise to the confidentiality or integrity of personal information, this fact in accordance with section 20 of this Act.]

Option 2

20. The responsible party must take all reasonable steps to ensure that where -

(a) an information security compromise of personal information held by the responsible party or under the authority of a responsible party has taken place; and
(b) the identity of a person affected by the compromise can be established,

such a person is notified of the compromise or suspected compromise and provided with such information as may be relevant to allow the person to protect himself or herself against the potential consequences of the compromise.

426 Provincial Administration Western Cape; Law Society of South Africa; Mark Heyink.

427 Land and Agricultural Development Bank; Department of Communications; Vodacom; SNO Telecommunications (Pty) Ltd); Board of Health Care Funders; Foschini's; Banking Association; Nedbank; SAIA.

4.2.272 Supporters of option 1 argued that security compromises must always be made known to those affected, as well as to the Information Protection Regulator. In this regard, option 1 was preferred as set out in the discussion document. It was suggested that SMS notification of any breach should be included as an option since cellular phones are more or less ubiquitous and this would be a cheap and generally effective method of notification.[428]

4.2.273 Supporters of option 2 argued that it is a simpler, more effective option,[429] legally sufficient in their view, and in line with international precedent.[430] Notification is too costly and not always possible or necessary given the balance of harm.[431] Option 2 is also more optional, quick and does not place onerous requirements on companies.[432] Sectors and industries are inherently different and option 2 would allow the adoption by each entity, sector or industry to deal with security compromises relating to them. It would furthermore ensure that there is flexibility and tailor-made industry or sector specific standards dealing with security compromises through the formulation and adoption of specific industry codes of conduct on these issues as contemplated in terms of clause 54 of the Discussion Paper Bill.[433] Option 1 entails a significantly more interventionist role to be played by the Commission and it is respectfully submitted that where less extreme restrictions are available to the legislature that will achieve the same purpose, the less extreme provision should be preferred.[434]

4.2.274 A third option, that was suggested, was that the publication of the breach will occur only under limited circumstances.[435] Under this construction of the section, publication can only be

---

428 Law Society of South Africa.

429 Banking Association; SNO Telecommunications Ltd; Nedbank.

430 SNO Telecommunications (Pty) Ltd.

431 CAPES.

432 Land and Agricultural Development Bank.

433 Vodacom.

434 Foschini's/DMA/SOCCAM.

435 Banking Association.

ordered where the responsible party cannot to the satisfaction of the Commission contain or limit the effects of the breach. This would arise in a situation where the responsible party does not know which personal information in its possession has been breached. Arguably speaking, in these circumstances the only manner to remedy the situation would be to publicise the details of the breach.[436]

4.2.275 In general it was furthermore submitted that -

* clause 19(4) of the Discussion Paper Bill should only be applicable in relation to laws relevant to data protection.[437]

* the nature of the compromise rather than the details should be posted in terms of clause 20(4)(c) of the Discussion Paper Bill, since posting of the details of the compromise will destroy the privacy of the data subject.[438] The current wording in subsection (c) may be interpreted to mean that details of the compromise, including the personal information that may have been compromised, be published.[439] While this cannot be the intention, it was argued that the current wording of subsection (c) is open to such interpretation and that it should be amended to read as follows: “on its website that a compromise has taken place”.[440]

* Principle 6 should be qualified in clause 17(1) of the Discussion Paper Bill with reference to what is technically and financially reasonable in the circumstances, given the business of the responsible party, the type of information sought, and the purpose of the information. It is a well-known commercial risk that technology is increasingly the victim of fraud, hacking, manipulation and interception. Legal protection already exists

436 Nedbank.

437 Department of Communications.

438 Department of Communications.

439 Board of Healthcare Funders.

440 Sovereign Health.

in relation to unsolicited marketing in section 45 of the ECT Act[441], and unlawful interception in section 2 of the RICA.[442] It was submitted [443] that the context within which the word *"appropriate"* has been used in sections 17(1) and 17(2)(b) of the Discussion Paper BIlll indicates that the appropriateness of a safeguard could only be determined with regard to the nature and severity of the risk posed. Different levels of security are therefore envisaged for different categories of risk. A weighing up of factors including the nature and severity of the risk and the costs of implementing different types of security technologies to mitigate against the risk is a reasonable exercise for any responsible party to undertake with regard to implementing appropriate technical and organisational measures to ensure the integrity of personal information.

* All safety or security measures must, of necessity, represent a balance between the costs, the risks of certain events occurring, the impact or severity of such events, and practical operating considerations. Certain failures are therefore to be mitigated or tolerated in the application of the balance. Clause 17 of the Discussion paper Bill, however, could be interpreted in an absolute sense, as a "zero breach or failure". It is recommended that clause 17 be amended to provide that the various safety or security measures be implemented on an appropriate risk-based approach, given the circumstances of the responsible party.[444] The relevant standards should therefore take into account both the size and nature of the business in question, together with the use to which the data is being put, as well as the likely threat to breaches in personal information which is likely to occur. Again, from a bank's perspective, such requirements need to cater for a certain amount of flexibility, particularly at the outset of the implementation of the Bill, as it may require

441 Section 45 of the ECT Act addresses unsolicited goods, services or communications and imposes an obligation on "a*ny person who sends unsolicited commercial communication to consumers*" to provide the consumer with the option to cancel his or her subscription to the mailing list of that person and supply the particulars of the source from whom the person obtained the consumer's personal information, on request. Section 45 (2) provides further that no agreement will be concluded where a consumer fails to respond to an unsolicited communication. Continuing to send unsolicited communication to a person who has advised that such communications are not welcome, is liable to conviction of an offence and certain penalties.

442 SNO Telecommunications (Pty) Ltd.

443 Foschini's/DMA/SOCCAM.

444 Banking Association.

organisations such as the bank to potentially have to upgrade their database and security systems in order to meet the requirements of the Bill. A reasonable grace period to allow for compliance is strongly suggested. When deciding on an appropriate period of time, the Commission should take cognisance of the fact that the overhaul, upgrading or modification of information systems cannot be effected in a very short period of time and require considerable planning.[445]

* Clause 19(4) of the Discussion Paper Bill imposes potentially unenforceable obligations on responsible parties to ensure that processors in other countries comply with the laws of the *other* country. Since the purpose of harmonising data protection principles under an umbrella standard is to ensure that international trade can take place on similar terms and conditions, it is possible that this principle will become less of an issue in practise, but there is a concern that the SALRC might be suggesting that businesses situated in South Africa would have an obligation to enforce the laws of other countries against their trading partners. [446] The wording in clause 19(4) should be clarified to refer to "applicable data protection" to be inserted before "laws of that other country…." It is the bank's view that this is too onerous in that the responsible party is required to ensure that the processor, established in another country, complies with all laws of that country. This implies that the responsible party must ensure that the processor complies with all laws of the country where it is established. This is probably unintended as it would place a huge burden on the responsible party, which burden limits the benefits of the outsourcing agreement significantly.[447]

* A provision should be included which requires the responsible party to inform the Commission in advance, and on an ongoing basis, of the measures taken to

---

445 Nedbank.

446 SNO Telecommunications (Pty) Ltd.

447 Nedbank.

preserve security.[448] Such a report will aid the Commission in the fulfilment of its duty of monitoring compliance with the Act, pursuant to clause 39(1)(b) of the Bill.

* It was noted[449] that the international standards organisation technical committee on health informatics standards (ISO/TC 215) has a working group on health information security. One of the work items is aimed at developing a standard ISO 27799 (information security in health). The more general information security standard, ISO 17799, which includes provisions for ensuring data privacy from an information system perspective, is already in use in SA.[450]

* The fields of electronic security (including authentication), on the one hand, and privacy, on the other, are approaching each other closely. For this reason it seems a pity that one of the most important ways of stratifying data semantically, namely by means of XML (Xtended Markup Language) seems not to have been dealt with. Biometrics is, of course, another modern field where privacy and authentication considerations overlap. Another omission seems to be the question of privacy in the mobile environment (cellular telephony). Information in this format is much more "inter-active" than its computer equivalent. Would the same privacy considerations apply to an SMS-message as to its e-mail or paper counterparts, for instance? The so-called "3G" (third generation) of cell phone technology makes it possible to have interactive video conversations, to show one's partner in such a conversation video recordings of one's immediate surroundings etc. These capabilities may have a considerable effect on privacy.[451]

(iii) Recommendation

---

448 Society of Advocates of Kwazulu-Natal.

449 SABS.

450 SA Medical Research Council.

451 Prof Dana Van der Merwe.

4.2.276 The Commission agrees with Richard Thomas, the UK Information Commissioner, where he says that getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of customer trust and confidence.[452] Many firms are failing to identify the data risk they face for three main reasons: they do not appreciate the gravity of the risk; some do not have the expertise to make an assessment of the key risk factors and to devise ways of mitigating them and thirdly, some fail to devote or coordinate adequate resources to address the risk.[453] Poor data security is currently a serious widespread and high-impact risk to the objective to reduce financial crime. [454]

4.2.277 In addressing these problems the Commission has noted and incorporated the following trends in their considerations:[455]

(a) An increasing recognition that information security is a legal obligation;

(b) An emerging legal standard against which information security compliance will be measured; and

(c) A new emphasis on a duty to disclose breaches of information security.

4.2.278 Thus, rather than telling companies what specific security measures they must implement, the Bill requires companies to engage in an ongoing and repetitive process that is designed to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented and ensure that they are continually updated in response to new developments. In most cases it does not require use of any specific security measures, instead leaving the decision up to the company. Key to the new legal standard is a requirement that security be responsive to the companies fact

---

452 Foreward by UK Information Commissioner to the ***Financial Services Authority Report.***

453 ***Financial Services Authority report*** at 7.

454 ***Financial Services Authority report*** at 9.

455 Smedinghoff T "Trends In The Law of Information Security" ***BNA. International World Data Protection Report*** August 2004.

specific risk assessment.[456]

4.2.279 Furthermore, the most significant legal obligation raised by the recent series of security breaches, is the duty to notify persons who may be affected by the breach (eg. persons whose personal information has been disclosed). The Bill therefore seeks to impose on companies an obligation similar to the common law "duty to warn" of dangers. Provisions requiring disclosure of security compromises, particularly in cases where personal information has been compromised, have therefore been incorporated in the Bill.

4.2.280 Provision has also been made for an obligation on responsible parties to ensure, by way of contract or other legal act, that operators or persons acting under the authority of the responsible party establishes and maintains adequate security measures.

---

456 It is significant that the King Committee on Corporate Governance ***King Report on Corporate Governance for South Africa*** 2002 specifically addresses the issue of risk management in its "Code of Corporate Practices and Conduct" . In paragraph 3 of the Code it is stated as follows:

"3.1.1 The board is responsible for the total process of risk management, as well as forming its own opinion on the effectiveness of the process. Management is accountable to the board for designing, implementing and monitoring the process of risk management and integrating it into the day to day activities of the company. . . .

3.1.5 The board is responsible for ensuring that a systematic documented assessment of the processes and outcomes surrounding key issues is undertaken, at least annually, for the purpose of making its public statement on risk management. It should, at appropriately considered intervals, receive and revue reports on the risk management process in the company. This risk assessment should address the company's exposure to at least the following:

* Physical and operational risks;
* Human resource risks;
* Technology risks;
* Business continuity and disaster recovery;
* Credit and market risks; and
* Compliance risks . .

3.1.6 Risk management and internal controls should be practised throughout the company by all staff, and should be embedded in the day to day activities."

4.2.281 Finally, the Commission is in full support of the use of new technologies that enhance the security of personal information, especially in so far as it promotes the principles of minimality and anonymisation or de-identification.[457]

4.2.282 The Commission recommends that the legislative enactment of Principle 7 should read as follows:

PRINCIPLE 7

Security safeguards

Security measures to ensure integrity of personal information

18.(1) A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent -

(a) loss of, or damage to, or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1) the responsible party must take reasonable measures to -

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risk identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

---

457 See discussion on these principles above.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Information processed by operator or person acting under authority

19.(1) An operator or anyone processing personal information on behalf of a responsible party or an operator, must -

(a) process such information only with the knowledge or authorisation of the responsible party, unless otherwise required by law; and

(b) treat personal information which comes to their knowledge as confidential and must not disclose it unless required by law or in the course of the proper performance of their duties.

Security measures regarding information processed by operator

20.(1) A responsible party must ensure that an operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 18 above.

(2) The processing of personal information for a responsible party by an operator on behalf of the responsible party must be governed by a written contract between the operator and the responsible party, which requires the operator to establish and maintain confidentiality and security measures to ensure the integrity of the personal information.

(3) If the operator is not domiciled in the Republic, the responsible party must take reasonably practicable steps to ensure that the operator complies with the laws, if any, relating to the protection of personal information of the territory in which the operator is domiciled .

Notification of security compromises

21.(1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party, or any third party processing personal information under the authority of a responsible party, must notify -

(a) the Regulator; and

(b) the data subject, unless the identity of such a data subject cannot be established.

(2) The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

(3) The responsible party may only delay notification if the South African Police Services, the National Intelligence Agency or the Regulator determine that notification will impede a criminal investigation.

(4) The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways -

(a) mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

(5) A notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including if known

to the responsible party, the identity of the unauthorised person(s) who may have accessed or acquired the personal information.

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

(h) Principle 8: Data subject participation

(i) Proposals in the Discussion Paper

4.2.283 This principle provides that persons should be able to participate in, and have a measure of influence over, the processing by other individuals or organisations of personal information which relates to them.[458] The expectation is that individuals themselves can do much to mitigate any problems arising from the wrong people using the wrong information for the wrong purposes.[459]

4.2.284 Information protection instruments rarely contain one special rule expressing this principle in the manner formulated above. Rather, the principle manifests itself more obliquely through a combination of several categories of rules. First there are rules which aim at making people aware of information processing activities generally. (See above: openness)

4.2.285 There are furthermore rules which grant persons the right to gain access to personal

458 See discussion in Roos thesis at 497.

459 Roos 1998 ***THRHR*** at 504 and references made therein.

information relating to them and kept by other persons and organisations. [460] This right is known as "the right to access". Most, if not all, information protection instruments make provision for such a right. An influential formulation of the right is given in Article 12 of the EU Directive.[461] Principle 7 of the OECD Guidelines[462] also deals with individual participation.

---

460 Clause 21 of Principle 7 of the Discussion Paper reads as follows:

PRINCIPLE 7
Individual participation

Access to personal information

21. (1) Where a responsible party holds personal information, the data subject is entitled to-
(a) obtain from the responsible party, free of charge, confirmation of whether or not the responsible party holds personal information about him or her; and
(b) have communicated to him or her, after having provided adequate proof of identity, the particulars of the personal information held, including information as to the identity of all persons who have had access to his, her or its personal record -
i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner;
iv) in a form that is generally understandable.

(2) Where, in accordance with subsection (1)(b) of this section, personal information is communicated to a data subject, the data subject must be advised that, under principle 7, the data subject may request the correction of information.

461 Article 12 of the EU Directive reads as follows:

Right of access

Member states shall guarantee every data subject the right to obtain from the controller:
(a) without constraint at reasonable intervals and without excessive delay or expense:
*confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed .
*communication to him in an intelligible form of the data undergoing processing and of any available information as to their source
*knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1) .
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

462 Principle 7 of the OECD Guidelines reads as follows:

Individual Participation Principle

An individual should have the right -

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

(i) within a reasonable time;

(ii) at a charge, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is readily intelligible to him;

4.2.286 The right in Article 12 of the EU Directive is similar to, but also more extensive than, the equivalent rights found in the other main international information protection instruments. See Art 8 of the CoE Convention[463] and Principle 4 of the UN Guidelines. Only the UN Guidelines, specifically mentions the right to be informed of the recipients of data.

4.2.287 In New Zealand this principle is set out in Principle 6.[464] This right to access is subject to many exemptions, but this is not unusual when one compares it to legislation in other jurisdictions. It remains to be seen whether in practice these exemptions will result in the right of access being unduly curtailed.[465]

---

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

463 Art 8 of the CoE Convention states as follows:

Additional safeguards for the data subject

Any person shall be enabled:
a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him or such data in an intelligible form;
c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;
d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs (b) and (c) of this article is not complied with.

464 **PRINCIPLE 6**

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled -

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and
(b) To have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts IV and V of this Act.

465 Roos 1998 ***THRHR*** at 504.

4.2.288 With respect to rectification rights, most information protection instruments have provisions which give persons the right to demand that incorrect, misleading, irrelevant or obsolescent information relating to them be rectified or deleted by those in control of the information.[466]

4.2.289 In this regard, the individual must have the power to procure a correction of misleading or incomplete information, or the deletion of information which are false or obsolete, or information obtained in an unlawful manner, or information not reasonably connected with (or relevant to) or necessary for the specified purpose. This right is essential for preventing or terminating an infringement of the individual's personality interests.[467]

4.2.290 In the Commonwealth Model Law for the public sector the principle manifested in section 15[468] and in New Zealand this principle is set out in Principle 7[469]

---

466 Clause 22 of Principle 8 of the Discussion Paper Bill reads as follows:

Correction of personal information

22.(1) Where a responsible party holds personal information, the data subject is entitled to -
(a) request correction of the information; or
(b) request that there be attached to the information a statement of the correction sought but not made.

(2) A responsible party that holds personal information must, if so requested by the data subject or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where a responsible party that holds personal information is not willing to correct that information in accordance with a request by the data subject, the responsible party must, if so requested by the data subject, take such steps (if any) as are reasonably practicable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by the data subject of the correction sought.

(4) Where the responsible party has taken steps under subsection (2) or subsection (3) of this section, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of these steps.

(5) Where a responsible party receives a request made pursuant to subsection (1) of this section, the responsible party must inform the data subject of the action taken as a result of the request.

467 These powers are recognised to a greater or lesser extent by all foreign legislation dealing with data protection (***see Neethling's Law of Personality*** at 279; Neethling ***Huldigingsbundel WA Joubert*** at 124 fn 128).

468 **Correction of personal information**

15. (1) Where a document of a public authority to which access has been given under any enactment, contains personal information of a person and that person claims that the information–
(a) is incomplete, incorrect or misleading; or
(b) not relevant to the purpose for which the document is held, the public authority may, subject to subsection (2), on the application of that person, amend the information upon being satisfied of the claim.

(2) An application under subsection (1) shall –
(a) be in writing; and

4.2.291 From the foregoing it appears that a person must be given active control over his own information records if he is to be properly protected by law. This is therefore one of the important information protection principles.

4.2.292 In South Africa the right of access to information held by the state and private bodies is specifically provided for in the Constitution. [470] This includes information that is specifically about

---

(b) as far as practicable, specify:
(i) the document or official document containing the record of personal information that is claimed to require amendment;
(ii) the information that is claimed to be incomplete, incorrect or misleading;
(iii) whether the information is claimed to be incomplete, incorrect or misleading;
(iv) the applicant's reasons for so claiming; and
(v) the amendment requested by the applicant.

(3) To the extent that it is practicable to do so, the public authority shall, when making any amendment under this section to personal information in a document, ensure that it does not obliterate the text of the document as it existed prior to the amendment.

(4) Where a public authority is not satisfied with the reasons for an application under subsection (1), it may refuse to make any amendment to the information and inform the applicant of its refusal together with its reasons for so doing.

469 **PRINCIPLE 7**

Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled -

(a) To request correction of the information; and
(b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

470 Section 32 of the Constitution provides as follows:
Access to information
32. (1) Everyone has the right of access to -
(a) any information held by the state; and
(b) any information that is held by another person and that is required for the exercise or protection of any rights.

(2) National legislation must be enacted to give effect to this right and may provide for reasonable measures to alleviate

someone and, more generally, the information the state uses to make decisions affecting someone.[471]

4.2.293 This provision therefore also enables a data subject to gain access to his or her personal information. In this aspect the provision is therefore a duplication of the privacy principle discussed above. However, it should be noted that privacy legislation does not deal with the right to access to information other than personal information (general information) or to the right to access of personal information of a third person.

4.2.294 The Promotion of Access to Information Act (PAIA) which was enacted to give effect to section 32(2) of the Constitution, provides that the responsible party must, on the data subject's request, allow the data subject reasonable access to his or her information records. This power (or entitlement) of access[472] is necessary for effective and equitable control of information,[473] for only thus will such a person be able to ascertain whether the information is correct, necessary for the purposes of processing, necessary for the protection of a legitimate interest, etcetera.[474] Of course, there may be exceptions to the right of access to information in particular circumstances.[475]

4.2.295 Detailed provision was furthermore made for the correction of information in clauses 51,

---

the administrative and financial burden on the state.

471 De Waal et al ***Bill of Rights Handbook*** at 526.

472 See section 11 (public bodies) and 50 (private bodies) for the right of access to records. The procedure is set out in section 18 and further (public bodies) and 53 (private bodies).

473 This power is recognised in all foreign statutes dealing with data protection. See also De Klerk A "The Right of a Patient to have Access to his Medical Records" 1991 ***SALJ*** 166-170.

474 It should, however, be made clear that PAIA is not to be regarded as a data protection or privacy statute. Klaaren J & Penfold G "Access to Information" in Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D & Woolman S (eds) ***Constitutional Law of South Africa*** 2ed Juta Kenwyn 2002 (hereafter referred to as "Klaaren in Chaskalson et al") at 62-9 states that data protection legislation performs three functions: it prevents unauthorised disclosure and use of private information; it allows for the correction of personal information held by another body; and it allows for access to one's own information. The focus of such legislation is on the protection of privacy and not on access to information. It does, however, contain certain elements of data protection legislation in that it allows for personal requesters to obtain access to information. It also makes provision for the correction of personal data in section 88.

475 ***Neethling's Law of Personality*** at 279 and the references made therein.

52 and 53 of the original Open Democracy Bill, but only section 88 of PAIA survived. [476] However, section 88 of PAIA does not deal with correction sufficiently and therefore it should be dealt with comprehensively in information protection legislation. This means that individuals should have a right to view all information that is collected about them and they must be able to correct certain information. [477]

4.2.296 Privacy is sometimes set up in opposition to access to information. However, in order to give effect to a person's right to privacy such a person needs access to his or her personal information that is being kept by a responsible party. Eiselen emphasises that it is through this right of access to the information that the data subject gains a measure of control over the information.[478] At this level the right of access to information and the right to privacy is therefore not in conflict.[479]

4.2.297 Both privacy and access to information are therefore aspects of individuals' freedom in tension with the power of the state, and increasingly the power of corporations.[480] Where access is sought to the personal information of a third party the two rights may come into opposition. This aspect is, however, not dealt with in the privacy legislation.

---

476 **Correction of personal information**

88. If no provision for the correction of personal information in a record of a public or private body exists, that public or private body must take reasonable steps to establish adequate and appropriate internal measures providing for such correction until legislation providing for such correction takes effect.

Accessing of personal data for the purpose of checking it is obviously dealt with in the Act, although not specifically (Sections 11 and 50).

477 CDT's Guide.

478 Reference to Eiselen in Roos thesis at 659.

479 This particular section of the privacy legislation can in fact be seen as giving effect to section 32(2) of the Constitution.

480 Andrew Rens; Piller***, Macworld*** at 6 refers to Marc Rotenberg, Director of Computer Professionals for Social Responsibility, Washington DC who, however, warns against believing arguments that access and privacy rights are inherently incompatible. He argues that such conflicts are often promoted by those who stand to profit by expanding access to private data.in its "Code of Corporate Practices and Conduct" Freedom of information and privacy/data protection should rather be seen as different, but complementary aspects making up the "wholeness" of human rights. See Tang R "Data Protection, Freedom of Expression and Freedom of Information - Conflicting Principles or Complimentary Rights?" Paper delivered at the 24th International Conference of Data Protection and Privacy Commissioners held in Cardiff on 9-11 Sept 2002.

4.2.298 In this regard it is interesting to note the position in the United Kingdom regarding the relationship between the UK Data Protection Act 1998 and the UK Freedom of Information Act 2000.

4.2.299 The Data Protection Act is built around a set of enforceable principles. These are intended to protect personal privacy, to encourage good practice in the handling of personal information and to give individuals a right of access to information about themselves, for example to their own health or financial records.

4.2.300 The Freedom of Information Act 2000[481] gives a person a general right of access to all recorded information held by or on behalf of public authorities. It is intended to promote a culture of openness and accountability amongst public sector bodies.

4.2.301 However, if the personal information requested is about the person requesting the information then there is no "right to know" under the Freedom of Information Act (FOIA). There is, in other words, an absolute exemption.[482] Such requests automatically become subject access requests under the Data Protection Act and must be treated as such.[483] That means that despite the exception under the FOIA, the applicant has a right to his or her information under the Data Protection Act.

4.2.302 If the personal information requested is about someone other than the applicant, there is an exemption (which permits the withholding of information) if disclosure would breach any of the Information Protection Principles. The term "third party information" is used to describe personal information about someone other than the applicant. When an applicant asks for third party information, that request can only be refused if disclosure would breach any of the information protection principles. The first principle requires personal information to be processed fairly and lawfully. In practice this will be the key issue when considering an application for third party information. The system set out in the Data Protection Act has therefore been incorporated in the FOIA.

---

481 The Freedom of Information Act came into operation on January 1, 2005.

482 Section 40 of the Freedom of Information Act 2000.

483 Information Commissioner ***Freedom of Information Act Awareness Guidance No 1.***

4.2.303 Both Acts are administered by the Information Commissioner. It is proposed that a similar provision should be made in South Africa.

(ii) Evaluation

General

4.2.304 Submissions from commentators overwhelmingly supported the introduction of the individual participation principles in the privacy legislation.[484] It was noted that sections 21 and 22 of the Discussion Paper Bill encompass very important issues and should suitably reduce the unnecessary power of credit bureaux, credit granting organizations and others which hold information about any individual without unduly affecting the business value of the information generally held by such organisations. They also accord with the principles of access to information contained in our Promotion of Access to Information Act and generally represent a desirable degree of empowerment of individuals in South Africa.[485]

4.2.305 There was, however, some support for the idea that access to information should be dealt with under PAIA only.[486]

4.2.306 On the other hand, however, it was argued that PAIA is not sufficient in this regard in that -

* PAIA does not address correction adequately. It only requires that some method for correction should be put in place.
* It does not constrain a party from revealing private information provided the revelation

---

484 The Banking Council; ENF for Nedbank.

485 Law Society of SA.

486 CAPES; NIA.

does not take place in response to a request.[487] [488]

* It is desirable that the scope of PAIA and of privacy legislation be consistent, in light of the fact that both access to information and privacy are constitutional rights which may have to be balanced against each other in the case of a conflict arising.[489]

4.2.307 Concern was, however, expressed that legislation supplementing the right to access to information under PAIA (eg, the National Archives Act) may need to remain unaltered to ensure that the constitutional right of access to information is given effect to. Considerations of privacy should not be used to justify reducing access to information under legislation currently providing for more liberal access than does PAIA (eg, the National Archives Act) to a greater extent than is necessary to give effect to the constitutional right to privacy.[490]

4.2.308 Concern was raised[491] that no provision is made in section 21(1) of the Discussion Paper Bill for exemptions in instances where individual (data subject) participation is inappropriate for reasons of public interest, to avoid prejudice to the maintenance of the law, etc.

4.2.309 There should be some grounds for the refusal to provide personal information.[492] This is especially so in the context of the Promotion of Access to Information Act. In other words, any exemptions which would be applicable in terms of such Act should be applicable in the context of section 21 of the Discussion Paper Bill.

4.2.310 There should therefore be no limitations to the data subject's right of access ito sec

---

487 Section 88 reads as follows:

Correction of personal information.

88. If no provision for the correction of personal information in a record of a public or private body exists, that public or private body must take reasonable steps to establish adequate and appropriate internal measures providing for such correction until legislation providing for such correction takes effect.

488 Andrew Rens.

489 SAHA; Andrew Rens.

490 SAHA.

491 SABRIC; Vodacom (Pty) Ltd.

492 SAIA.

21(1)(b) of the Discussion Paper BIll. [493]It may be necessary to consider such limitations for instance where such access may lead to potential prejudice of criminal investigations. Section 21 (1)(c) may be included to read:

> (c) The responsible party shall not be obliged to communicate such information to the data subject where providing such information to the data subject will prejudice any criminal investigations and or proceedings by any statutory body or security agencies in relation to any matter as against the data subject or any other natural or juristic person".

Costs

4.2.311 In so far as costs are concerned, it was argued that, for example, credit reports should be accessed for a reasonable fee which covers the costs of making such a report available and providing an interpretation of the report. It should also be noted that the Promotion of Access to Information Act allows for a reasonable fee to be charged for making information available. In this regard, however, it might be appropriate to indicate that to allow free credit reports for all may place undue financial and administrative pressures on the credit bureaux and the right of access to credit reports must be balanced with the right to recover the reasonable costs of producing such a credit report.[494]

4.2.312 On the other hand it was argued that information in terms of clause 21 of the Discussion Paper Bill should be provided to the data subject without charge.[495] It is submitted that if a person wishes to collect information that person should bear all the carrying costs pertaining to such data as a natural consequence of the particular activity. This would be consistent with the requirement set out in clause 23 of the Discussion Paper Bill that the responsible party must ensure that the measures that give effect to the principles set out in this chapter are complied with.

4.2.313 A further argument was that PAIA provides that personal requesters are exempted

---

493 Eskom Holdings Ltd.

494 Credit Bureau Association.

495 Society of Advocates of Kwazulu-Natal.

from paying request fees. This arrangement should be adopted unless there can be a motivation to the effect that data subjects pay the request fee, as against PAIA.[496] The following example was provided as to how the Canadian legislation reads with regard to fees:

> If an individual is required by an organisation to pay a fee for services provided to the individual to enable the organisation to respond to a request, the organisation -
>
> (a) must give the applicant a written estimate of the fee before providing the services, and
> (b) may require the applicant to pay a deposit for all or part of the fee (section 32 of Canada)

4.2.314 Clearly the written estimate fees, referred to above, means the access fees in terms of PAIA. PAIA makes provision for search and preparation of a record whilst the Canadian legislation makes provision for estimate fees for services to respond to a request. PAIA exempts a personal requester from paying a request fee. An inference can be drawn from the Canadian position where no request or application fee has to be paid. Notwithstanding the proposal above, it was further proposed that a threshold be set for the appropriate fees to be paid by the indigent. Currently, PAIA has thresholds which may be applied in this Bill.

Access

4.2.315 Clause 21(1)(a) of the Discussion Paper Bill should also require the data subject to provide proof of identity to establish that it is the data subject's information that is being held.[497]

4.2.316 Clause 21(1)(b) of the Discussion Paper Bill provides that upon a request received from a data subject a responsible party must provide them with, amongst other things, information as to the identity of all persons who have had access to his or her personal records.

4.2.317 It was submitted that where data is stored electronically, and in particular where such data is necessarily accessible (for example in a call centre established by medical schemes or their

---

496 SAHRC.

497 SNO Telecommunications.

administrators) to deal with member queries, to be required to provide the identity of ALL persons that may have theoretically had access to such data, would be irrelevant and the cost of maintaining such information prohibitive. It was suggested that responsible parties be required to ensure that proper and adequate access controls be instituted and maintained and that codes of conduct cover such issues. Clearly where there has been a breach of a data subject's privacy the responsible party should be held liable and required to take whatever steps are practicable to identify the individual or individuals that might have had access at the time of such breach. [498]

4.2.318 A further concern was raised in that in the banking environment a large number of people access that information on a daily basis. While it may or may not be a requirement in terms of Principle 6 to keep a list of all individuals who access personal information, this section effectively creates an obligation to do so. Apart from the issue of keeping a record of who accessed what information, furnishing this information to data subjects would be too onerous in that, especially in the context of a longstanding client, the list will be extensive. The section contains no time limitation, which means that the record of persons who have accessed the information could stretch extremely far back, lengthening the list even more.[499]

4.2.319 The form in which the information is recorded may also pose certain difficulties. In the context of voice contracting, a data subject's personal information will be in the form of a voice recording. In cases where there is no need to capture information contained in a voice recording onto a different format, such as the banks' information system, in the context where an oral application for a credit card is declined, it will be onerous to expect the bank to transcribe a large quantity of voice recordings in order to provide data subjects with their personal information on which a decision was taken. The problem is aggravated by fact that the Bill specifically provides that records must be kept, at the very least, for a period long enough to allow the data subject to request access to the information. [500]

4.2.320 A solution to this problem would be to allow the bank to furnish the information in a reasonable "form". Clause 21(1)(iii) of the Discussion Paper Bill provides that the information must be

---

498 Board of Health Care Funders; Momentum Health.

499 Banking Association; Credit Bureau Association.

500 Banking Association.

furnished to the subject in a reasonable “manner”. The word “manner” could have been intended to include the “form” in which the information is to be conveyed. The clause should, furthermore, be amended to at least refer to all persons other than employees or contractors of the Responsible Party who have had access to his or her record. This should not apply retrospectively.

Correction

4.2.321 Subclause 22(4) of the Discussion Paper Bill requires a responsible party, "if reasonably practicable," to inform each person or body to whom personal information has been disclosed of the fact that the information has been corrected or that a request for correction was received and declined.

4.2.322 On the one hand it was argued that refusal by the responsible party to correct information when so requested by the data subject should be based on sound reasons. Together with a statement from the data subject requesting the information, a statement by the responsible party setting out reasons for its refusal of the request should also be posted as contemplated in clause 22(3) of the Discussion Paper Bill.[501]

4.2.323 On the other hand, it was stated that the concept "reasonably practicable" is unclear, and ignores the costs associated with implementing systems to ensure compliance by contacting a possible large number of persons. Perhaps the words "and cost effective" should be added to the concept "reasonably practicable" to provide the courts with scope to adjudicate on the balance of conflicting needs or rights.[502] Clause 22(4) of the Discussion Paper Bill places a huge technical burden on a responsible party, especially where there is a huge database of customers or employees involved. It is extremely onerous to have to notify all parties to whom information has been disclosed. It was suggested[503] that this obligation should be qualified to refer only to instances where the changed information has an impact on the use of the information by the person in question and not in circumstances where there is no intention of ongoing use of such information. An example of this

501 Vodacom (Pty) Ltd.

502 Banking Council.

503 Nedbank.

would be disclosure of information relating to a bank client to a prospective employer of such client. Such information will only be used at that point in time.[504]

4.2.324 If information is corrected it would also be very difficult to inform the consumer of all persons to whom the information was reported prior to the correction and the question was posed how far back this should go. In terms of the National Credit Act, if a person disputes data, the credit bureau must investigate the circumstances. If no credible evidence is found in support of the data it must be removed, if credible evidence is found it is provided to the consumer and the consumer can challenge the evidence through the CIO or Regulator. The question was posed why, if credible evidence is provided to someone in support of data, should a statement still be attached in terms of the Bill for the protection of personal information?[505]

4.2.325 With regard to the wording in clauses 22(1)(b) and 22(3) of the Discussion Paper Bill, it was recommended[506] that the words "attached" and "attach" respectively be replaced by "referenced" and "reference". It would be impractical and onerous to attach manual requests for correction to electronic records.

(iii) Recommendation

4.2.326 After consideration of the comments received, the Commission, in principle, confirms its proposals regarding data subject participation as set out in the Discussion Paper subject to amendments necessary to improve clarity. Data subjects are accordingly entitled to access to and correction of their personal information where it is in the possession or control of a responsible party.

4.2.327 The Protection of Personal Information Bill will deal with the access requests of

---

504 Nedbank.

505 Credit Bureau Association.

506 Nedbank.

requesters regarding their own personal information and PAIA will regulate the right to access to all other information.[507] Data subjects will utilise the request procedures set out in sections 18 and 53 of PAIA to access their personal information. A responsible party may refuse to disclose personal information requested in terms of the Bill where the grounds of refusal set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of PAIA apply.

4.2.328 A single authority will furthermore administer both Acts. See discussion on monitoring and supervision in Chapter 7 below.

4.2.329 Where personal information is corrected or deleted in accordance with requests from data subjects, the responsible parties are required to notify any third parties to whom the information was distributed, of their actions. This would prevent third parties from using incorrect information in their decision making processes.

4.2.330 Where a data subject has disputed the correctness of the information held by the responsible party and the responsible party was able to provide the subject with credible evidence in support of the data, notification will not be necessary. However, where there is still disagreement between the opposing parties, an indication of the request received has to be attached to the information (clause 23(2)(c)) and notification of this action is required in terms of clause 23 (3).

4.2.331 The Commission recommends that the legislative enactment of Principle 8 should read as follows:

PRINCIPLE 8

Data subject participation

Access to personal information

507 Amendments to PAIA to be effected by consequential amendments.

22.(1) A data subject, after having provided adequate proof of identity, has the right to -

(a) request a responsible party, to confirm, free of charge whether or not the responsible party holds personal information about the data subject; and

(b) request from a responsible party, a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information -

(i) within a reasonable time;

(ii) at a prescribed fee, if any, that is not excessive;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) If, in accordance with subsection (1)(b) of this section, personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 23 to request the correction of information.

(3) If a data subject is required by a responsible party to pay a fee for services provided to the data subject in terms of subsection 22(1)(b) to enable the responsible party to respond to a request, the responsible party -

(a) must give the applicant a written estimate of the fee before providing the services, and

(b) may require the applicant to pay a deposit for all or part of the fee.

(4) A responsible party may or must refuse to disclose any information requested in terms of subsection (1) to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act 2 of 2000 apply.

(5) If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of subsection (4), every other part must be disclosed.

Correction of personal information

23.(1) A data subject has the right to request a responsible party to -

(a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete or misleading, or obtained unlawfully; or

(b) destroy or delete a record of personal information about the data subject that it is no longer authorised to retain in terms of section 14.

(2) On receipt of a request in terms of subsection (1) a responsible party must do the following -

(a) correct the information;

(b) destroy or delete the information;

(c) provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or

(d) where agreement cannot be reached between the responsible party and the data subject, and if the data subject so request, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

(3) If the responsible party has taken steps under subsection (2) of this section that results in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of these steps.

(4) The responsible party must notify a data subject, who has made a request in terms of subsection (1) of the action taken as a result of the request.

Manner of access

24. The provisions of section 18 and section 53 of the Promotion of Access to Information Act 2 of 2000 apply to requests made in terms of sections 22 and 23 of this Act.

4.3 Processing of special personal information (sensitive information)[508]

a) Proposals in the Discussion Paper

4.3.1 As stated in Chapter 3 above, the EU Directive lays down additional conditions (over and above the usual criteria for making processing lawful) for the processing of so-called "special categories of information" (usually referred to as sensitive information). These conditions therefore primarily manifest in rules that place special limits on the processing of predefined categories of information.

4.3.2 The most influential list of these information categories is provided for in Article 8(1) of the EU Directive:[509] it embraces information on a person's "racial or ethnic origin", "political opinions", "religious or philosophical beliefs", "trade union membership",[510] "health" and "sexual life". Further, Article 8(5) makes special provision for data on criminal records and the like.[511]

4.3.3 Similar lists are found in numerous other data protection instruments at both international and national level,[512] though these vary somewhat in scope. For instance, the list in Article 6 of the CoE Convention omits data on trade-union membership, while the list in the UN Guidelines includes data on membership of associations in general (not just trade unions).

---

508 See discussion on sensitive information in Chapter 3 above.

509 Art 8(1) of the EU Directive provides as follows:
1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

510 This has caused some problems in EU countries about the publishing of membership lists of such bodies for which consent is now required.

511 Art 8(5) of the EU Directive provides as follows:
5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

512 The UK Data Protection Act, 1998 sets out conditions for the processing of sensitive data as part of its First Principle (data to be processed fairly and lawfully) and includes **explici**t consent to processing.

4.3.4 The lists in some national laws also include, or have previously included, information revealing a person to be in receipt of social welfare benefits, social affiliation, and so-called "private matters". Genetic information is furthermore in some instances formally defined as information on health. [513] Information on credit worthiness or debts is sometimes subject to special restrictions.[514] In France such information is regarded as subject to special obligations of confidentiality (in particular when processed by financial institutions) and thus subject to strict scrutiny, in particular as concerns disclosures and secondary uses. [515]

4.3.5 By contrast the UK data protection authority has expressed fundamental doubts about the need for treating certain information as (always) special. It would mean that even relatively benign information has to be afforded special treatment. It has been argued that personal information is sensitive because of the circumstances in which it is processed not simply because of its content.[516]

4.3.6 The absence of extra safeguards in the OECD Guidelines appears to be due partly to failure by the Expert Group responsible for the drafting of the Guidelines to achieve consensus on which categories of information deserve special protection, and partly to a belief that the sensitivity of personal information is not an a priori given but dependent on the context in which the information is used. The previous or current absence of extra protection for designated categories of especially sensitive information in some national information protection laws would appear to be due to much the same considerations, along with uncertainty over what the possible extra protection should involve.[517]

4.3.7 Another question that arises is whether information that indirectly reveals certain sensitive

---

513 The Netherlands.

514 The Netherlands, Portugal, Denmark etc.

515 Korff ***Comparative Study*** at 85.

516 Korff ***Comparative Study*** at 85; The Information Commissioner accepted that it was a traditional feature of data protection law, but did not agree.

517 Bygrave ***Data Protection*** at 69 and references therein eg Law Reform Commission of Hong Kong, Report on the Reform of the Law Relating to the Protection of Personal Data 1994 at n158, vol 2 paras 1218ff.

matters is covered. Thus, the fact that someone regularly buys kosher or hala'l meat or subscribes to certain magazines, or visits certain web sites may not be information on or as to that person's beliefs, but such a fact can be said to nevertheless reveal such special information. The French law expressly stipulates that information which "indirectly" reveals sensitive matters is also subject to the in-principle prohibition.[518]

4.3.8 Most national laws provide for express consent for the processing of special information and this has been interpreted as requiring that the consent must be in writing. The French data protection authority has however, accepted that, with regard to processing on the Internet, one may substitute a "double-click" for this consent (i.e. one "click" to confirm that one is aware of the proposed processing, and a further one to "expressly" consent to it).[519] In terms of the Electronic Communications and Transactions Act, section 13(5) provides for an "expression of intent" being adequate where an electronic signature is not required. In the circumstances, unless a signature is specifically required, consent may be given and be deemed to be in writing under and in terms of section 13(5).

4.3.9 The laws in several member states expressly provide for the issuing of more specific ad hoc authorisation as envisaged in Article 8(4), but only the UK has in fact issued them. [520] A special Order has been issued on the processing of sensitive data.[521]

4.3.10 In the Discussion Paper the Commission proposed that additional conditions have to be imposed for the processing of so-called special information. Part B of Chapter 3 of the Discussion Paper Bill makes provision for a general prohibition on processing of special information coupled

---

518 Korff ***Comparative Study*** at 84.

519 Korff ***Comparative Study*** at 90.

520 Article 8 (4) provides as follows:
Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

521 Data Protection (Processing of Sensitive Personal Data) Order 1999.

with general and specific exemptions to this principles. [522] See para (b) evaluation below for a discussion on the specific proposals as set out in the draft Bill.

(b) Evaluation

(i) General

4.3.11 In general, it was welcomed that special personal information will enjoy additional protection under Part B of Chapter 3.[523]

4.3.12 Commentators stated that the additional protection was appropriate in light of South Africa's history. It was argued that special personal information should not be relayed or even accessed without specific consent of the individual concerned, whilst the practice of collecting superfluous

---

522 Clauses 24 and 31 of the Discussion Paper Bill read as follows:

Part B

Processing of special personal information

Prohibition on processing of special personal information

24. It is prohibited to process personal information concerning [Sometimes the words "revealing" or "on" are used and the words "directly or indirectly" are included.] a person's religion or philosophy of life, race, political persuasion, health or sexual life, or personal information concerning trade union membership, criminal behaviour, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct, except where the data subject has given his or her explicit consent to the processing of the information or as otherwise provided in this section.

General exemption to the prohibition on processing of special personal information

31. (1) Without prejudice to sections 25 to 30, the prohibition on processing personal information referred to in section 24 does not apply where:

(a) this is carried out with the express consent of the data subject;
(b) the information has manifestly been made public by the data subject;
(c) this is necessary for the establishment, exercise or defence of a right in law;
(d) this is necessary to comply with an obligation of international public law, or
(e) this is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy and this is provided for by law or else the Commission has granted an exemption.

(2) The prohibition on the processing of personal information referred to in section 24 for the purpose of scientific research or statistics does not apply where:

(a) the research serves a public interest,
(b) the processing is necessary for the research or statistics concerned,
(c) it appears to be impossible or would involve a disproportionate effort to ask for express consent, and
(d) sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

523 Department of Home Affairs; Law Society of SA.

personal information should be discouraged.[524]

4.3.13 Agreement was expressed with the exceptions to the processing of special personal information set out in the EU Directive and it was furthermore indicated that clauses 24 to 31 of the draft Bill covered this aspect adequately in accordance with the Directive. The proposed exemptions are sensible since the South African society does have inequities that still need to be addressed.[525]

(ii) Children

4.3.14 Personal information of children was not dealt with separately in the Discussion Paper Bill. However, since the Information Protection Principles are applicable to all personal information, they were accordingly, in terms of that Bill, also applicable to the processing of children's personal information. This position is in accordance with most privacy legislation in other jurisdictions where it is assumed that all individuals, regardless of age, have the same privacy rights.[526]

4.3.15 During consultations with various stakeholders [527] the need for additional protection of personal information of children has become clear.[528] In many instances personal information relating to children is gathered from many different sources, such as on-line registration pages, survey forms, order forms and on-line contests allowing profiling and accurate targeting of children.

4.3.16 Schools and child care services also process a vast array of personal information regarding children. This include names, addresses, family information, subjects studied, grades and

---

524 Law Society of SA.

525 Law Society of SA.

526 ***ALRC Discussion Paper*** at 1777.

527 Lawyers for Human Rights Child Rights Project focus group meeting at the SA Human Rights Commission on 29 March 2007 dealing with the protection of children from exposure to adult content through the Internet and other applications, particularly wireless applications provided on new generation cell phones; See, however, the presentation of Leon Perlman, Chairman of the Wireless Application Service Providers Association (WASPA) entitled "Protection of Minors From Age-Restricted Content" where the Association's commitment to self-regulation was explained.

528 Submission from Mark Heyink at Project Committee meeting on 28 June 2007.

behavioural information, health information, photos and videos.[529]

4.3.17 According to a study conducted by Youth Dynamix and reported on 7 March 2007, 47 percent of children aged 7-9 has access to a mobile phone, 50 percent of children aged 10-12 and 58 percent of children 13-15.[530] While mobile communications devices are currently used by children in South Africa mainly for SMSing and receiving phone calls, they will increasingly also be used for MMSing, SMS chatting, downloading logos, accessing all kinds of content, as a payment method, accessing the Internet, audio and video streaming, gambling, gaming, and as a location device. Social network sites such as MySpace, Facebook and YouTube, furthermore, provide a forum for young people to share their thoughts and experiences with other like-minded people.

4.3.18 The inherent vulnerability of children coupled with the vast amount of personal information being collected already, seems to motivate special treatment. On-line networking throws up two additional issues for consideration. The first is young people choosing to disclose information about themselves.[531] Secondly, is the ability for third parties to post, alter or remove personal information about another.[532] Children should therefore first of all be protected against their own immaturity and, secondly, against malicious third parties.

4.3.19 Children are more facile and make more use of information and communications technologies than their parents. The parents are therefore in many instances not aware of the dangers that their children may expose themselves to and the children themselves are too young to appreciate certain of the dangers.[533]

---

529 ***ALRC Discussion Paper*** at 1795; EU Article 29 Working Party ***Working Document 1/2008 on the Protection of Children's Personal Data (General guidance and the special cases of schools)*** 18 February 2008.

530 Thornton L "Protecting Minors form Harmful Content via Mobile Phones" Discussion Paper for Focus Group hosted by Lawyers for Human Rights Child Rights Project on 26 March 2007 (hereafter referred to as "Thornton paper") at 3.

531 This is the first generation to have their sexual adventures, drug taking, immature opinions, and personal photographs indelibly recorded electronically. See the reference to P Balzalgette "Your Honour,Its About Those Facebook Photos of You at 20" The Observer 20 May 2007 in ***ALRC Discussion Paper*** at 1730.

532 ***ALRC Discussion Paper*** at 1729.

533 ***ALRC Discussion Paper*** at 1717 states that where older generations have adapted to new technology, the new generations now live and breath the internet, e-mail, instant messaging and mobile technologies that have revolutionised communications. They live in a global village, where you can communicate across the globe through a variety of instantaneous media.

4.3.20 Children are, furthermore, especially susceptible to the lures of downloading ring tones, logos, games and music and this is often done without the knowledge of the parent, who is paying for the service. Children are also particularly vulnerable to deceptive advertising practices and fraud. They will also hand out personal and confidential information such as credit card details[534] without a second thought. Children sometimes take pictures of one another in compromising activities, such as toileting and having sex, and then distribute those images via MMS.[535]Their concerns seem to be linked to identity theft and receiving spam, rather than stalking and harassment.[536]

4.3.21 Interactive services are, however, of concern in relation to children because they provide a means for predatory individuals to lure children into face-to-face meetings, where they may be abused, abducted or even killed. [537]

4.3.22 The fact that children may seem careless about their personal information does not mean that children do not value their privacy or that they do not sometimes experience the need to be able to change their minds. Privacy protection is not only about control of the disclosure of your information. The protection of privacy is also about the ability to control your personal information, even after you have disclosed it.[538]

4.3.23 It was therefore proposed that the control of the processing of children's personal information, even where it is for legitimate purposes, should be established in order to provide proper protection of their personal information and to assist efforts of protecting children against the abuse that we see reflected in the media on a daily basis.[539]

4.3.24 The right of privacy for children is set out in Article 16 of the United Nations Convention on

---

534 Thornton paper at 8; ***ALRC Discussion Paper*** at 1729.

535 Thorton paper at 9.

536 ***ALRC Discussion Paper*** at 1721.

537 Thornton paper at 8.

538 See ***NM v Smith*** supra at 263 para [44].

539 Mark Heyink.

the Rights of the Child.[540] The term "child" is defined in the Convention as a person under the age of 18 years old. It reads as follows:

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation.
2. The child has the right to the protection of the law against such interference or attacks.

4.3.25 South Africa ratified the CRC on 16 July 1995. Any legislation, policy or practice that is inconsistent with CRC would mean that South Africa is in breach of its international obligations.

4.3.26 Section 28 of the Constitution furthermore provides that all the rights in the Bill of Rights apply to children. One of the rights entrenched in the Bill of Rights is the right to privacy. [541]

4.3.27 In examining other jurisdictions, the USA stands out as an example where specific provision has been made for the protection of children's personal information. The Children's Online Privacy Protection Act (COPPA) Rule regulates the online collection of personal information from children under 13 years of age. The primary goal of the COPPA Rule is to give parents control over what information is collected from their children online and how such information may be used.

4.3.28 As a result of the implementation of COPPA in the United States, many social networking sites are developing standards for their terms of participation which set age limits and encourage parental monitoring and reporting of under-age use.[542]

4.3.29 The Federal Trade Commission has approved TRUSTe as a COPPA Safe Harbor programme. By obtaining a TRUSTe Children's Seal it certifies that a business is compliant with the COPPA Rule, letting parents know that their kids' information is safe. It therefore brands an organisation and web site as "child friendly".

---

540 United Nations Convention of the Rights of the Child, Adopted and opened for signature, ratification and accession by the General Assembly Resolution 44/251 on 20 November 1989, entered into force generally on 2 September 1990 (hereafter referred to as "CRC").

541 See discussion on the right to privacy in Chapter 2.

542 ***ALRC Discussion Paper*** at 1746.

4.3.30 The FTC has, furthermore, a sliding scale approach to obtaining verifiable parental consent, with the requirements for obtaining consent becoming more rigorous where the intended use of the information involves disclosure to third parties rather than internal use.[543]

4.3.31 In principle, verifiable parental consent seems to form the basis of the protection of the information of children. This is in accordance with the CRC which states in art 5 [544] that State Parties must respect the responsibilities, rights and duties of parents to provide appropriate direction to the child.

4.3.32 Verifiable parental consent can be obtained through the use of an email message to the parent, coupled with additional steps to provide assurances that the person providing the consent is, in fact, the parent. [545]

4.3.33 A second aspect to be noted, however, is that the CRC embodies a balancing exercise in that Article 12 [546] refers to the child's right to be heard in matters affecting the child. It, therefore, recognises that the family is the fundamental unit of society, but that as children are individuals who are not wholly subsumed in the family.

4.3.34 The question to be determined is what the age requirement for parental consent should be.

---

543 ***ALRC Discussion Paper*** at 1790; In September 2006 the FTC imposed a civil fine of $1 million on the blog hosting site Xanga.com and its owners for various breaches of COPPA. The fine is more than double any previous fine for such an infringement and demonstrates the high priority given by the regulator to the issue of child privacy. See discussion in Walker C "Regulation and Guidance on the Use of Child Data" ***Data Protection Law and Policy*** Newsletter for Data Protection Professionals October 2006 Vol 3 Issue 10 at 4.

544 Art 5 of CRC reads as follows:

States Parties shall respect the responsibility, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognised in the present Convention.

545 ***ALRC Discussion Paper*** at 1732.

546 Art 12 of CRC reads as follows:

1. States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.

2. For this purpose, the child shall in particular be provided the opportunity to be heard in any judicial and administrative proceedings affecting the child, either directly, or through a representative or an appropriate body, in a manner consistent with the procedural rules of national law.

COPPA, for instance, only provides protection to children under 13 years of age.

4.3.35 A final very important point is, furthermore, that the need for education of children, young people and their teachers and parents to inform them of the possible pitfalls in sharing information online and how to use networks safely and appropriately, could not be overstated.[547] In this regard it is the community at large that should accept responsibility, but the Information Protection Regulator has a special responsibility since one of the stated duties of the Regulator is that of education. See discussion in Chapter 7 below.

4.3.36 The Commission has therefore decided to make specific provision for the regulation of children's information. The Bill provides for a prohibition on the processing of personal information of children who are subject to parental control, unless processing is carried out with prior parental consent. No specific age requirement has been set. A child is defined in the Bill as a natural person under the age of 18 years. The additional qualification of parental control provides for a measure of flexibility since different laws in South Africa dealing with children's issues make provision for different age requirements for parental control. Where a child is not subject to parental control, the ordinary Information Protection Principles will regulate the processing of information. See clauses 25 and 32 at 303 and 308 below.

(iii) Religion

4.3.37 Provision was made in the Discussion paper for an exemption to the prohibition of processing of personal information concerning a data subject's religion or philosophy of life. [548]

---

547 At the 29th Conference of Data Protection and Privacy Commissioners reference was made in the Children's Privacy Education workshop to three privacy education modules that have been effectively used in the classroom in Canada: Media Awareness Network "Privacy Playground: The First Adventure of the Three Cyberpigs"; Alberta Civil Liberties Research Centre "Techno-tonomy manual"; On the Identity Trial Project "In Your I" . In so far as the goals of privacy education is concerned it was stated that a public education strategy not only seeks to inform but also to engage individuals in a process that challenges them to draw their own conclusions and incorporate what they have learned into their own framework of values.

548 **Exemption to the prohibition on processing of personal information concerning a person's religion or philosophy of life**

4.3.38 Comment was received [549]on the fact that written consent is required in clause 25(1)(c) but not in clause 25(2).

4.3.39 It was, furthermore, noted[550] that, in terms of clause 25(1)(c), the prohibition on processing personal information concerning a person's religion or philosophy of life does not apply where the processing is carried *out* by an institution provided that *it is necessary for the spiritual welfare of the data subjects.* The question was posed who would determine whether the processing of this information is necessary for the spiritual welfare of the data subject.

4.3.40 The Commission's attention was also drawn[551] to the fact that specific reference is made to church associations and not for eg to ashrams, temples, mosques or synagogues. It was argued that it could appear as if special preference has been accorded to church associations. It was suggested that, in the interests of equality, all religions should be referred to, or none at all, in which case references should be to spiritual and religious organisations.

4.3.41 The Commission's recommendation is that the reference to "church associations "be withdrawn and replaced with "spiritual or religious organisations". "Consent" is, furthermore, defined and used consistently throughout the Bill and written consent by the data subject is therefore not necessary. The Commission, however, decided to retain, for

---

25. (1) The prohibition on processing personal information concerning a person's religion or philosophy of life, as referred to in section 24, does not apply where the processing is carried out by -

(a) church associations, independent sections thereof or other associations founded on spiritual principles, provided that the information concerns persons belonging thereto;
(b) institutions founded on religious or philosophical principles, provided that this is necessary to the aims of the institutions and for the achievement of their principles, or
(c) other institutions provided that this is necessary to the spiritual welfare of the data subjects, unless they have indicated their objection thereto in writing.

(2) In the cases referred to under subsection(1)(a), the prohibition also does not apply to personal information concerning the religion or philosophy of life of family members of the data subjects, provided that -

(a) the association concerned maintains regular contacts with these family members in connection with its aims, and
(b) the family members have not indicated any objection thereto in writing.

(3) In the cases referred to under (1) and (2), no personal information may be supplied to third parties without the consent of the data subject.

549 Department of Communications.

550 Department of Communications.

551 Sovereign Health.

evidentiary purposes, the reference to written consent in so far as family members of the data subject are concerned. See clause 26 at 304 below.

(iv) Race

4.3.42 Provision has been made in the Discussion paper[552] for an exemption to the prohibition on processing of personal information concerning a person's race.

4.3.43 One commentator[553] noted that section 26 requires that, whilst the processing of information relating to a data subject's race is allowed if done pursuant to black economic empowerment, such processing must cease if the data subject objects thereto in writing. However, in terms of the Financial Services Charter banks have certain obligations and are required to submit reports to government regarding how they have performed in meeting empowerment targets. The possibility that data subjects can prevent the processing of their race entails that there is a risk to the bank that its report will not be a true reflection of its actual performance in this regard.

4.3.44 The Commission noted the abovementioned comments and decided to amend the exemption in order not to make provision for the data subject's objection any more. See clause 27 at 304 below.

(v) Political persuasion

---

552 **Exemption to the prohibition on processing of personal information concerning a person's race**

26. The prohibition on processing personal information concerning a person's race, as referred to in section 24, does not apply where the processing is carried out -

(a) with a view to identifying data subjects and only where this is essential for that purpose;

(b) for the purpose of assigning a preferential status to a person from a particular ethnic or cultural group with a view to eradicating or reducing actual historical or socio-economic inequalities, provided that the data subject has not indicated any objection thereto in writing.

553 Banking Association.

4.3.45 Provision has been made in the Discussion paper[554] for an exemption to the prohibition on processing information concerning a data subject's political persuasion.

4.3.46 One commentator[555] submitted that the provisions of section 27(1)(b) which exempt a person from the prohibition on processing personal information concerning a person's political persuasion in certain cases, are unnecessary and not sufficiently defensible. It was not clear why political persuasions would be relevant in relation to the performance of administrative duties, and what would constitute a "*reasonable*" application of a political persuasion under section 27(1)(b). It was suggested that this subsection be deleted.

4.3.47 The Commission noted the comment and deleted the subsection. See clause 29 at 305 below.

(vi) Health and sex life

4.4.48 Provision was made in the Discussion paper[556]for an exemption to the prohibition on

---

554 **Exemption to the prohibition on processing of personal information concerning a person's political persuasion**

27. (1)The prohibition on processing personal information concerning a person's political persuasion, as referred to in section 24, does not apply where the processing is carried out -
(a) by institutions founded on political principles with respect to their members or employees or other persons belonging to the institution, provided that this is necessary to the aims of the institutions and for the achievement of their principles, or
(b) with a view to the requirements concerning political persuasion which can reasonably be applied in connection with the performance of duties in administrative and advisory bodies.
(2) In the cases referred to under subsection(1)(a), no personal information may be supplied to third parties without the consent of the data subject.

555 SNO Telecommunications PtyLtd.

556 **Exemption to the prohibition on processing of personal information concerning a person's health or sexual life**

29. (1) The prohibition on processing personal information concerning a person's health or sexual life, as referred to in section 24, does not apply where the processing is carried out by:
(a) medical professionals, healthcare institutions or facilities or social services, provided that this is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;
(b) insurance companies, provided that this is necessary for:
(i) assessing the risk to be insured by the insurance company and the data subject has not indicated any objection thereto, or
(ii) the performance of the insurance agreement; or
(iii) the enforcement of any contractual rights and obligations.
(c) schools, provided that this is necessary with a view to providing special support for pupils or making special arrangements in connection with their health or sexual life;
(d) institutions for probation, child protection or guardianship, provided that this is necessary for the performance of their legal duties;

processing of personal information concerning a data subject's health and sexual life.

4.3.49 It is well known that nothing affects man as closely as his own health. And as much as we depend on support from others and new techniques, we want to determine for ourselves who has knowledge of what, and in what circumstances, about our health problems. Technical progress can therefore not only be a source of hope, but also of concern. [557]

4.3.50 Privacy and confidentiality have long been recognised as essential elements of the doctor-patient relationship. [558] For optimal care of the patient, it is essential for the medical profession (medical practitioners, dentists, psychiatrists and psychologists) to collate information on the health

---

(e) the Ministers of Justice and Constitutional Development and of Correctional Services, provided that this is necessary in connection with the implementation of prison sentences or detention measures, or
(f) administrative bodies, pension funds, employers or institutions working for them, provided that this is necessary for:
(i). the proper implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sexual life of the data subject, or
(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In the cases referred to under subsection (1), the information may only be processed by persons subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or under a written agreement.

(3) Where responsible parties personally process information and are not already subject to an obligation of confidentiality by virtue of office, profession or legal provision, they are required to treat the information as confidential, except where they are required by law or in connection with their duties to communicate such information to other parties who are authorised to process such information in accordance with subsection (1).

(4) The prohibition on processing other personal information, as referred to in section 24, does not apply where this is necessary to supplement the processing of personal information concerning a person's health, as referred to under subsection (1)(a), with a view to the proper treatment or care of the data subject.

(5) Personal information concerning inherited characteristics may only be processed, where this processing takes place with respect to the data subject from whom the information concerned have been obtained, unless:
(a) a serious medical interest prevails, or
(b) the processing is necessary for the purpose of scientific research or statistics.

(6) More detailed rules may be issued by regulation concerning the application of subsection (1)(b) and (f).

557 Jacob J "Health at the Heart of Files" Paper presented at the 23rd International Conference of Data Protection Commissioners in Paris September 2001 (hereafter referred to as "Jacob"); see also ***NM ao v Smith ao*** supra at 762 where Madala J stated as follows in par 41: Individuals value the privacy of confidential medical information because of the vast number of people who could have access to the information and the potential harmful effects that may result from disclosure. The lack of respect for private medical information and its subsequent disclosure may result in fear jeopardising an individual's right to make certain fundamental choices that he/she has a right to make. There is therefore a strong privacy interest in maintaining confidentiality.

558 Klinck E Legal Advisor, Human Rights, Law and Ethics Unit, SAMA ***Health Data Confidentiality and Privacy : Standards*** Document based in part on the document generated by Dr Pino Mavengere, Previous Team Leader, Privacy and Confidentiality Subcommittee of the Committee on Standardisation of Data and Billing Practices (hereafter referred to as "Klinck") at 1.

of their patients[559] into a complete medical record.

4.3.51 Each time a patient sees a doctor, is admitted to hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information.[560] This record is used for a wide variety of purposes including insurance functions, co-ordination of care, and research.[561] Databases are also established containing information in health and genetic materials so as to be able to do research on diseases and disorders with a genetic component.[562]

4.3.52 The longstanding friction between these two goals, namely patient privacy and access to information, has been heightened by the transition to electronic health information and a push toward integrated information in support of health care delivery and health data networks. While these developments are intended to improve health care,[563] they also raise many questions about the role of privacy in the health care environment. [564]

4.3.53 It is therefore important, when using data relative to health, to give high priority to the right of the people concerned to self-determination in this essential and private domain.[565]

4.3.54 The public has some reason to be concerned. Today there is little consistency in approaches to patient confidentiality apart from the general constitutional provisions that are not aimed at the specifics of doctor-patient-medical relationship. Note should, however, be taken of the Patient

---

559 Neethling ***Huldigingsbundel WA Joubert*** at 109.

560 US Department of Health and Human Sciences ***Fact Sheet*** May 9, 2001.

561 Klinck at 1.

562 Example of Islandic Health Sector Database as set out in Hreinsson P "Projects and People (Islandic Health Sector Data base)" Paper delivered at the 23rd International Conference of Data Protection Officers, Paris September 2001.

563 Alvarez R "On guard: Electronic Health Records and Safeguarding Patient Privacy" Presentation made at the Health Information Privacy Day in Toronto on 24 September 2007 indicates that the advantages of electronic health records are-

- increased patient participation in care;
- well managed chronic illness;
- improved access to care in remote and rural communities;
- fewer adverse drug events;
- better prescribing practices;
- reduction in duplicate or unnecessary tests; and
- reduced waiting times.

564 Klinck at 1.

565 Jacob at 2.

Confidentiality Subcommittee of the National ICD-10 Task Team of the Health Professions Council of South Africa which conducted an investigtaion into the regulatory review on ICD-10 and the right to privacy or confidentiality and published a document entitled “Patient Confidentiality” on 18 July 2007.

4.3.55 A person may indeed be harmed by the use of his or her health information outside the core health care arena. The following examples have been noted:[566]

- an employee was fired from a job days after being diagnosed with a genetic disorder that required expensive treatment. The employer, who is self-insured, fired her to avoid the projected expenses.
- a woman’s photograph and medical records was posted on the Internet by anti-abortion activists without her permission after receiving treatment at a hospital for complications from an abortion.
- Several thousand patient records inadvertently lingered on public Internet sites for two months due to a mistake made at a Medical Centre.
- An employee was automatically enrolled in a “depression program” by her employer after her prescription drugs management company reported that she was using anti-depressants.
- A drug company inadvertently revealed 600 patient e-mail addresses of persons using Prozac when an e-mail was sent to all the participants instead of to individual users.
- A data subject’s medical information maybe misused and even exploited when personal medical records are stored or sold for marketing purposes.[567]

4.3.56 Genetic engineering without bioethics would furthermore risk breaking various protective taboos. Thus, decoding the genome[568] in order to evaluate the human being and his worth to society would risk flouting every man’s right to his intrinsic value and to the recognition of his dignity, which

---

566 Goldman at 2.

567 EPIC Testimony and Statement by Marc Rotenberg and Chris Hoofnagle before the Subcommittee on Financial Institutions and Consumer Credit Committee on Financial Services, United States House of Representatives in the Hearing on the Role of FCRA in Employee Background Checks and the Collection of Medical Information at 2.

568 It was announced on CNN on 12 April 2003 that scientists working together in six countries have finalised their work in decoding the genome.

cannot be calculated from hereditary biological factors. It is therefore the fear that the usefulness of a human being may be evaluated based on recordings of the state of his health and that this might determine, for example, whether he gets or keeps a job, his creditworthiness, even possibly his life and death when measured against the costs needed for the necessary treatment.[569]

4.3.57 The situation has therefore developed where billions of dollars have been spent mapping the human genome and yet people are afraid to get a genetic test. The Internet can zip medical information and services from doctor's offices into your home, and yet people are afraid to go online. The fear and reticence that cause people to withdraw from full participation in their own care should be the common cause around which to unite.[570]

4.3.58 The National Health Act[571] provides that every patient is entitled to confidentiality of all health information, including health status, treatment or stay in a private or public establishment.[572] This information is only to be disclosed if the user consents in writing, if a law or a court order authorises the disclosure or if non-disclosure represents a serious threat to public health.

4.3.59 Mechanisms for the protection of health records held by any private or public health establishment are furthermore found in section 17 of the Act.[573] It lists some 9 types of conduct that would constitute an offence.[574]

---

569 Jacob at 1.

570 Goldman at 7.

571 National Health Act 61of 2003.

572 Section 14 of the National Health Act, 2003 contains the following prescript in relation to patient information and records:
Confidentiality

14. (1) All information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment, is confidential.
(2) Subject to section 15, no person may disclose any information contemplated in subsection (1) unless -
(a) the user consents to that disclosure in writing;
(b) a court order or any law requires that disclosure; or
(c) non-disclosure of the information represents a serious threat to public health.

573 See also ***Tshabala-Msimang ao v Makhanya ao*** supra at para [26].[27] and [31] and ***NM ao v Smith ao*** supra at para [40]and[43].

574 Included are:
… (g) without authority, connects the personal identification elements of a user's record with any element of that record that concerns the user's condition, treatment or history;
(h) gains unauthorised access to a record or record-keeping system, including intercepting information being transmitted from one person, or one part of a record-keeping system, to another;

4.3.60 The more intimate [that] information, the more important it is in fostering privacy dignity and autonomy that an individual makes the primary decision whether to release the information. That decision should not be made by others.[575] It is for this reason that the National Health Act recognises confidentiality of records and the privacy attaching to such information. It also recognises the need to protect the information that is contained therein and regulates the position regarding the keeping, maintenance, access, and disclosure of a user's health records.[576]

4.3.61 However, one also has to take note of conflicting rights of the parties in this regard. Insurance companies, or other persons having to pay the costs of medical treatment, may demand certain information necessary for controlling their expenses. Another conflict exists between the patient's right to privacy and the important interests of others in the fight against contagious diseases.[577]

4.3.62 Medical schemes are provided with patient health information for the purpose of medical aid and one can argue that by joining a scheme the patient and his/her dependants consent to the use of their medical information for scheme purposes (e.g. pay-out or non-pay-outs, etc.). The Medical Schemes Regulations authorises the transmission of patient health information, but *only where there is a managed care arrangement.*

4.3.63 In terms of regulation 15(10) a medical scheme must have access to any treatment records held by the provider and other information pertaining to the diagnosis, treatment and health status of the member *in terms of the arrangement*. Such information may not be disclosed by the provider to any other person without the written consent of the member, unless such disclosure is in terms of any legislation. Regulation 15(9) provides for the information in relation to diagnosis, treatment

---

(i) without authority, connects any part of a computer or other electronic system on which records are kept to -
(i) any other computer or other electronic system; or
(ii) any terminal or other installation connected to or forming part of any other computer or other electronic system; or
(j)without authority modifies or impairs the operation of -
(i) any part of the operating system of a computer or other electronic system on which a user's records are kept; or
(ii) any part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept.

575 O'Regan J in ***NM ao v Smith ao*** supra at par [132].

576 ***Tshabalala-Msimang aov Makhanya ao*** supra at par [32].

577 Jacob at 3.

or health of any member of a medical scheme or of any dependant of such member to be treated as confidential. The Medical Scheme is bound by this confidentiality and may not pass on, share, sell or deal with the information without a law authorising it or the patient's informed consent. Intermediaries are, by implication, bound by these regulations.

4.3.64 The World Medical Association passed a statement on ethical considerations regarding Health Databases, which sets the tone for medical associations world-wide. As with the Canadian Code, the WMA states that the primary purpose of collecting patient information is to care for the patient. Confidentiality is at the heart of medical practice and is essential for maintaining trust and integrity in the patient-physician relationship. Knowing that their privacy will be protected gives patients the freedom to share sensitive personal information with their physician.[578]

4.3.65 Quality assurance, risk management and research are so-called secondary purposes of data collection. Care must be taken that secondary uses of information do not inhibit patients from confiding information for their own health care needs, exploit their vulnerability or inappropriately borrow on the trust that patients invest in their physicians. Where possible, data for secondary purposes should be de-identified. It defines de-identified data as data where the link between the patient and information has been broken and cannot be recovered. If this is not possible, however, the use of data where the patient's identity is protected by an alias or code should be used in preference to readily identifiable data.[579]

4.3.66 The statement reaffirms that information may only be disclosed with informed consent or in terms of national law. The statement also requires documentation on what information is held and why, what consent has been obtained by patients, who may access data, why, how and when the data may be linked to other information and the circumstances under which data will be made available to third parties.[580]

---

578 World Medical Association ***Declaration on Ethical Considerations Regarding Health Databases*** Adopted by the WMA General Assembly, Washington 2002 (hereafter referred to as "WMA Declaration") at 1.

579 WMA Declaration at 3.

580 WMA Declaration at 3-4; See also the practical suggestions for protection of patient health information in Zaroukian MH "EHR's and Patient Data Privacy - Building Trust Through Effective Identity Profiling, Authentication and Authorisation" Presentation made at the Health Information Privacy Day, Toronto September 2007.

4.3.67 National medical associations should cooperate with the relevant health authorities, ethical authorities and personal data authorities, at national and other appropriate administrative levels, to formulate health information policies based on the principles in this document.[581]

4.3.68 This means that any person other than the doctor or facility who wants that information has to get the patient's consent in writing or do so in accordance with a law or court order.

4.3.69 From this it is clear that decoding of systems of de-identification is prohibited, as is the connecting of systems "without authority". It can be assumed that in view of the provisions of section 14, that authority must include consent or authorisation by law or court order. Administrative staff may have access to records for "any legitimate purpose within the ordinary course of their duties" (section 17), eg for submitting accounts to medical schemes.[582]

4.3.70 Other international sources on this issue include the following:

a) The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data binds European signatories. The regulation of data and privacy protection is supplemented by a number of Recommendations issued by the Committee of Ministers, most notably the Recommendation on the Protection of Medical Data (1997).[583]

b) The EU Directive sets out the circumstances under which personal data may be processed[584] as well as the exceptions to the processing of the data. Subsection 3 indicates that where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management

---

581 WMA Declaration at 4.

582 Klinck at 5.

583 Recommendation No R (97) 5 on the protection of medical data defines "personal data", "genetic data" and "medical data". Data may only be collected by health care professionals, or those working on behalf of the professionals (who should be subject to the same rules of confidentiality). Non-professionals controlling files are subject to rules of confidentiality comparable to those binding the professional. The Recommendation also deals with genetic data. It also provides for the withdrawal of consent at any stage by a person. Consent has to be free, express and informed. Many of the aspects already alluded to above in connection with control over the data, the right to know who has what on one and what its used for, etc. are addressed as well.

584 See discussion on EU Directive in Chapter 9 below.

> of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4.3.71 In Australia the protection of health information is regulated by the Privacy Act, 1988.[585] In June 2000 an Australian Health Ministers' Advisory Council National Health Privacy Working Group (AHMAC) was established to address the need for a nationally consistent framework for health information privacy.[586] They developed a framework referred to as the National Health Privacy Code in 2003 making provision for 11 National Health Privacy Principles. This code has, however, not yet been finalised or implemented. The ALRC has argued[587] that two sets of privacy principles seem to be undesirable and that the regulation should remain within the Information Privacy Office and the Privacy Act.

4.3.72 The Commonwealth's proposal, HealthConnect, is intended as a voluntary national health information network under which health-related information about an individual would be collected in a standard, electronic format at the point of care.[588] [589] In July 2001 the Department of Health announced that all negotiations on the implementation of this system and the introduction of the enabling legislation had been postponed due to "technical difficulties". [590] In the interim the Department is consulting with the Privacy Commissioner in order to ensure standards for patient privacy.[591]

---

585 Health services are primarily delivered by the public sector in Australia, with only around a third of the population having private health insurance. The responsibility for delivery of health services is shared between the Commonwealth Government, which is responsible for much of the funding of the health system, and the States, which operate hospitals and community health services.

586 ***ALRC Discussion Paper*** at 1573.

587 ***ALRC Discussion Paper*** at 1574.

588 For details see <http://www.health.gov.au/healthonline/connect.htm>.

589 As a first phase of this system the Department of Health and Aged Care drafted the Better Medication Management System Bill that would establish individual electronic medication records in order to improve access to information about drugs for doctors and patients. The system was widely criticized by consumers and doctors groups concerned about patient confidentiality and professional liability. "Medicos Oppose Data Bill," Karen Dearne, ***Australian IT*** July 24, 2001.

590 'Medical E-Files 'Delayed For Poll' by John Kerin, ***Australian IT***, July 30 2001.

591 "Your Health On The Line" ***Australian Financial Review*** May 25 2002.

4.3.73 In December 2001 the National Health and Medical Research Council (NHMRC) issued guidelines (under section 95A of the Privacy Act 1988) on privacy in medical research. Genetic privacy was furthermore subject to a joint review by the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council.

4.3.74 The British Medical Association has struggled to obtain political support for the formulation of proper medical data-protection/confidentiality legislation so as to settle the variety of issues in this regard. It is the BMA's view that anonymous data may be used freely. Administrative and clinical information should be separate, and assurances as to real anonymity have to be provided.[592] In the UK case of Source Informatics Ltd[593] it was stated that the anonymisation of information does not remove the duty of confidentiality. For research, medical advancement and proper administration of the NHS, consent may be construed as implied where doctors and the Health Service use anonymised information for these purposes.

4.3.75 The American Medical Association[594] keeps to the US Constitution and ethical duties so as to provide guidance to doctors in patient confidentiality. According to the AMA a breach of confidentiality is a disclosure to a third party, without patient consent or a court order, of private information that the physician has learned within the patient-physician relationship. Disclosure can be oral or written, by telephone or fax, or electronically, for example, via e-mail or health information networks. The medium is irrelevant, although special security requirements may apply to the electronic transfer of information. The general rule regarding release of a patient's medical record is that information contained in a patient's medical record may be released to third parties only if the patient has consented to such disclosure.

4.3.76 The Canadian Medical Association affirms that in terms of the CMA Code of Ethics (1996), medical records are confidential documents. Although the records are the property of the physician or health care institution that compiled them, patients have a right to examine their records and to obtain a copy of the information contained in them. Physicians should provide an explanation of the

---

592 Dates of birth, postal codes etc, especially when used in combination, can identify a person.

593 (1999) LTL 2/6/99, quoted in ***Confidentiality and Disclosure of Health Information*** 1999 at http://www.bma.org.uk/public.

594 http://www.ama-assn.org/ama/pub/category/4610.html.

medical record to the patient when requested to do so. Unless the law requires otherwise, or if the maintenance of confidentiality would result in a significant risk of substantial harm to others or to the patient if the patient is incompetent, patient authorisation is necessary for the disclosure of information contained in medical records to third parties.

4.3.77 The Canadian Medical Association (CMA) has adopted a Health Information Privacy Code[595] to protect the privacy of its patients, the confidentiality and security of its health information and the trust and integrity of the therapeutic relationship. The Code is based on the Canadian Standards Association's Model Code for the Protection of Personal Information ("CSA Code") as a sectoral code of the CSA Code. The Code provides instruction and guidance respecting health information collection, use, disclosure and access.

4.3.78 It is clear that people must maintain some degree of control over their own lives, and in this case, over the information they share about themselves in order to get health care and benefits. No right is absolute, and privacy is no exception. The power of health privacy is that it benefits individuals, improves access to care and quality of care, enhances the reliability of data downstream and is a boost for health care organisations.[596]

4.3.79 In general, the comments received on the Commission's legislative proposals set out in the Discussion Paper were positive.

4.3.80 A private organisation, IMS Health South Africa[597] indicated[598] that the organisation's Canadian office does not collect identifiable patient information. It does, however, collect prescription sales data information that identifies the prescriber via electronic means from dispensing pharmacies. The company then uses these prescription sales data and various statistical methods to produce prescriber information in the form of estimates of normative prescribing patterns of

---

595 Canadian Medical Association ***Health Information Privacy Code*** 16 September 1998 accessed at http://www.cma.ca/cma/common/displayPage. on 15/11/2002.

596 Goldman at 7.

597 IMS Health SA is part of IMS Health, the world's premier provider of healthcare information services to the global health sector.

598 IMS Health SA (Prop)Ltd "Submission in response to the draft Electronic Commerce and Transactions Bill of the Republic of South Africa" May 2002 (A Response prepared on behalf of IMS Health SA by Moore CM and Gunning K).

physicians, as well as estimates respecting individual physicians' prescribing patterns. The company only discloses estimates respecting an individual physician's prescribing patterns with the express consent of the individual prescriber; otherwise, prescriber information is disclosed only in aggregate form. In terms of clause 5 of POPIA the Bill will not be applicable to information that has been anonymised or de-identified. See discussion in Chapter 3 above.[599]

4.3.81 The Commission received a number of submissions [600] requesting that medical schemes, medical scheme administrators and managed healthcare organisations should enjoy an exemption under clause 29(1) of the Bill with the other "medical professionals, healthcare institutions or facilities or social services". The motivation provided was that medical schemes in SA (governed by Medical Schemes Act 131 of 1998) - unlike jurisdictions such as the UK- are not regarded from a legislative point of view as short-term or long-term insurers, although their business is essentially one of insurance.

4.3.82 Schemes manage their risk posed to it by members and applicants. In order to do this the scheme uses data such as information provided by applicants, inter alia, in their application forms and information obtained from member's claims. Using the data, the scheme can predict its financial obligations to its beneficiaries and design benefits and determine contributions accordingly.

4.3.83 Without the exemption, it would be necessary to have every applicant and every current beneficiary give explicit consent to the processing of their medical information. However, it would not be possible to deny membership of the scheme to a person on account of him/her not providing consent (medical schemes are characterised by the principle of "open enrolment": no person who applies may be denied membership). Information contained in the application forms is used to assess the applicability of waiting periods; identify claim trends and predict the scheme's financial obligations; design appropriate benefits and determine contributions and thereby comply with the statutory duty of remaining financially sound and sustainable; to process and pay claims.

---

599 See,however, the contentious issue of anonymisation vs pseudo-anonymisation and the question whether genetic data can ever be anonymised. Gundermann L "Genetics and Privacy: Biobanking- Trustees- Audits" Paper delivered at Health Information Privacy Day in Toronto 24 September 2007.

600 Discovery Health; Board of Health Care Funders; Sovereign Health; Momentum Health.

4.3.84 It was, furthermore, submitted[601] that regulation 5(f) of the Medical Schemes Act, 1998 requires all health service providers to include a diagnosis code on claim forms. ICD 10 is a diagnostic code standard adapted by the Department of Health that standardises the data collection processes in the industry, facilitates an efficient payment system of claims from the providers and improves risk management practices of medical schemes. ICD 10 also enables accurate communication about healthcare data among any participants in the health care industry in a standard format.

4.3.85 No diagnosis description is included on claims in order to maintain patient confidentiality. However the ICD 10 codes included on claims by health care providers are more specific than was the case previously where healthcare providers included only a general diagnosis on claims. While the ICD 10 codes contained on a claim submitted by a healthcare provider would not be easily decoded by the general public thereby ensuring greater patient confidentiality, such codes may become well known to employees of organisations who operate in the administration and managed care of medical schemes, which may result in the erosion of patient confidentiality.

4.3.86 Presently the identity of the member together with the membership number is reflected on the claim form and perhaps the exclusion of the member's name from the claim from would assist in preserving confidentiality.

4.3.87 The Commission's attention was, finally, drawn[602] to the provisions of the National Health Act (61 of 2003), clauses 14-17 (confidentiality; access to health records; access to health records by health care provider; protection of health records). See discussion above.

4.3.88 The Commission noted the comments received. It was decided to include a specific reference to medical aid schemes, medical administrators and managed healthcare organisations in the exemption. In so far as the operation of the National Health Act is concerned the Commission reiterates the fact that Clause 5 of POPIA specifically states that the Act does not affect the operation of any other legislation that regulates the processing of personal information where this legislation is capable of operating concurrently with the

---

601 Sovereign Health.

602 SA Medical Research Council.

Act. As stated above, the provisions of the National Health Act are, in principle, in line with the Information Protection Principles set out in POPIA. Where the other legislation provides safeguards for the protection of personal information that are more extensive than those set out in the Information Protection Principles, the more extensive safeguards will prevail. If the sector specific legislation is not compliant with POPIA it will have to be amended through consequential amendments. POPIA, furthermore, makes provision for sector specific codes of conduct which will be able to deal with aspects such as the ICD 10 codes. See clause 30 at 305 below.

(vii) Criminal behaviour

4.3.89 Provision was made in the Discussion Paper[603] for an exemption to the prohibition on the processing of information concerning a person's criminal behaviour.

4.3.90 A submission was received[604] that stated that Article 8(5) of the EU Directive should not be supported. To restrict information gathering on fraud issues to an "official authority" will give the criminal element in South Africa a *carte blanche* to conduct unbridled criminal conduct to the

---

603 **Exemption to the prohibition on processing of personal information concerning a person's criminal behaviour**

30. (1) The prohibition on processing personal information concerning a person's criminal behaviour, as referred to in section 24, does not apply where the processing is carried out by bodies, charged by law with applying criminal law and by responsible parties who have obtained this information in accordance with the law.

(2) The prohibition does not apply to responsible parties who process this information for their own purposes with a view to:

(a) assessing an application by data subjects in order to take a decision about them or provide a service to them, or
(b) protecting their interests, provided that this concerns criminal offences which have been or, as indicated by certain facts and circumstances, can be expected to be committed against them or against persons in their service.

(3) The processing of this information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

(4) The prohibition on processing other personal information, as referred to in section 24, does not apply where this is necessary to supplement the processing of information on criminal behaviour, for the purposes for which this information is being processed.

(5) The provisions of subsections (2) to (4) are likewise applicable to personal information relating to a ban imposed by a court concerning unlawful or objectionable conduct.

604 SAFPS.

detriment of business, consumers and the South African economy.[605]

4.3.91 In other submissions[606] it was, furthermore, argued that this exemption appears highly restrictive and perhaps requires further consideration. The Board of Healthcare Funders, a company registered in terms of section 21 of the Companies Act and which represents the interests of the healthcare funding industry (i.e. medical schemes) has established a Forensic Management Unit ("FMU") to identify and reduce fraud in the industry. Information relating to the criminal conduct of persons may be distributed between the members to prevent fraud from occurring or to reduce the risk thereof. It should be noted that the cost of medical fraud has been calculated to run into tens of millions of rand annually and it is imperative that all steps possible are taken to minimise these losses. The exemption in clause 30 does not appear to allow for such sharing of information and it was requested that this be amended so as to permit such cooperative functions.

4.3.92 The Commission decided to confirm its proposal in the Discussion Paper. It will be impossible to regulate private institutions if they do not have to comply with the Bill. Provision is made for exceptions in the Principles themselves and also for exemptions to specific principles. See discussion in par 4.4 below. It is the opinion of the Commission that these exemptions and exceptions will be sufficient to enable the Board and others to continue with their work, but within the confines of the regulatory framework.

c) Recommendation

4.3.93 The recommendation for the protection of special personal information have been set out above in order to make provision for specific circumstances in each case. The Commission has, furthermore, decided to include the regulation of trade union membership[607]

---

605 SAFPS.

606 Board of Health Care Funders, Momentum Health.

607 **Exemption to the prohibition on processing of personal information concerning a person's trade union membership**

28. (1) The prohibition on processing personal information concerning a person's trade union membership, as referred to in section 24, does not apply where the processing is carried out by the trade union concerned or the trade union federation to which this trade union belongs, provided that this is necessary to the aims of the trade union or trade union federation;

in order to ensure harmonisation with the EU Directive.

4.3.94 The legislative enactment of the regulation of the processing of special personal information reads as follows:

Part B

Processing of special personal information

Processing of special personal information (including information in respect of a child) prohibited

25. Unless specifically permitted by this Part, a responsible party may not process personal information -

a) concerning a child who is subject to parental control in terms of the law; or

b) concerning a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour.

Exemption to the prohibition on processing of personal information concerning a data subject's religious or philosophical beliefs

26.(1) The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs, referred to in section 25, does not apply if the processing is carried out by-

(a) spiritual or religious organisations, or independent sections of those organisations, provided that the information concerns data subjects belonging to those organisations;

(b) institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles, or

(c) other institutions provided that this is necessary to protect the spiritual welfare of the

---

(2) In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

data subjects, unless they have indicated that they object to the processing.

(2) In the cases referred to under subsection(1)(a), the prohibition also does not apply to processing of personal information concerning the religion or philosophy of life of family members of the data subjects, if -

(a) the association concerned maintains regular contacts with these family members in connection with its aims; and

(b) the family members have not objected in writing to the processing.

(3) In the cases referred to in subsection (1) and (2), personal information concerning a data subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the data subject.

Exemption to the prohibition on processing of personal information concerning a data subject's race

27. The prohibition on processing personal information concerning a data subject's race, as referred to in section 25, does not apply if the processing is carried out to -

(a) identify data subjects and only when this is essential for that purpose; and

(b) comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

Exemption to the prohibition on processing of personal information concerning a person's trade union membership

28.(1) The prohibition on processing personal information concerning a person's trade union membership, as referred to in section 25, does not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which this trade union belongs, if this is necessary to achieve the aims of the trade union or trade union federation.

(2) In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

Exemption to the prohibition on processing of personal information concerning a data subject's political persuasion

29.(1) The prohibition on processing personal information concerning a data subject's political persuasion, as referred to in section 25, does not apply to processing by an institution founded on political principles, of the personal information of their members or employees or other persons belonging to the institution, provided that this is necessary to achieve the aims or principles of the institutions.

(2) In the cases referred to under subsection(1), no personal information may be supplied to third parties without the consent of the data subject.

Exemption to the prohibition on processing of personal information concerning a data subject's health or sexual life

30.(1) The prohibition on processing personal information concerning a data subject's health or sexual life, as referred to in section 25, does not apply to the processing by -

- *(a) medical professionals, healthcare institutions or facilities or social services, if this is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;*
- *(b) insurance companies, medical aid schemes, medical scheme administrators and managed healthcare organisations, provided that this is necessary for -*
  - *(i) assessing the risk to be insured by the insurance company or covered by the medical aid scheme and the data subject has not objected to the processing;*
  - *(ii) the performance of an insurance or medical aid agreement; or*
  - *(iii) the enforcement of any contractual rights and obligations.*
- *(c) schools, if this is necessary to provide special support for pupils or making special arrangements in connection with their health or sexual life;*
- *(d) institutions for probation, child protection or guardianship, if this is necessary for the performance of their legal duties;*
- *(e) the Ministers for Justice and Constitutional Development and of Correctional Services, if this is necessary in connection with the implementation of prison*

sentences or detention measures; or

(f) administrative bodies, pension funds, employers or institutions working for them, if this is necessary for -

(i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sexual life of the data subject; or

(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In the cases referred to under subsection (1), the information may only be processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.

(3) Responsible parties that are permitted to process information concerning a data subject's health or sexual life in terms of this section and are not subject to an obligation of confidentiality by virtue of office, profession or legal provision, are required to treat the information as confidential, unless they are required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information in accordance with subsection (1).

(4) The prohibition on processing any of the categories of personal information referred to in section 26, does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, as referred to under subsection (1)(a), with a view to the proper treatment or care of the data subject.

(5) Personal information concerning inherited characteristics may only be processed in respect of a data subject from whom the information concerned has been obtained, unless -

(a) a serious medical interest prevails; or

(b) the processing is necessary for the purpose of scientific research or statistics.

(6) More detailed rules may be prescribed concerning the application of subsection (1)(b) and (f).

Exemption to the prohibition on processing of personal information concerning a data subject's criminal behaviour

31.(1) The prohibition on processing personal information concerning a data subject's criminal behaviour, as referred to in section 25, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained this information in accordance with the law.

(2) The prohibition does not apply to responsible parties who process the information for their own lawful purposes to -

(a) assess an application by a data subject in order to take a decision about, or provide a service to, that data subject, or

(b) protect their legitimate interests in relation to criminal offences which have been, or can reasonably be expected to be, committed against them or against persons in their service.

(3) The processing of this information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

(4) The prohibition on processing any of the categories of personal information referred to in section 25 does not apply if this is necessary to supplement the processing of information on criminal behaviour permitted by this section.

General exemption to the prohibition on processing of special personal information

32. Without prejudice to sections 26 to 31, the prohibition on processing personal information referred to in section 25 does not apply if -

(a) processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law;

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law; or

(d) the Regulator has granted authority in terms of section 34 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject's privacy;

or insofar as section 25(b) is concerned, if -

(a) processing is carried out with the consent of the data subject; or

(b) the information has deliberately been made public by the data subject.

4.4 Exemptions and exceptions

a) Proposals in the Discussion Paper[608]

608 **CHAPTER 4**

EXEMPTIONS FROM INFORMATION PROTECTION PRINCIPLES

General

32. References in any of the information protection principles to personal information or to the processing of personal information do not include references to information or processing which by virtue of this Chapter are exempt from that principle or provision.

Commission may authorise processing of personal information---

33. (1) The Commission may authorise a responsible party to process personal information, even though that processing would otherwise be in breach of an information protection principle if the Commission is satisfied that, in the special circumstances of the case -

(a) the public interest in that processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from that processing; or

(b) that processing involves a clear benefit to the data subject or a third party that outweighs any interference with the privacy of the data subject or third party that could result from that processing.

(2) The public interest referred to in subsection (1) above includes the -
(a) interests of State security;
(b) the prevention, detection and prosecution of criminal offences;
(c) important economic and financial interests of the State and other public bodies;
(d) interests of supervising compliance with legal provisions established in the interests referred to under (b) and (c), or
(e) scientific research and government statistics.

(3) The Commission may impose in respect of any authority granted under subsection (1) of this section such conditions as the Commission thinks fit.

4.4.1 We have already seen above that the information protection principles apply to all personal information processed by responsible parties. However, information protection laws usually make provision for specific exceptions to the information protection principles, and certain entities may be excluded or exempted from some or all of the provisions of a particular information protection law.

4.4.2 Drafting exceptions and exemptions should be seen as part of setting down the extent of any privacy law. Statutory exemptions from particular principles are to be preferred over exclusion from the Act of an entire class of responsible party or information. However, some types of responsible party and information will need to be excluded from the coverage of privacy principles if they are to remain workable, general and not overly complex.[609]

4.4.3 The difference between exclusions, exemptions and exceptions can be explained as follows:[610]

a) Exceptions to privacy principles define their extent. Very few privacy principles are absolute and only a proper understanding of the relevant exceptions will give an accurate picture as to what the law requires. The exception actually limits the nature of the rule itself. The exception maps out the extent of the obligations under the rule - or principle - in our case. For example, Information Protection Principles 2, 3,4 and 6 each have a number of exceptions written into them. The exceptions are identical in several of the principles. Other appear in one principle but not another.

b) Exemptions, on the other hand involves lifting a burdensome obligation from a responsible party while the burden continues to apply to others. It follows that an exemption does not really change the character of an information protection principle: it just changes the range of people (or information) to which it applies.

c) To this should be added exclusions, where certain classes of responsible parties are

---

609 Stewart B "The New Privacy Laws: Exemptions and Exceptions to Privacy" Paper prepared for The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century Sydney 19 February 1997 accessed at http://www.privacy.org.nz/media/comfin.html on 24/06/2005 (hereafter referred to as "Stewart ***Exemptions and Exceptions***") at 7.

610 Stewart ***Exemptions and Exceptions*** at 2 and further.

excluded completely from the coverage of the law. These have been dealt with in Chapter 2 of the Bill dealing with the scope or application of the legislation.

4.4.4 Broadly speaking, exclusions, exceptions and exemptions cover two situations: firstly where the risks to the privacy or identity of the data subject are relatively small[611] and secondly, where other interests override the data subject's rights to privacy and identity.[612] In general, these exclusions, exceptions and exemptions appear to be justified.[613]

4.4.5 In so far as the first situation is concerned, we have already dealt with the restriction of the scope of the proposed legislation in Chapter 3 and it has been noted that personal information kept in the course of a purely personal or household activity and any de-identified information are excluded from the ambit of the proposed legislation.[614]

4.4.6 In terms of the second situation referred to above, the EU Directive provides for a number of exceptions and relaxations to its provisions. Four categories are distinguished, namely those relating to:[615]

a) Freedom of expression;
b) Freedom of information;
c) Major public interests; and
d) The protection of data subjects or others.

4.4.7 These categories will be briefly discussed.

i) Freedom of expression

4.4.8 For a discussion on the way this right (which is set out in South Africa in section 16 of the

611 Eg Processing of information for activities exclusively intended for personal or home use.

612 Eg public interest, interests of other parties or those of the data subject himself or herself.

613 Roos thesis at 522.

614 See Chapter 3; The exclusions should also pertain to responsible parties who are subject to obligations that are, over all, at least the equivalent of the relevant obligation in POPIA. The need to comply with two equivalent regimes would unnecessarily add to the compliance burden for such entities. ***ALRC DIscussion Paper*** at 586.

615 Korff ***Comparative Study*** at 130 and further.

Constitution) is to be dealt with in the information protection legislation, see Chapter 3 above dealing with the substantive scope of the proposed legislation.[616]

ii) Freedom of information

4.4.9 The right of access to official and other documents, usually referred to as "freedom of information" is increasingly recognised as a fundamental right in developed democracies and also in South Africa. [617]

4.4.10 Although there are two fundamental principles (information protection and freedom of information) that have to be reconciled, it is globally seen as two sides of the same coin, with a general, balanced approach in individual cases.[618]

4.4.11 For a discussion of the way in which these two rights (which are set out in South Africa in sections 14 and 32 of the Constitution) are to be dealt with in the information protection legislation, see Principle 8: Data Subject Participation in Chapter 4 above.[619]

iii) Major public interests

4.4.12 It may be permissible in the public interest to restrict the scope of the rights and obligations provided for by the information protection principles in the sense that provision may be made for total or partial exemption from some of those principles.[620]

4.4.13 Laws dealing with this category refer to national security, defence, the investigation and

---

616 Para (x): Processing of information for journalistic, artistic or literary purposes.

617 Section 32 of the Constitution.

618 Korff ***Comparative Study*** at 128.

619 At 184.

620 Roos thesis at 523.

prosecution of offences, financial interests of the state, public health, social protection, scientific research and government statistics.

4.4.14 There seems to be a general acceptance in Europe that processing of personal information for police-, public order- and similar purposes can be regulated in accordance with the EU Directive, taking into account the possibilities for exemptions provided for in the Directive - with some states indeed feeling that those exemptions can be narrowed down further or made subject to additional formal requirements. The exemptions for these kinds of interests often cross-refer to other laws.[621] It is important to remember, though, that such other laws must also be applied in accordance with the Directive.[622] See the discussion on critical information in Chapter 3 above.

4.4.15 For a discussion regarding the restriction of the scope of the legislation in so far as scientific research and government statistics are concerned, see also Chapter 3 dealing with anonymised or de-identified information.

iv) The protection of data subjects and others

4.4.16 Article 13(1)(g) of the Directive states as follows:

> Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes necessary measures to safeguard ..... the protection of the data subject or of the rights and freedoms of others.

4.4.17 Most of the EU member states have adopted a general exception clause on the lines suggested above. [623] However, they apply different tests in this regard. In the Netherlands the same wording is used as in the Directive,[624] but the explanatory memorandum to the law stresses

---

621 Douwe Korff ***EC Study*** at 128.

622 Douwe Korff ***EC Study*** at 128.

623 Not including Belgium, France, Luxembourg and Portugal.

624 Art 43 of the Dutch Personal Data Protection Act stipulates as follows:
Responsible parties are not required to apply Articles 9(1), 30(3), 33, 34 and 35, where this is necessary in the interests of :
(a)-(d).....

that the "necessity" test should be applied strictly and only to avoid "absurd" consequences from the application of the normal rules.[625] The law in the UK contains a series of more specific exemption clauses which reflect the view of the legislator on how the balance between conflicting parties must be struck in particular contexts.[626]

4.4.18 An example of where the data subject him or herself is protected by denying him or her access to personal information is where sensitive medical or psychological information is to be conveyed and the data subject's health or mental state is such that it would be to his or her detriment if the information were conveyed directly to him or her; in other words, it would be to his or her benefit if the information were conveyed indirectly through a health professional.[627]

4.4.19 Third-party information may be linked to that of the data subject and in certain circumstances it might therefore be reasonable to prohibit access by the data subject to such information in order to protect the interests of the third party. An example is where a third party has written a confidential letter of recommendation. In certain cases it might be reasonable to withhold the name of the third party in order to encourage referees to give frank and open evaluations. [628]

b) Evaluation

4.4.20 Most commentators agreed that provision should be made for exemptions and exceptions, but argued around the degree of the threshold to be introduced. The following arguments were raised:

* Some commentators [629] referred to the possibility of using thresholds to exclude

---

(e) protecting the data subject or the rights and freedoms of other persons.

625 Korff ***Comparative Study*** at 146.

626 Sections 27- 39 of the UK Data Protection Act 1998.

627 Roos thesis at 523.

628 Roos thesis at 523.

629 Board of Health Care Funders; Momentum Health.

smaller enterprises from the operation of the Draft Bill. It was acknowledged that any thresholds need to be carefully considered in the light of the type of business being transacted as well as the sophistication of the enterprise itself. The recommendation was that, rather than removing the obligation to comply with any of the provisions of the Draft Bill, specified entities be exempt solely from complying with the administrative provisions of the Draft Bill. Such entities would then be bound by the principles embodied in the Draft Bill and would be required to comply with the detail of the legislation and subject to penalties in the event of default.

* One commentator noted [630] that it, or its public and private partners, would have to apply for certain exemptions or an exclusion in terms of inter alia section 33, but that this aspect could be addressed in due course only when the legislation has finally been promulgated.

* In one submission it was suggested that subclause 33(3) be amended to read as follows:[631]

  The Commission may impose *reasonable* conditions in respect of any authority granted under subsection (1) of this section.

4.4.21 However, one commentator[632] argued that the draft legislation fails in its inclusion of broad exemptions to the IPP it establishes and as such results in insufficient privacy protection for South Africans. See discussion on critical data. Another[633] stated that the power given to the Commission seems very much like one that should rest with the judiciary – perhaps a party can be informed of an intended intrusion and if they object or if the purpose of the intrusion requires that they are not aware of it then a designated judge must decide whether, to what extent and for how long such an intrusion is warranted.

---

630 SABRIC.

631 Banking Association.

632 Lawyers for Human Rights.

633 Contemporary Gazette(Pieter Stassen).

4.4.22 In so far as the exceptions are concerned, the Commission was referred[634] to the fact that the exception to compliance in sections 10(1)(f) and 11(2)(vi), namely the lawful interests of the responsible party or of a third party to whom the information is supplied, has not been repeated in sections 13(4)(c), 15(3)(c), and 17(5)(c). It was suggested that such a ground for non-compliance also be included there.

c) Recommendation

4.4.23 The Commission considered the submissions received and its final recommendations are as follows:

a) Provision has been made in Chapter 2 of the proposed Bill for the restriction of the scope of the Bill.[635] In terms of this chapter, the following categories of personal information have been dealt with-

(i) personal information kept in the course of a purely personal or household activity;
(ii) de-identified information;
(iii) critical information;
(iv) personal information for journalistic purposes[636];
(v) cabinet and committees, judicial functions of the courts.

b) Freedom of information is dealt with in Principle 8 of the Bill (data subject participation) as well as in the Promotion of Access to Information Act 2 of 2000.

c) Provision has been made for a number of exceptions found within the principles themselves. These exceptions can be regarded as qualifications to the Principles. See discussion of the Principles in Chapter 4 above.

---

634 Banking Association.

635 Referred to as exclusions.

636 No specific provision has been made for exemptions regarding processing of personal information for artistic or literary expression.

d) Wide provision has also been made for responsible parties[637] to approach the Commission for exemptions from specific information principles under specified circumstances. This will include processing in the public interest as well as processing necessary to safeguard the protection of data subjects or third parties.

4.4.24 The Commission therefore proposes that the legislative enactment of recommendation (d) reads as follows:

CHAPTER 4

EXEMPTIONS FROM INFORMATION PROTECTION PRINCIPLES

General

33. Processing of personal information is not in breach of an information protection principle if the processing is authorised by the Regulator in terms of section 34.

Regulator may authorise processing of personal information --

34.(1) The Regulator may authorise a responsible party to process personal information, even if that processing is in breach of an information protection principle if the Regulator is satisfied that, in the circumstances of the case -

(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from the processing; or

(b) the processing involves a clear benefit to the data subject or a third party that

637 Including both public and private bodies.

outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from the processing.

(2) The public interest referred to in subsection (1) above includes -

(a) the legitimate interests of State security;
(b) the prevention, detection and prosecution of criminal offences;
(c) important economic and financial interests of the State and other public bodies;
(d) fostering compliance with legal provisions established in the interests referred to under (b) and (c); or
(e) historical, statistical or research activity.

(3) The Regulator may impose reasonable conditions in respect of any authority granted under subsection (1) of this section.

CHAPTER 5: RIGHTS OF DATA SUBJECTS IN SPECIFIC CIRCUMSTANCES

5.1 Direct marketing and unsolicited electronic communications (SPAM)

5.1.1 Direct marketing involves the promotion and sale of goods and services directly to consumers.[1] Specific agencies exist which make lists of the addresses of individuals, usually for advertising purposes,[2] and process statistical facts on groups (for example, research by sociologists).[3] Details may be collected from many sources, including publicly available sources.[4]

5.1.2 Direct marketing, therefore, entails the communication by whatever means (including but not limited to mail, fax, telephone, on-line services) of any advertising or marketing material, which is carried out by the direct marketer itself, or on its behalf, and which is directed to particular individuals.[5]

5.1.3 It is generally accepted[6] in both Europe and the USA that an e-mail or other address constitutes personal information for the purposes of all information protection legislation. It usually entails the surname, first name and or work or home address of its owner and can relate to a

---

1 ***ALRC Discussion Paper*** at 699.

2 McQuoid-Mason 1982 ***CILSA*** at 146-147 where he states at 146: "Mail advertisements are a reminder that there are agencies somewhere about which the consumer knows nothing, but which know something about him."

3 See ***Neethling's Law of Personality*** at 294.

4 Enquiries have shown that some marketers purchase lists from list brokers or list providers without knowledge of how that data was originally compiled (which may have been with or without the consent of the data subject). Some will pull contact information from public directories, such as the white pages or from other public records such as the Deeds Office, local municipalities, SA Post Office or Telkom. Marketers may also create lists of ID numbers and addresses from public records and then ask credit bureaux to provide credit scores and or names and contact information for those ID numbers.

5 Federation of European Direct Marketing (FEDMA) ***European Code of Practice for the Use of Personal Data in Direct Marketing*** accessed at http://www.fedma.org/data-protection/ on 29 August 2008 (hereafter referred to as "***FEDMA Code")*** Approved by the EU Art 29 Working Party as fulfilling the requirements of the EU Directive in June 2003 (added on-line section to be discussed as from September 2007).

6 ***FEDMA Code*** at 3.

natural or juristic person.[7]

5.1.4 Direct marketing now accounts for the lion's share of commercial communications.[8] The statistics show that it has overtaken traditional advertising. [9]

5.1.5 However, with the rise of the Internet and electronic commerce, there is a growing concern in modern society over the unlimited harvesting and uncontrolled trading of personal information, the creation of vast information bases of personal profiles, aggressive advertising, increasing use of unfair practices and serious breaches of privacy.[10]

5.1.6 Worldwide, a distinction is therefore currently being made between the general practice of direct marketing and the more specific practice of unsolicited electronic communication, generally referred to as "spam".[11] "Spam" can be defined as the mailing[12] (mostly in bulk, sometimes repeatedly) of unsolicited e-mail or other electronic messages, usually of a commercial nature, to individuals with whom the mailer has had no previous contact and whose contact details are mostly collected from the public spaces of the Internet:[13] newsgroups, mailing lists, directories, web sites

---

7 See submission of Michalsons Attorneys on behalf of the Direct Marketing Association dated October 2005 (hereafter referred to as "First Michalsons submission") where they indicated that only sensitive information should be protected and that the name, identity number and contact information of a person should fall outside the protection provided. See the Argentina Personal Data Protection Act, 2000 where processing of similar information is excluded from the requirement of express, written consent in ordinary circumstances. It is, however, included for all other purposes.

8 SAIA indicated that, on the short-term side, insurers that are involved in database marketing are Hollard Insurance, Santam, Mutual and Federal, Standard Bank Insurance Company. On the life side, companies that are involved in direct marketing are Hollard Life; African Life; Channel Life; Metropolitan Life; Old Mutual Group Schemes; AIG Life; Absa Life; Assupol Life; Clientele Life; Liberty Active; Prosperity Insurance Co Ltd.

9 ***Unsolicited Commercial Communications and Data Protection*** at 11.

10 **Unsolicited Commercial Communications and Data Protection** at 5.

11 See submission of Michalsons Attorneys on behalf of the Direct Marketing Association dated 11 May 2007(hereafter referred to as "Second Michalsons submission") at 6 where it is stated that a distinction between electronic and ordinary marketing practices is both illogical and contrary to the interests of South African society.

12 It should, however, be recognised that not all bulk messages are spam - there are many examples of messages that are sent in high volume entirely legitimately. See OECD Task Force on Spam ***Anti-spam Regulation*** 15 November 2005 (hereafter referred to as "***OECD Anti-spam Regulation***") at 6.

13 Centre for Democracy and Technology ***Why am I Getting All this Spam? Unsolicited Commercial E-mail Research*** **Six month Report** March 2003: The greatest amount of spam received is from e-mail addresses harvested from the public Web; amount of spam received by an address posted on the Web is directly related to the amount of traffic that Web site receives; e-mail addresses harvested from the Web appear to have a relatively short "shelf life"; obscuring an e-mail address is an effective way to avoid spam; sites that publish their policies and make choice available to users generally respected those policies; domain name registration does not seem to be a major source of spam.

etc.[14]

a) Proposals in the Discussion Papers

5.1.7 In the Discussion Papers the general position regarding direct marketing was addressed as part of the Information Protection Principles in accordance with the provisions of the EU Directive[15] and the comparable position in other jurisdictions. [16] This position is still valid since it forms the basis of all direct marketing practices. The more specific example of spam was brought to the Commission's attention during the consultation process, is discussed in para (b) below, and will form part of the final recommendations in para (c).

EU Directive

5.1.8 The EU Directive establishes the basic principles for the collection, storage and use of personal information that should be respected by governments, businesses and any other organisations or individuals engaged in handling personal information.[17]

5.1.9 The position in terms of the Directive (which is technologically neutral) is as follows:[18]

---

14 **Unsolicited Commercial Communications and Data Protection** at 5; See also discussion in ***OECD Anti-spam Regulation*** at 5.

15 EU Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

16 See eg the position in the Netherlands where the code of conduct agreed to by the Privacy Commission states that personal data for marketing activities must be processed fairly by preferably collecting the information directly from the data subject and notifying the data subject of the marketing objective. Netherlands Privacy Commission ***Code of Conduct for the Processing of Personal Data by Financial Institutions*** at 8; see also the discussion of legislation in other jurisdictions at 342 below.

17 Article 6

Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

18 Article 7

1. Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or
(b) - (e) .....
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third

party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Article 10 Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11 Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

Article 12 Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

a) Explicit consent is a requirement for the processing of personal information where sensitive/special information is processed. [19] In other cases consent is only one of the possible requirements for the lawful processing of the information.

b) The Directive lays down strict rules governing the collection of personal information (specified, explicit and legitimate purpose, fair and lawful processing) and information requirements (obligation to advise individuals of their right to object to commercial use of disclosure of their information to third parties).

c) The data subject must be informed at the point of collection of the purpose for which the information will be used and the parties to which it will be disclosed. Data subjects have the right to object to the processing of their information.

d) A distinction can be made between:[20]

* customers or prospective customers who supplied their e-mail or other addresses to the sender themselves;
* individuals whose e-mail or other addresses were obtained by the sender from a third party who in turn obtained them directly from the individuals

---

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred .to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Article 14 The data subject's right to object

Member States shall grant the data subject the right:

(a) .....
(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

19 See, however, the limited exceptions to this principle set out in the Directive and in Part B of Chapter 3 of POPIA.

20 **Unsolicited Commercial Communications and Data Protection** at 97.

themselves; and

* individuals whose e-mail or other addresses were collected in a public space on the Internet (website, directory or mailing list) or in the real world without their knowledge.

e) Binding rules for both the public[21] and the private sectors are established in the Directive.

OECD

5.1.10 The OECD position, set out in two guidelines, supports the position set out in the EU Directive and reads as follows:

* The OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980) sets out eight broad internationally accepted principles to guide a harmonious approach to privacy regulation. These principles broadly correspond with the principles set out in the EU Directive 95/46/EC.

* The OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)[22] provide that business-to-consumer electronic commerce should be conducted in accordance with the recognised privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980), and taking into account the OECD Ministerial Declaration on the protection of privacy on Global Networks (1998), to provide appropriate and effective protection for consumers.

---

21 Public bodies may share information when this is done in conformity with information protection rules. Public access to information does not mean unfettered access: all Member States base their legislation on this philosophy. When personal information are made public, either by virtue of a regulation or because the data subject himself authorises it, the data subject is not deprived of protection, ipso facto and forever. He is guaranteed such protection by law in accordance with the fundamental principles of the right to privacy. In order to strike a balance between the right to privacy and the protection of personal information on the one hand and the right of the general public to access public sector information on the other, the following factors should be taken into account:

- the principle of purpose and legitimacy;
- the obligation to inform the data subject/consent;
- the data subject's right to object.

22 See also OECD ***Consumers in the On-line Marketplace: the OECD Guidelines Three Years Later*** Report by the Committee on Consumer Policy on the Guidelines for Consumer Protection in the Context of Electronic Commerce February 2003 (DSTI/CP (2002) FINAL).

Discussion Paper Bill: *general privacy provisions applicable to direct marketing*

5.1.11 Chapter 3 of the Discussion Paper Bill provides for the conditions for the lawful processing of personal information. Part A of Chapter 3 sets out the Information Protection Principles that have to be complied with. These principles are internationally regarded as accepted best practice and are technologically neutral. All the principles are equally important and have to be read together. These principles are always applicable and any other rules or regulations (including sectoral legislation and other sections in the Bill dealing with specific issues such as for eg unsolicited electronic communications) may only particularise and complement these principles. Part B of Chapter 3 deals with sensitive/special information and has to be read with Part A.[23]

5.1.12 Part A of Chapter 3 provides that consent is only one of the possible requirements for the lawful processing of the information. Part B of Chapter 3 provides that consent is a requirement for the processing of personal information where sensitive/special information is processed.[24] See, however, the exemptions to this principle set out in Part B of Chapter 3, which would have the effect that Part A would be applicable again.

5.1.13 Direct marketing would, in general, not deal with "special information" and will therefore mostly fall within the provisions of Part A. A direct marketing firm will most probably be able to argue that direct marketing is a "legitimate interest" and will therefore in this way comply with section 10(1)(f) (Principle 2) and will not need to seek consent for the processing of the information ito section 10(1)(a). Consent is, of course, always the best option.

5.1.14 The process in terms of Part A of Chapter 3 is therefore an opt-out position.

5.1.15 At this stage it is important to note what is meant by opt-in and opt-out consent in the

---

23 See also Crombie G "Spam for Breakfast, Lunch and Dinner: What will the Unsolicited Electronic Messages do for Privacy?" Minter Ellison Rudd Watts Lawyers Spam and Privacy Issues 30 March 2006 (hereafter referred to as "Crombie ***Spampape***r".

24 Section 26 and further.

context of direct marketing.[25] Under opt-in consent (also referred to as "express consent") the responsible party presents an opportunity for the data subject to express positive agreement to a stated purpose. Unless the data subject takes action to "opt-in" to the purpose - in other words, says "yes" to it - the responsible party does not assume consent. This is the strongest form of consent.[26]

5.1.16 With opt-out consent, on the other hand, the responsible party presents the data subject with an opportunity to express non-agreement to an identified purpose. Unless the data subject takes action to "opt-out" of the purpose - that is, say "no" to it - the responsible party assumes consent and proceeds with the purpose.[27]

5.1.17 The difference, therefore, lies in the question as to where the responsibility lies. With the opt-in option the responsibility is with the responsible party to obtain consent before he or she may proceed with the processing. With opt-out consent, the responsibility lies with the data subject to opt out in order to terminate processing of the information.

5.1.18 However, the sending of marketing messages also entails the prior collection of address lists and other personal information which constitutes personal information.

5.1.19 The manner in which this information is collected must also be in conformity with the rules laid down by information protection legislation. This means that the information should preferably be collected directly from the data subject. Where this is not possible, such steps should be taken as are necessary to ensure that the data subject is aware of the information being collected.

5.1.20 The Bill lays down strict rules governing the collection of personal information (specified, explicit and legitimate purpose, fair and lawful processing). This means that the data subject must be informed at the point of collection of the purpose for which the information will be used and the

---

25 See also the discussion on consent in Chapter 4, Principle 2 above.

26 Office of the Privacy Commissioner of Canada "Determining the appropriate form of consent under the Personal Protection and Electronic Documents Act" ***Fact Sheet*** accessed at http:// www.privcom.gc.ca/fs-fi/ on 25 May 2006.

27 Ibid.

parties to which it will be disclosed.[28] The data subject has the right to object on legitimate grounds. The information may furthermore not be processed for a purpose other than the originally stated purpose ,[29] such as for eg. direct marketing.

5.1.21 In general, the legitimacy of the sending of an unsolicited message therefore depends, in the first instance, on the circumstances in which the address concerned was obtained. The problems that a direct marketer may encounter in terms of Chapter 3 of POPIA will therefore focus on the circumstances in which the addresses are initially collected rather than on the conditions on which they may legitimately be sent.

5.1.22 The Information Protection Principles ensure that a legitimate business that has collected personal information for a specific purpose will not be able to spam or be involved in spamming activities. If it did, a breach would be quite easy to establish and would likely present a serious publicity problem for the business. However, it should be noted that spam is not something that typically comes from a legitimate business. [30]

5.1.23 It would be unlawful to process the personal information of individuals whose e-mail or other addresses are collected in a public space on the Internet (website, directory or mailing list) or in the real world without their knowledge.[31] See also discussion below on directories.

Sectoral legislation

5.1.24 Note should also be taken of other legislation dealing with aspects of direct marketing:

(i) Electronic Communications and Transactions Act 25 of 2002

---

28 Section 12 and 13 of POPIA, Principle 3.

29 Section 15 of POPIA, Principle 4.

30 Crombie ***Spam paper*** para 3.4. and 3.5 at 3.

31 E-mail harvesting is unlawful under the general 95/46/EU Directive. It constitutes unfair processing of personal data and respects neither the purpose limitation principle nor the obligation of information collection. See European Union Article 29 Data Working Party Opinion 5/2004 on Unsolicited Communication for Marketing Purposes under Article 13 of Directive 2002/58/EC WP90 11601/EN adopted on 27 February 2004 (hereafter referred to as "Art 29 Opinion 5/2004") at 6.

5.1.25 The position regarding unsolicited communication is set out in section 45. It makes provision for the so-called opt-out option.[32] Advertisers must give consumers the option of being removed from their mailing lists. If they still bombard people with communications despite being asked not to, they will be guilty of a criminal offence and risk a fine or jail term.

(ii) Electronic Communications Act 36 of 2005

5.1.26 Section 75 corresponds with section 89A of the Telecommunications Amendment Act 103 of 1996 which TELKOM has apparently used in the past to prohibit the electronic access to the phone directories for marketing purposes.[33]

(iii) National Credit Act 34 of 2005

---

32 **45 Unsolicited goods, services or communications**

(1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer-
(a) with the option to cancel his or her subscription to the mailing list of that person; and
(b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89 (1).

(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89 (1).

33 Section 75 of the Electronic Communications Act 36 of 2005 reads as follows:

75. Directory services

The Authority may prescribe or impose through licence conditions, as the case may be, measures in respect of directories and directory enquiry services, regarding-

(a) the protection of personal data;
(b) the protection of privacy;
(c) language preferences;
(d) the prevention of fraud;
(e) the prohibition of marketing and unfair trading practices;
(f) the provision of assistance to security services or other public safety officials;
(g) related charges;
(h) the establishment of a national directory information database;
(i) the availability of a directory; and
(j) such other related matters as the Authority may determine.

5.1.27 The National Credit Act makes provision in section 74 for an opt-out option for consumers when entering into a credit agreement.[34]

b) Evaluation

5.1.28 During the consultation phase the Commission was referred to the fact that countries worldwide have recently put in place specific regulatory measures for unsolicited bulk e-mail and other electronic messaging (spam).

5.1.29 E-mail is an extremely important and effective means of communications and is used by millions of people on a daily basis for personal and commerial purposes.[35] Its low cost and global reach offer unique opportunities for the development and growth of commerce.[36] Its convenience

---

34 **74 Negative option marketing and opting out requirements**

(1) A credit provider must not make an offer to enter into a credit agreement, or induce a person to enter into a credit agreement, on the basis that the agreement will automatically come into existence unless the consumer declines the offer.

(2) Subject to section 119 (4), a credit provider must not make an offer to increase the credit limit under a credit facility, or induce a person to accept such an increase, on the basis that the limit will automatically be increased unless the consumer declines the offer.

(3) A credit provider must not make a proposal to alter or amend a credit agreement, or induce a person to accept such an alteration or amendment, on the basis that the alteration or amendment will automatically take effect unless the consumer rejects the proposal, except to the extent contemplated in section 104, 116 (a), 118 (3) or 119 (4).

(4) A credit agreement purportedly entered into as a result of an offer or proposal contemplated in subsection (1), is an unlawful agreement and void to the extent provided for in section 89.

(5) A provision of a credit agreement purportedly entered into as a result of an offer or proposal contemplated in subsection (2) or (3) is an unlawful provision and void to the extent provided for in section 90.

(6) When entering into a credit agreement, the credit provider must present to the consumer a statement of the following options and afford the consumer an opportunity to select any of those options:
(a) To decline the option of pre-approved annual credit limit increases as provided for in section 119 (4), if the agreement is a credit facility; and
(b) to be excluded from any-
(i) telemarketing campaign that may be conducted by or on behalf of the credit provider;
(ii) marketing or customer list that may be sold or distributed by the credit provider, other than as required by this Act; or
(iii) any mass distribution of email or sms messages.

(7) A credit provider-
(a) must maintain a register in the prescribed manner and form of all options selected by consumers in terms of subsection (6); and
(b) must not act in a manner contrary to an option selected by a consumer in terms of subsection (6).
[Date of commencement of s. 74: 1 June 2007.]

35 Office of the Press Secretary The White House ***Fact Sheet: President Bush Signs Anti-SpamLaw*** 16 December 2003.

36 Congressional findings and policy ***Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003*** 15 U.S.C. 7701-7713 at par 1.

and efficiency, however, are increasingly threatened by the rise in spam. Spam currently accounts for over half of all-email traffic.[37]

5.1.30 Spam thrives for one major reason - the costs incurred by the spammer sending the spam are extremely low. In contrast, the costs incurred by an ISP, a business or an individual to receive, store and download spam far outstrip the costs incurred by the spammer.[38] Traditional off-line marketing methods, such as bulk postal mail and telemarketing, are based on a sender pays model, where the sender bears all the costs, and the cost to the recipient of this advertising is negligible.[39]

5.1.31 It should be noted that the main impacts of unsolicited electronic marketing and promotional messages are economic and consumer related.[40] It is for this reason that many countries deal with spam in specific legislation distinct from their privacy legislation.[41] However, it is an accepted fact that there is also a privacy dimension in the collecting and using of information for purposes not agreed to by the data subject and certain harmful aspects of personal information handling (such as misleading conduct in the collection and use of personal information). Regulation of spam will, therefore, bring many privacy benefits, including a possible reduction in identity theft and other forms of identity fraud.[42] Anti-spam legislation has therefore been introduced as part of the privacy laws in most European countries.

---

37 White House ***Fact Sheet*** supra; see also US Senate Republican Policy Committee **Legislative Notice** No 43 October 22, 2003 and its reference at 3 to an April 2003 Federal Trade Commission (FTC) report entitled "False Claims in Spam" where it was stated that 66 percent of all spam contains some kind of false, fraudulent or misleading information, either in the e-mail's routing information, its subject line, or the body of the message. The FTC also found that get-rich-quick opportunities and pornographic or adult-oriented material accounted for 38 percent of all spam (hereafter referred to as "***Legislative Notice 43***").

38 In ***Legislative Notice 43*** reference was furthermore made to the Radical Group's estimates in 2004 that, on a worldwide basis, spam could cost corporations over $113 billion by 2007; See also Crombie ***Spam paper*** at par 2.3 and 2.6 and the reference to the Information Technology Minister of New Zealand, David Cuncliffe who referred to spam, at the first reading of the Unsolicited Electronic Messages Bill, as "a drain on the business and personal productivity of New Zealanders".

39 OECD Task Force on Spam ***Spam Issues in Developing Countries*** 26 May 2005 (hereafter referred to as ***"OECD Spam Issues, Developing Countries")*** at 6.

40 See Second Michalsons submission where it was stated that a prohibition against unsolicited electronic communications cannot logically be grounded in a right to privacy of personal information.

41 See discussion on legislation in other jurisdictions below.

42 Office of the Privacy Commissioner of New Zealand ***Report to the Minister of Justice in Relation to the Unsolicited Electronic Messages Bill*** 3 April 2006 at 1.

Additional EU Directives

5.1.32 There are a number of relevant EU Directives dealing specifically with or relevant to the regulation of unsolicited electronic communications/spam.

5.1.33 Recital 5 of EU Directive 2002/21/EC[43] provides that the convergence of the telecommunications, media and information technology sectors means all transmission networks and services should be covered by a single regulatory framework. That regulatory framework consists of this Directive and four other specific Directives.[44]

5.1.34 The importance of this Directive for our discussion is the fact that the definitions set out in this Directive - together with those in Directive 95/46/EC - are applied everywhere else. See, for instance, in this regard the definition of “communication” and “electronic mail”.

5.1.35 Provision was also made for opt-out registers in Directive 2000/31/EC.[45] Service providers undertaking unsolicited commercial communications are obligated to consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.This provision was made applicable to legal persons as well by Directive 2002/58/EC. [46]

5.1.36 Between May and October 2000 the EU undertook a comprehensive survey of European industry federations in order to identify all the private sector initiatives which had been or were being undertaken in member states. It was found that opt-out lists were being set up in the UK, Germany, the Netherlands, Spain, Norway, Sweden, Finland and Italy. The UK’s direct marketing

---

43 EU Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, 25 June 2002.

44 EU Directives 2002/20/EC, 2002/19/EC, 2002/22/EC and 2002/58/EC.

45 EU Directive 2000/31/EC on Electronic Commerce.

46 See the discussion on the position regarding an opt-out register in the Consumer Protection BIll.

association has joined with the American DMA to build a joint register. [47]

5.1.37 Finally, the EU Directive 2002/58/EC[48] reflects continuing technological developments in telecommunications and other electronic services and provides an equal level of privacy protection to personal information regardless of the technologies used to provide the services. It repeals and replaces Directive 97/66/EC of 15 December 1997. It translates the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector.

5.1.38 In so far as public directories are concerned, the Directive provides as follows:

* Member States shall ensure that subscribers to electronic communications services are informed, free of charge and before they are included in a printed or electronic directory that is available to the public or obtainable through directory inquiry services, of the possible uses that may be made of such directories.[49]
* Subscribers have the right to determine whether they are listed in a public directory. They also have the right, free of charge, to verify, correct, or withdraw personal information listed in a directory.[50]
* If personal information will be shared, subscribers should be informed of the possibility that their personal information may be transmitted to one or more third parties. The subscriber should be informed of the recipients or possible categories of recipients.[51]
* Article 12 does not apply to directories already printed. Where personal information of fixed line or mobile telephone subscribers is included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and Article 11 of

---

47 **Unsolicited Commercial Communications and Data Protection** at 4.

48 EU Directive 2002/58/EC on Privacy Protection in the Electronic Communications Sector.

49 See Article 12(1) and Recitals 38 & 39.

50 See Article 12(2).

51 See Recital 39.

Directive 97/66/EC before national legislation implementing the new Directive becomes effective, the personal information of such subscribers may remain in the public directory (including versions with reverse search functions) unless subscribers indicate otherwise.[52]

5.1.39 With regard to unsolicited communications for direct marketing the Directive:

* Adopts an opt-in approach to unsolicited commercial e-mail. The new standard provides that the use of electronic mail, automatic calling machines or facsimile machines for the purposes of direct marketing may be allowed only with subscribers who have given their prior consent.[53] Any message by electronic communications where the simultaneous participation of the sender and the recipient is not required is covered by this concept of electronic mail.[54]

* For (fixed and mobile) voice telephony marketing calls, other than via automated calling machines, a choice is possible between an opt-in and opt-out system.[55]

* A company that has obtained electronic contact details (in accordance with Directive 95/46/EC) within the context of an existing customer relationship may use that information to offer users its own similar products or services. Consumers, however, must have the right to object, free of charge and in an easy manner, to receiving such materials.[56]

* Consent of a user or subscriber as used in this directive is defined in the same manner as used in Directive 95/46/EC. Generally, consent may be provided by any appropriate method that indicates "a freely given specific and informed indication of the user's wishes, including by checking a box when visiting an Internet web site."[57]

---

52 Article 16.

53 Lists which have not been established according to the prior consent requirement may, in pinciple, not be used anymore under the opt-in regime, at least until they have been adapted to the new requirements. Selling such incompatible lists to third parties is not legal either. See ***Article 29 Working Party Opinion 5/2004*** at 6.

54 ***Article 29 Working Party Opinion 5/2004*** at 4.

55 Para 3 of Article 13 of Directive 2002/58/EC.

56 See Recital 41 and Article 13(2).

57 See Recital 17.

* The Directive prohibits sending direct marketing e-mails that disguise or conceal the identity of the sender, or that do not include a valid address to which the recipient may send a request that such communications cease. This requirement is necessary in order to facilitate effective enforcement of the rule on unsolicited messages.[58]

* As regards "cookies" the Directive adopts an opt-out approach, specifying that cookies cannot be used unless users have been provided with clear and precise information on their purposes and the opportunity to refuse them.

* The Directive states that Governments may require service providers to retain traffic data (transactional information, not content) associated with the communications of their subscribers so that it would be available if subsequently requested for law enforcement and national security purposes. The Directive makes it clear that such data retention requirements can be imposed only by national legislation and only when such requirements constitute "a necessary, appropriate, and proportionate measure within a democratic society".[59]

* Member states must ensure that the legitimate interests of legal persons, over and above those of natural persons, are sufficiently protected, but they remain free to determine the appropriate safeguards to do so.[60]

Direct marketing legislation in other jurisdictions

5.1.40 In the EU countries enforcement of the EU Directives lies with the Member States. Many EU countries have chosen to introduce anti-spam legislation within the framework of modifications of privacy and data protection laws.[61] The Directives require that infringement penalties and

---

58 See Article13 (4).

59 Global Internet Policy Initiative **EU Directive on Privacy Protection in the Electronic Communications Sector** October 2002 (accessed at http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/spamstudy-en.pdf on 16 August 2007) at 2.

60 Paragraph 5 of Article 13.

61 See eg the UK Privacy and Electronic Communications Regulations, 2003; See also the UK Direct Marketing Association code of practice for e-mail marketing at www.dma.org.uk/content/Pro-BestPractice.asp/.

remedies must be in place and that individual rights to judicial remedy and compensation for damages must be provided.[62]

5.1.41 In the USA the CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act)[63] applies to e-mail which primary purpose is advertising or promotion of a commercial product or service. The CAN-SPAM Act prohibits deceptive subject lines, failure to provide an opt-out method and honour opt-out requests, failure to include a valid physical postal address and, for sexually explicit messages, failure to include a warning label.[64] Enforcement of the Act is primarily the responsibility of the Federal Trade Commission (FTC) as well as the Department of Justice (DoJ) as regards criminal sanctions.[65]

5.1.42 The Australian Spam Act 2003 is consent-based legislation that covers commercial electronic meassages including e-mail, SMS and mobile messaging. Enforcement is undertaken by the Australian Communications and Media Authority (ACMA) which has the power to send formal warnings, issue fines and undertake court actions in respect of breaches of the Act.[66]

5.1.43 The Act on Promotion of Information and Communications Network Utilisation and Information protection in Korea prohibits the transmission of spam.The approaches are blended into the Act by requiring an expressed consent for sending an electronic commercial advertisement to phones or fax, while applying opt-out consent for e-mail messages in general.[67]

---

62 ***OECD Anti-Spam Regulation*** at 34.

63 117 Stat. 2699 Public Law 108-187, December 16 2003.

64 See eg Los Angeles Times May 14 2008: "My Space wins $234-million judgment over junk messages".The popular on-line hangout My Space has won a $234 million judgment over junk messages sent to its members in what is believed to be the largest anti-spam award so far.

65 ***OECD Anti-Spam Regulation*** at 35; ***Legislative Notice 43*** at 1; See criticism of CAN-SPAM Act: regarded as a serious failure of the United States Government to understand the spam problem as it attempts to regulate rather than ban the practice of spamming. "Spamhaus Position on CAN-SPAM Act of 2003 December 2003 accessed at http://www.spamhaus.org/position/CAN-SPAM Act 2003.html at 12 June 2007.

66 ***OECD Anti-Spam Regulation*** at 34.

67 ***OECD Anti-Spam Regulation*** at 35.

5.1.44 In New Zealand the Unsolicited Electronic Messages Act, 2007[68] is consent-based legislation and has as its aim the promotion of responsible use of electronic messages. The Act provides for civil, rather than criminal penalities, for breach. The maximum penalty that the High Court may impose is $200,000 for an individual and $500,000 for an organisation. The Act is designed to be part of a multi-pronged attack on spam. It will be an effective tool alongside other intiatives such as codes of practice,[69] industry guidelines, technical measures and education campaigns.[70]

5.1.45 In studying the Directives and developments in other countries it is clear that POPIA would not be effective, on its own, to prevent spam.[71] Generally, however, businesses whose e-mail practices abide by the privacy legislation will largely already comply with the provision of the new EU Directive. [72] See, however, the distinction in emphasis between opt-in and opt-out consent set out above.

Regulation of spam in developing countries

5.1.46 It is interesting, for South Africa, to note that the OECD has studied the problems of spam specific to developing economies, its impact on these economies, and suggested means and measures that can be taken to mitigate the impact of spam on developing countries.[73]

5.1.47 In the OECD area 23 countries have implemented spam legislation. Many developing

---

68 Royal assent on 5 March 2007, came into force on 5 September 2007.

69 See eg Internet Service Providers Spam Code of Practice ***A Code for Internet Service Providers Providing E-mail Services*** May 2007. The Act adresses the spam problem principally by targeting senders of spam. However, since senders of spam require the services of Service Providers in order to send their spam, enlisting the support of those Service Providers has the potential to be an efficient and pro-active way of addressing the spam problem.

70 Crombie ***Spam paper*** at 8.

71 See Crombie ***SpamPaper*** at 3.

72 Crombie ***Spam paper*** at 8.

73 ***OECD Spam Issues, Developing Countries*** at 4.

countries have yet to consider adopting legislation against spam. [74]

5.1.48 The OECD found[75] that spam is a much more serious issue in developing countries than in the developed world, as it is a heavy drain on resources that are scarcer and costlier in developing countries than elsewhere. ISP's and network providers in developing countries lack the capacity and resources to deal with sudden surges in spam that occur from time to time, and this often causes their mail servers to break down or function at a sub-optimal level. Indeed, their capacity to cope with even normal (though fairly high) levels of spam is much weakened because resources such as hardware, bandwidth and software licences tend to cost much more as a percentage of a developing country's ISP budget. Similarly, end users, both consumers and business, may lack knowledge of potential resources available to them to take effective action, and even those resources that they do have available, cost relatively more. [76]

5.1.49 These problems experienced in developing countries are exacerbated by the fact that spammers - for whom it has become difficult or too risky operating from the United States or Europe - may decide to "migrate" to developing countries,[77] where they know they can enjoy a certain degree of impunity.[78]

Cross-border regulation of spam[79]

5.1.50 It should further be noted that spam may originate in one country, but it may have an impact in a number of other countries where recipients of spam reside. This has lead to a growing volume

---

74 ***OECD Spam Issues, Developing Countries*** at 14.

75 ***OECD Spam Issues, Developing Countries*** at 4.

76 These factors also reflect the deep concern felt by representatives of developing countries, and strongly expressed at the ITU/WSIS Thematic Meeting on Spam held in Geneva in July 2004 about how spam and net abuse were bleeding the Internet economy in their countries of scarce and costly bandwidth.

77 Shift base or outsource to a local spammer.

78 ***OECD Spam Issues, Developing Countries*** at 30.

79 OECD ***Draft Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Against Spam*** C (2006) 57 31 March 2006.

of cross-border complaints and investigations on spam and spam-related threats.

5.1.51 In April 2004 the OECD appointed a joint Task Force on Spam[80] which, inter alia, identified cross-border co-operation in the enforcement of legislation against spam as a fundamental in the development of an effective international enforcement framework. They recommended that member countries should:

a) establish a domestic framework by, inter alia, introducing and maintaining an effective framework of laws, spam enforcement authorities and practices for the enforcement of laws connected with spam;

b) improve the ability of their authorities to co-operate with foreign spam enforcement authorities by sharing information and providing investigative assistance;

c) improve procedures for co-operation by making use of common resources, international networks and existing law enforcement instruments; and

d) cooperate with relevant private sector entities.[81]

5.1.52 In the absence of formal multilateral civil enforcement agreements, several anti-spam regulators have agreed on a broad co-operative framework, the "London Action Plan".[82] Co-operation is enhanced where national legislation is broadly consistent between countries.[83]

Consumer Protection Bill

---

80 In view of the potential for economic and social harm caused by spam, and the potential for further problems as a result of the convergence of communications technologies and the emergence of ubiquitous communications and a mobile Internet the OECD decided to create a horisontal ad hoc "joint ICCP-CCP Task Force on Spam" in April 2004 in order to develop a policy framework.

81 See also ***OECD Anti-Spam Regulation*** at 9 reiterating that, firstly, a country needs robust and effective domestic anti-spam measures and secondly, partnerships and mutual agreements with other countries.

82 Information on the London Action Plan is available at e-com.ic.gc.ca/epic//inecicceans.nsf/vwapj/.

83 ***OECD Anti-spam Regulation*** at 30.

5.1.53 In South Africa a Consumer Protection Bill[84] has been developed by the Department of Trade and Industry. The initial draft of the Bill contained sections regulating the conduct of business with regards to the collection, collation and distribution of personal information.[85] Following discussions between the Department and the Commission it was agreed that clause 11 would be deleted, as these aspects would be better regulated in POPIA. Clause 11 in its entirety has been deleted from the Bill.

5.1.54 The final draft of the Bill now contains minimal protection relating to the rights of consumers in relation to unwanted or unsolicited direct marketing. The revised Bill provides for various opt-out mechanisms for the consumer.[86] This is in accordance with the general privacy principles set out in EU Directive 1995/46/EC. The Bill does not, in any way, deal with the collection, retention and distribution of personal information and there is, therefore, no overlap with POPIA. The Dti has indicated its support of the spirit and content of POPIA as it is aligned with the objectives of the

---

84 B 19-2008 as introduced in the National Council of Provinces; explanatory summary of Bill published in the Government Gazette No 31027 of 5 May 2008.

85 Clause 11 of Part B of Chapter 2 – Consumers' Right to Privacy.

86 The new Clause 11 of the new draft of the Bill now reads as follows:

Right to restrict unwanted direct marketing

11.(1) The right of every person to privacy includes the right to -
(a) refuse to accept;
(b) require another person to discontinue;
(c) in the case of an approach other than in person, to pre-emptively block,

any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing.

(2) To facilitate the realisation of each consumer's right to privacy, and to enable consumers to efficiently protect themselves against the activities contemplated in subsection (1), a person who has been approached for the purpose of direct marketing may demand during or within a reasonable time after the communication that the persons responsible for initiating the communication desist from initiating any further communication.

(3) The Commission may establish, or recognise as authoritative, a registry in which any person may register a pre-emptive block, either generally or for specific purposes, against any communication that is primarily for the purpose of direct marketing.

(4) A person authorizing, directing or conducting any direct marketing -
(a) must implement appropriate procedures to facilitate the receipt of demands contemplated in subsection (2); and
(b) must not direct or permit any person associated with that activity to direct or deliver any communication for the purpose of direct marketing to a person who has -
  (i) made a demand contemplated in subsection (2); or
  (ii) registered a relevant pre-emptive block as contemplated in subsection (3).

(5) No person may charge a consumer a fee for making a demand in terms of subsection (2) or registering a pre-emptive block as contemplated in subsection (3).
(6) The Minister may prescribe regulations for the operation of a registry contemplated in subsection (3).

Consumer Protection Bill.[87]

Proposed regulation of unsolicited electronic communications in terms of POPIA

5.1.55 The new position regarding the regulation of unsolicited electronic communications as set out in POPIA is only applicable to automated calling machines, faxes, electronic mails and SMS's used for direct marketing:[88]

5.1.56 In the case of automated calling machines, faxes or electronic mails, including SMS's, consent has to be given by subscribers prior to their personal information being used for the purposes of direct marketing (this is a new stricter opt-in position).

5.1.57 However, consent is not required for existing customers, subject to the obligation to offer an opt-out possibility, on collection of the information and again in each and every message sent, using the same communication service.

5.1.58 For fixed and mobile person-to -person voice telephony marketing calls, other than via automated calling machines, the ordinary rules set out in Part A of Chapter 3 of the Bill above will apply.[89]

5.1.59 The sender on whose behalf an electronic communication is made may not conceal or disguise its identity.

5.1.60 Public bodies may share personal information when this is done in conformity with the

---

87 Written submission by the Department of Trade and Industry on POPIA received in November 2007.

88 See section 66 of POPIA below.

89 See also the Consumer Protection Bill above.

information protection principles.[90] See discussion above.

5.1.61 In order to strike a balance between the right to privacy and the protection of personal information, on the one hand, and the right of the general public to access public sector information, on the other, the following factors should be taken into account:

- the principle of purpose and legitimacy;
- the obligation to inform the data subject/consent;
- the data subject's right to object.

5.1.62 Subscribers to electronic communications services must be informed, free of charge and before they are included in a printed or electronic directory that is available to the public or obtainable through directory inquiry services, of the possible uses that may be made of such directories.[91] (Please note, however, that this section is in conformity with the information protection principles set out in Part A of Chapter 3 of the Bill and strictly speaking need not be referred to specifically.)

5.1.63 Subscribers have the right to determine whether they are listed in a public directory. They also have the right to verify, correct, or withdraw personal information listed in a directory.

5.1.64 If personal information will be shared, subscribers should be informed of the possibility that their personal information may be transmitted to one or more third parties. The subscriber should be informed of the recipients or possible categories of recipients.

5.1.65 Section 96 does not apply to directories already printed. Where personal information of fixed line or mobile telephone subscribers is included in a public subscriber directory in conformity with

---

90 See discussion on public registers in Chapter 3 above.

91 See section 67 of POPIA.

the information principles before national legislation implementing the new Directive becomes effective, the personal information of such subscribers may remain in the public directory (including versions with reverse search functions) unless subscribers indicate otherwise.[92]

5.1.66 In conclusion, it should therefore be noted that, in order to address the problems created by spam, a diverse strategy must be employed consisting of five complementary elements: strong, effective domestic legislation, education of end users; action by the e-marketing and Service Provider industries; technological solutions, and, finally, international cooperative efforts.[93]

Written comments received on the Discussion Paper Bill and on the amended direct marketing provisions

5.1.67 During the consultation process the Commission received a number of written submissions. Some commentators argued for strict regulation of direct marketing practices while others emphasised the importance of direct marketing for the economy and wanted no regulation at all. There was agreement that direct marketing could be of assistance to consumers if carried out properly.[94]

5.1.68 It was argued that the selling of mailing lists should be prohibited. The selling of these lists is a gross violation of the individuals whose name and information appears on such lists.[95]

5.1.69 Support was expressed[96] for the implementation of an opt-in rather than an opt-out approach which would improve the fairly rudimentary anti-spam provisions contained in the Electronic

---

92 As stated above section 75 of the ECT Act corresponds to section 89A of the Telecommunications Amendment Act 103 of 1996 on which TELKOM has based its prohibition of the electronic access to the telephone directories for marketing purposes.

93 Internet Service Providers Spam Code of Practice May 2007 at 2.

94 See also ***ALRC Discussion paper*** at 702.

95 JD Enracht-Moony.

96 Law Society of South Africa.

Communications and Transactions Act of 2002. Spam is a much bigger problem now than it was when that Act was being drafted and tighter control of the use of personal data is therefore now necessary. A reported proposal that the Post Office should be allowed to sell all information it held for telephone directory purposes to any bidder, whenever it wished, must not be allowed to happen.

5.1.70 The Commission was referred to a comment written by David Harris against allowing opt-out consent in this context . His argument is simple (and has been used by others as well) that by legitimising opt-out it becomes an acceptable option for business to send unsolicited marketing material as long as they allow recipients to opt-out. This can potentially require so much effort from the recipient, that the recipient can be effectively overwhelmed by the number of received e-mails.[9798]

5.1.71 It was argued that rules should be put in place, whether in the Bill itself or in regulations to the Bill, or within the relevant codes of conduct, to ensure that the allowance for implied consent and "opt out" abilities are kept in check, particularly in the case of this leading to spamming and excessive direct marketing activities. It was noted that the notion of ensuring informed consent is also supported. As an example, a consumer should be aware of the fact that he is agreeing to allowing a bank to share his or her information with its insurance business and financial planning affiliated companies, and not for the benefit of a whole range of unrelated services, for example, travel services, IT services or for the sale of household products. Having said this, it was submitted that these concerns would be addressed by the purpose specification and further processing principles.[99]

---

97 Prof Martin Olivier.

98 Another example referred to by Prof Olivier, is that it is currently possible to opt-out of cookie-collection by DoubleClick — one of the largest collectors of web-related consumer behaviour. However, most consumers will neither be able to establish how to opt-out, nor understand the technology involved to opt-out (and therefore find it hard to establish whether opting out is a safe proposition). Worse, one can just imagine the effort required to locate and opt-out of all such services. And it is hard to imagine what new services will be established in future; again expecting the consumer to keep abreast of such new services and opting out of each is unrealistic. It was suggested that the possibility to opt-out is not a valid form of consent for any ‘service’ that directly affects the consumer, such as sending unsolicited bulk e-mail. The case where it potentially has an indirect effect on consumers — such as when tracking cookies are placed on a user’s disk — is more problematic and needs serious discussion to attempt to identify (and delineate) those few cases where allowing opt-out as a form of consent does indeed warrant consideration.

99 Nedbank.

5.1.72 It was noted that the problem of spam marketing is on the increase in South Africa and it was strongly suggested that this Bill deals with this issue, by narrowing the wording of the Principles and other sections in the Bill to make it clear that unsolicited marketing is not allowed without specific data subject consent.[100]

5.1.73 The Commission was referred[101] to the fact that the government, and more specifically, the DTI, has made a strategic decision to promote call centres[102] within South Africa and offers a number of incentives to attract call centre business to South Africa. In order to achieve this, the government offers a cash grant to local and foreign investors investing in a call centre in terms of the Small and Medium Enterprise Development Program. In addition, there are tax breaks for companies that take on learnerships through the Services Sector Education and Training Authority (SETA). The Commission was requested to determine the impact of the legislation on this new business opportunity.

5.1.74 Commentators in favour of the opt-out system suggested that a further subsection should be included which renders the processing of existing lists of data lawful, provided it meets specific requirements. This would prevent lists which have been lawfully collected and processed over many years, which may even form a significant part of businesses, to be classified as unlawful although it may meet the requirements set out in clause 9 of the Bill.[103]

5.1.75 Both the life and short-term insurance industry indicated that they have been involved in

---

100 Nedbank.

101 SAIA; Foschini's; First Michalsons submission.

102 A call centre is a centralised office used for the purpose of receiving and transmitting a large volume of requests by telephone. It is operated by a company to administer incoming product support or information inquiries from consumers. Outgoing calls for telemarketing, clientele and debt collection are also made. Increasingly, the voice and data pathways into the centre are linked through a set of new technologies called computer telephony integration (CTI). Most major businesses use call centres to interact with their customers. The relatively high cost of personnel and worker inefficiency accounts for the majority of call centre operating expenses, influencing outsourcing to other countries in the call centre industry. India, Malaysia and the Philippines are examples of countries where outsourcing has taken place. South Africa is emerging as a new call centre location. Factors such as relatively low labour costs, cultural affinity, good English and communication skills and reliable infrastructure have contributed to this development McKinsey & Co has predicted that South Africa could attract a significant portion of international business and in so doing could create upwards on 100000 new, sustainable call centre /BPO jobs. See McKinsy & Company, South Africa "Calling: South Africa's Global Business Process Outsourcing & Offshoring Opportunity Headline Report" June 2005. In order to make full use of outsourcing business, South Africa will, however, have to obtain an EU adequacy rating.

103 Telkom SA Ltd.

direct marketing activities for a number of years, offering value for money, simple products, largely to the lower end of the insurance market. Direct marketing initiatives generally target those consumers that are not serviced by the broker market, as the monetary value of the policies is too low to pay for the broker's cost of operations. In order to reach this target market, insurance companies make use of a variety of databases that are available to be purchased from database owners that have legally compiled these databases from a variety of sources such as census data, Telkom data etc. Outbound telemarketing or direct mail is used as the distribution channel and the impact of new legislation should be considered carefully.[104]

5.1.76 It was argued that responsible parties currently involved in direct marketing would no longer be able to source new clients from existing consumer or affinity databases, where consent from the data subject has not been obtained and this would therefore have a severe impact on the insurance direct marketing industry. [105]

5.1.77 The Commission was referred to the fact that marketing in a business environment is different to marketing aimed at consumers. Firstly, since businesses are both recipients and senders of marketing material, and as businesses do not ordinarily "shop" for products, business to business transactions are very dependent on marketing. There are, furthermore, natural persons who are decision makers within businesses that need to be marketed to as well. The Bill needs to take cognisance of the difference between business to business and business to consumer marketing.[106]

5.1.78 One commentator[107] proposed that a further subsection should be included in clause 9 of the Discussion Paper Bill (Principle 1: processing limitation) to read as follows:

> Personal information may only be processed if the -
> (a)-(h)....
> (i) Processing is related to the legitimate conveyance of commercial information and where the recipient is given an option to remove his or her contact details from the contact directory or contact list of the conveyer of the information and to receive, on

---

104 SAIA.

105 LOA; Premier Group.

106 Credit Bureau Association.

107 Foschini's.

request, the identifying particulars of the source from which that person's personal information was obtained.

It was furthermore suggested that failure to comply with the above sub-section (i) be made into an offence and, on conviction, subject to a fine or imprisonment in terms of section 9(1)(b) of the Discussion Paper Bill.

5.1.79 It was submitted that an opt-out approach represents a proportional balance between protecting a consumer's privacy and the reality of modern business marketing strategies. It was, furthermore, stated that this approach is similar to the approach suggested in Article 14 of the EU Directive in respect of the data subject's right to object.[108] A consumer should be able to opt out at any time subject to reasonable limits, eg. giving the company reasonable time to make the opt out effective.[109]

5.1.80 It was, however, noted that the question about opt-in *versus* opt-out forms of consent is one that has become particularly pressing, given the recent developments in legislation about spam worldwide.[110] [111]

5.1.81 The view was expressed that the combination of an opt-out mechanisms in respect of electronic communications together with a pre-emptive block mechanism against unsolicited telephonic communications specifically would constitute a sufficient and adequate means of controlling any potential nuisance of unsolicited commercial communications.[112]

5.1.82 It was submitted that direct electronic marketing to new customers has proven to be one of

---

108 A specific right to object is laid down in some data protection laws. The EU Directive contains important instances of such a right, namely in Art 14 (a) (right to object to data processing generally), Art 14(b) (right to object to direct marketing) and, most innovatively, Art 15 (1) (right to object to decisions based on fully automated assessments of one's personal character). These rights to object are not found in other main international data protection instruments; See Chapter 11 of the Bill dealing with the rights of the data subject.(See however, the ILO Code of Practice on Protection of Workers' Personal Data). Neither have they existed in the bulk of national laws though this situation no longer pertains in Europe due to the adoption of the Directive; Bygrave ***Data Protection*** at 66.

109 Sanlam Life; Legal Service.

110 See discussion on direct marketing below.

111 Prof Martin Olivier.

112 Second Michalsons submission at 11.

the most effective ways for a business to distribute information regarding its products or services to consumers for the purpose of raising consumer awareness and for generating sales. Direct marketing is an effective and relatively low cost means of generating sales.[113]

5.1.83 It was argued[114] that the opt-in requirements be limited to automatic calling machines only as this is the only instance where a consumer would find it impossible to opt out, thus being continually subjected to unsolicited calls.

5.1.84 The Commission was referred to the fact that, with the growth in the cellular market, especially the pre-paid market, Access Products can effectively be offered to this market via telemarketing.[115] The advantages are:

* This is a cost effective method of marketing. Agents and brokers are not able to cost effectively service this market.
* Telemarketing enables all calls to be voice recorded ensuring that all the FAIS regulations are adhered to and that the financially uneducated market receives good service.
* It enables insurers to contact the market, which may not have access to information as they may be in rural areas.
* It enables products to be explained in a mother tongue and also enables products to be offered to a segment that may still be illiterate or semi-illiterate. This should therefore increase the overall understanding of the product purchased.
* In terms of the Financial Services Charter, the insurer also needs to establish which clients fall within the lower income bracket and this can largely only be achieved by matching the existing databases against census data and other public records. However, in terms of the privacy laws, this may not be permitted, as this would mean processing information without the data subjects consent.

---

113 Ibid.

114 Department of Trade and Industry.

115 SAIA; LOA.

5.1.85 It is the stated object of the Direct Marketing Association[116] to create a balance of interest between the rights of the industry and the rights of the individual. The industry's position is that businesses have the right to collect and use information about their clients and prospects, provided that process is transparent, legitimate and fair, and the individual's right to privacy and choice is respected and protected.[117]

5.1.86 Finally, the argument was put forward that the broad definitions of "personal information" and "processing" and the restrictions on the processing of personal information in terms of the principles entailed overly broad limitations on the Constitutional rights of responsible parties to freedom of trade, freedom of expression and access to information. [118]

c) Recommendation

5.1.87 The Commission has evaluated the comments received and recommends that a

---

116 The Direct Marketing Association is a non-profit trade association representing all stakeholders in the South African direct marketing industry. Members include the widest range of private and governmental bodies involved in the making of sales and the developing of relationships directly by mail, telephone, television and radio, magazines and newspapers, fax, electronic mail and the Internet - all brought together by a common interest in responsible business practice. The Association represents some 300 companies and 1000 individuals, both local and international. Membership includes organisations ranging from entrepreneurial start-ups to the largest multi-national corporations, and is fully representative of both marketers in and suppliers to, the financial, retail, advertising, mail order, call centre, and electronic commerce industry, amongst others. All members are bound by a stringent Code of Practice based on international norms, and which has the endorsement of the Business Practices Committee of the Department of Trade and Industry.The Direct Marketing Association of Southern Africa is a founder member of the International Federation of Direct Marketing Associations (IFDMA). Over 29 DMA's from arond the world are members of IFDMA, and subscribe to its self-regulatory principles.

117 DMA submission on Open Democracy Bill, August 1998.

118 The Commission was referred to section 16(1)(c)(iv) of the Constitution which protects the right to freely impart or receive information. Direct marketing of commercial information is one the most frequently utilised methods of imparting or conveying commercial information to the market and it was submitted that if to "impart" information means to "communicate" or "convey" information to a person then the right to directly convey commercial or other information to a recipient must fall within the scope of section 16 of the Constitution. The concern was expressed that, as the draft Bill presently stands, the narrow circumstances under which data may be processed in terms of section 9 of the Discussion Paper BIll, read together with the broad definitions contained in the draft Bill of "personal information" and "processing", effectively prevent the direct marketing of new products and services to prospective customers or new customers/clients of a business and, as such, severely limit the application of the Constitutional rights contained in sections 32, 22 and 16 of the Constitution. In fact, the Electronic Communications and Transactions Act specifically permits the sending of unsolicited commercial communications subject to the grounds provided in section 45(1) and (4). See the submission of Foschini's in this regard. The Foschini Group, as a major retail organisation, acknowledges that the practice of a retail trade necessarily involves sales and marketing activities aimed at the generation of sales and orders. The right to engage in legitimate marketing activities, subject to regulation by law, must therefore be implicitly catered for in section 22 of the Constitution. In this regard, it is important to note that it is widely recognised by political and economic commentators that economic growth is essential for the realisation of social and economic transformation in South Africa. Fair marketing practices designed to approach, inform and retain customers must accordingly be regarded as of critical importance to the growth of the South African economy.

regulatory framework for direct marketing be promoted that will balance the rights of consumers not to be targeted unreasonably, with the right of business to communicate effectively with the public.

5.1.88 There is a strong view worldwide that some forms of direct marketing are, or have the capacity to be, more intrusive than others. Those forms of direct marketing should be subject to regulation that differs from the rules applicable to less intrusive forms of direct marketing.[119]

5.1.89 The Information Protection Principles in Chapter 3 of the Bill will therefore regulate direct marketing except to the extent that more specific provision is made in Chapter 8 of the Bill for a particular aspect or type of direct marketing, such as unsolicited electronic communications or spam.

5.1.90 In view of the prescripts set out in international instruments and implemented in comparative jurisdictions, the Commission recommends that the opt-in option should be applicable to automated/pre-recorded marketing messages, faxes, e-mail and SMS where there is no previous link between the marketer and the data subject.

5.1.91 The opt-out option will be applicable in all other cases of direct marketing where it will be dealt with as part of the general use, disclosure and information principles set out in Chapter 3 of the Bill.

5.1.92 In both opt-in and opt-out cases the business will be allowed to make contact with the data subject or consumer. However, with the opt-in position, if the data subject does not respond to the responsible party's invitation to make use of its direct marketing advances, the responsible party will not be able to contact the consumer for a second time. With the opt-out position the responsible party may keep on contacting the consumer until the consumer objects.

---

119 ***ALRC Discussion Paper*** at 707.

5.1.93 Processing of information (this includes collection of information) will not be possible without the knowledge of the data subject.

5.1.94 These principles will operate alongside the Consumer Protection Bill provisions that provide for a statutory register which will provide additional protection to the consumers (data subjects) against unreasonable direct marketing practices.

5.1.95 The position in respect of direct marketing as set out in the ECT Act is in accordance with the position set out in Chapter 3 of POPIA. However, since the developments worldwide regarding the stricter regulation of spam have only taken place after the enactment of the ECT Act, it is proposed that section 45 of the Act be repealed and that direct marketing be regulated in terms of Chapter 8 of POPIA.

5.1.96 The Commission takes cognisance of the fact that the real problem for direct marketers seems to be to initiate the permission-based relationship. Unfortunately, the only known method of doing this is by interrupting people, catching their attention and encouraging contact using various tricks of the trade. Without some way to grab the attention of a stranger, the permission process never starts.[120] Some methods which are regarded as legitimate ways of gathering personal information openly through a website in a permission-based context are the following:[121]

a) Opt-in forms placed on a network of sites. Visitors complete the forms in order to subscribe to a newsletter, take part in a competition or promotion, or receive special offers in line with the interests they register.

b) Free Internet access in return for exposure to advertising, information on university grants, Internet users are paid to surf the Internet, registration on a site dedicated to amateur guitarists, weight-loss program and specialised newsletter, registration on on-line game sites, electronic greeting cards,etc.

c) Banner advertising on web sites profiled by interests and lifestyles compatible

---

120 **Unsolicited Commercial Communications and Data Protection** at 61.

121 **Unsolicited Commercial Communications and Data Protection** at 50.

with the advertiser's products and services. Visitors are enabled to click through and initiate the opt-in e-mail relationship by completing a registration form.

d) Regulating the use of public directories (getting the approval up front of subscribers to use their information for direct marketing purposes) may create a situation where these directories will be more available to marketers.

5.1.97 A privacy framework for direct marketing purposes needs to be established. Consideration was given to the question whether direct marketing should be regulated in the privacy legislation or whether it should be dealt with in the ECT Act or Consumer Protection legislation.

5.1.98 The opinion of the Dti, set out in their written submission to the Commission, was that the section dealing with unsolicited electronic information should remain in POPIA and that consequential amendments should be effected to the ECT Act to require that the processing of information be in line with the principles set out in POPIA. This argument is in accordance with the broader agreement with the Department of Communications to the effect that the privacy provisions in the ECT Act should be seen as an interim arrangement until the privacy legislation is enacted.

5.1.99 The Commission decides to follow the recommendations of the Department of Trade and Industry to include the direct marketing proposals in POPIA. See the general principles in Chapter 3 and the specific prescripts in Chapter 8 as referred to above.

5.1.100 The legislative enactment reads as follows:

CHAPTER 8

RIGHTS OF DATA SUBJECTS RELATING TO UNSOLICITED ELECTRONIC COMMUNICATIONS AND AUTOMATED DECISION MAKING

Unsolicited electronic communications

66.(1) The processing of personal information of a data subject for the purpose of direct marketing by means of automatic calling machines, facsimile machines, SMSs or electronic mail is prohibited unless the data subject -

(a) has given his, her or its consent to the processing; or

(b) is a customer of the responsible party, subject to the provisions set out in section 66(2).

(2) A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of section 66(1)(b) -

(a) if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;

(b) for the purpose of direct marketing of the responsible party's own similar products or services; and

(c) if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details -

(i) at the time when the information was collected; and

(ii) on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

(3) Any communication for the purpose of direct marketing must contain -

(a) details of the identity of the sender or the person on whose behalf the communication has been sent; and

(b) an address or other contact details to which the recipient may send a request that such communications cease.

Directories

67.(1) A data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its personal information is included, must be informed, free of charge and before the information is included in the directory -

(a) about the purpose(s) of the directory; and

(b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.

(2) A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.

(3) Subsections (1) and (2) do not apply to editions of directories that were produced in printed or off-line electronic form prior to the entry into force of this section.

(4) If the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the information protection principles prior to the entry into force of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received the information required by section 67(1) above.

5.2 Profiling/ Information matching (automated decisionmaking)

a) Proposals in Discussion Paper[122]

122 **CHAPTER 10**
MISCELLANEOUS

Automated decision making

5.2.1 It has already been established that the mere collecting and storing of information may constitute an infringement of a subject's right to privacy if it is an unreasonable act. A further, more serious infringement, may occur where information which relates to the individual is structured in such a way that it can begin to answer questions about that person, so as to put his or her private behaviour under surveillance. This practice is referred to as information matching or profiling.

5.2.2 One example where profiling is used for ordinary marketing purposes is where a process referred to as information mining, enables the retailer to engage in targeted marketing.[123] An on-line bookstore might offer a customer recommendations based on what the customer has bought in the past, or looked at on the web site, usually other books by the same author or on the same subject.[124]

5.2.3 Another example, with more serious consequences for the data subject, is where the fact that a data subject purchases large quantities of halaal meat at times which relate to Muslim feast days may be passed on to a security agency which has also established that the subject has purchased books on the web relating to terrorist tactics, and that he or she has looked for information on how to get an American visa. Adverse inferences may then be drawn with regard to

---

93. (1) Subject to subsection 2, no one may be subject to a decision to which are attached legal consequences for him or her, or which affects him or her to a substantial degree, where this decision has been taken solely on the basis of the automated processing of personal information intended to provide a profile of certain aspects of his or her personality or personal habits.

(2) The provisions of subsection (1) do not apply where the decision referred to therein:

a) has been taken in connection with the conclusion or execution of a contract, and
(i) the request of the data subject in terms of the contract has been met; or
(ii) appropriate measures have been taken to protect the data subject's lawful interests; or

b) is based on a law or code of conduct in which measures are laid down for protecting the lawful interests of data subjects.

(3) Appropriate measures, as referred to under subparagraph 2(a), must be considered as taken where the data subjects have been given the opportunity to put forward their views on the decisions as referred to under subsection (1).

(4) In the case referred to under subsection (2), the responsible party must inform a data subject about the underlying logic of the automated processing of the information relating to him or her.

123 In the advertising world the practice exists of tracking internet users and compiling dossiers on them in order to target banner advertisements. A marketing profile is a record of an individual's characteristics created by acquiring personal information from mutiple sources and then using it to target products and services. Marketing profiles are created and used by the private sector to maintain old customers and to target new ones by identifying those persons as warranting solictation. National Telecommunications and Information Administration, Department of Commerce, United State of America (NTIA) ***Privacy Report*** Appendix A: Marketing Profiles at 3, available at http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

124 Andrew Rens.

the subject on account of this accumulated information, which may, or may not, be correct.[125]

5.2.4 Generally speaking, profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics. [126]

5.2.5 As such, the profiling process has two main components:

(a) profile generation – the process of inferring a profile;

(b) profile application – the process of treating persons/entities in light of this profile.[127]

5.2.6 The first component typically consists of analysing personal information in search of patterns, sequences and relationships, in order to arrive at a set of assumptions (the profile) based on probabilistic reasoning. The second component involves using the generated profile to help make a search for, and/or decision about, a person/entity. The line between the two components can blur in practice, and regulation of the one component can affect the other component.[128]

5.2.7 There is, generally speaking, no objection to the compiling of statistical information and profiles from personal information, where it is not possible to trace the personal information of any identifiable individual from such profiling.[129] Profiling is a valuable marketing tool and freely allowed as long as it is not making individualised personal information available.[130] This view was also

---

125 Tilley at 3.

126 Bygrave L A "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling" ***Computer Law and Security Report***, 2001 Vol 17 at 17-24 accessed at http://folk.uio.no/lee/publications/ on 2005/07/29 (hereafter referred to as "Bygrave ***Computer Law and Security Report*** 2001") at 2.

127 Bygrave ***Computer Law and Security Report*** 2001 at 2.

128 Bygrave ***Computer Law and Security Report*** 2001 at 2.

129 Section 9 of Chapter VIII of the ECT Act reads as follows:

(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data ,as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

130 ISPA notes that in practice Internet users are uniquely identifiable by the IP (Internet Protocol) address, which is assigned to them when they connect to the Internet. While it may not be immediately practical or possible for any third party to tie that IP address to a name and address, it is technically possible to track that IP address as the person 'surfs the web'.

confirmed in the response to a question posed in the Issue Paper 24 regarding the acceptability of profiling.[131]

5.2.8 An example of anonymous profiling would be in the development of score cards (for credit risk management) where banks would typically use the services of specialist score card developers where the latter would require to be provided with anonymous account information from the particular bank for analysing.[132]

5.2.9 The EU Directive only deals with profiling as such in Article 15(1) which provides for automated decisionmaking.[133]Article 15(1) states that EU member states shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of information intended to evaluate certain personal aspects relating to him, such as his performance at work,

---

This is standard practise with online advertising companies, which may advertise on many websites. Some advertisements leave a cookie on your computer, which is an additional level of unique identification, and this cookie can be used to harvest personal information and surfing habits. In the same measure, by merely accessing the image of an online advert, you are leaving an 'imprint' of your IP address in a log on a web server. If the same advertising host advertises on millions of web sites, it becomes easily possible to track user habits by processing the logs each time an advert is viewed, and by requesting referrer information in each instance. (Each time you click a link to go to a website or another section of the website, the web server on the receiving end not only gets information on the file you want, but also information on which link directed you there. This information is very useful for statistical analysis of who uses a website, and is largely harmless when it is impossible to tie an identity of an individual to an IP address.

131 One of the largest advertisers in the USA, DoubleClick, however, set off widespread public outrage when it began attaching personal information from a marketing firm it purchased to the estimate 100 million previously anonymous profiles it had collected. The company backed down due to public opposition, a dramatic fall in stock price and investigations from the FTC and several state attorneys-general. In January 2001 DoubleClick closed its online profiling divisions, and in May 2002 privacy class actions suits against the company were settled. See EPIC DoubleClick Pages at http://www.epic.org/privacy/doubletrouble/.; Privacy Advocates debate metrits of DoubleClick settlement; Computerworld May 22 2002 at http://www.computerworld.com/printthis/2002/.

132 The Banking Council.

133 **Article 15 Automated individual decisions**

Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

See, however, art 14 (b) of the Directive dealing with the right to object to direct marketing. This article does not deal with profiling as such.

creditworthiness, reliability, conduct, etc."

5.2.10 As an information protection provision, Article 15(1) is rather special in that, unlike the bulk of other rules in information protection instruments, its primary formal focus is on a type of decision as opposed to information processing. As such, Article 15(1) is akin to traditional administrative law rules on government decision making. This characteristic, though, does not have large practical significance given that decisions inevitably involve the processing of information. Moreover, the impact of Article 15(1) is likely to be considerably greater on the decision-making processes of the private sector than on the equivalent processes of the public sector.[134]

5.2.11 Article 15 derives from several concerns. The central concern is rooted in the perceived growth of automatisation of organisational decisions about individual persons. The drafters of the Directive appear to have viewed as particularly problematic the potential for such automatisation to diminish the role played by persons in shaping important decision-making processes.[135] The use of extensive information profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'information shadow'.[136]

5.2.12 A second expressed fear is that the increasing automatisation of decision-making processes engenders automatic acceptance of the validity of the decisions reached and a concomitant reduction in the investigatory and decisional responsibilities of humans.

5.2.13 Up until recently, such assessments have tended to be based primarily on information collected directly from the data subjects in connection with the assessment at hand. It is likely, though, that these assessments will increasingly be based on pre-collected information found in the databases of third parties. Indeed, with effective communication links between the databases of large numbers of organisations, sophisticated software to trawl these databases, and appropriate adaptation of the relevant legal rules, it is easy to envisage computerised decision-making processes that operate independently of any specific input from the affected data subjects.

---

134 Bygrave ***Computer Law and Security Report*** 2001 at 2.

135 Bygrave ***Data Protection*** at 3.

136 Bygrave ***Computer Law and Security Report*** 2001 at 5.

5.2.14 Additionally, there is ongoing growth in the frequency, intensity and ambit of organisational profiling practices. Not only is profiling an emergent industry in its own right, but the techniques upon which it builds (e.g. information warehousing and information mining) are evermore sophisticated.

5.2.15 An important rationale for the right in Article 15(1) is, therefore, protection of human integrity and dignity in the face of an increasingly automated and inhumane world.[137] It is, however, important to note that marketing profiles are not, per se, regarded as necessarily detrimental to the data subject. [138]

5.2.16 Examples of the prohibition against automated decision making in other jurisdictions can be found in article 42 of the Dutch Personal Data Protection Act, 2000; section 12 of the UK Data Protection Act 1998; and, since the implementation of the Directive, in the data protection legislation of most of the other European countries. However, no similar provision has been made in the Australian[139] and Canadian[140] legislation.

b) Evaluation

5.2.17 Different opinions were expressed regarding the problem of profiling. Some respondents saw identifiable profiling as a natural part of their business, while others expressed concern about the practice. A distinction was, furthermore, made between the data subject in this category having knowledge of the collection of the information and, on the other hand, having specifically given permission for the collection and use of the information.[141]

---

137 Bygrave ***Computer Law and Security Report*** 2001 at 8.

138 Nevertheless, some forms of advertising have at least a potential to significantly affect their targets. For instance, the cybermarketing process outlined above could plausibly be said to have a significant (significantly adverse) effect on the persons concerned if it involves unfair discrimination in one or other form of "weblining" (eg the person visiting the website is offered products or services at a higher price than other, assumedly more valuable consumers have to pay, or the person is denied an opportunity of purchasing products/services that are made available to others).

139 Privacy Amendment (Private Sector) Bill 2000.

140 Personal Information Protection and Electronic Documents Act 2000 (Bill C-6).

141 Andrew Rens.

5.2.18 Commentators, who were concerned about the use of profiling and argued for consent requirements, stated the following:

a) Since it is not possible to guarantee a subject's anonymity, affirmative consent should be required because of the potential for a trail to lead to a customer through an IP address and cookies.[142]

b) Written consent is necessary for non public information.[143] Consent should be obtained from the data subject involved prior to information profiling taking place.[144] Responsible parties who sell information to information profilers should obtain the prior consent of the data subject before proceeding to sell the information to information profilers, unless the public interests or those of the State dictate otherwise. Data subjects whose information is sold for information profiling purposes without the data subject's consent should be provided with adequate remedies to enable them to take action against the responsible party in breach.[145]

c) If personal information is being used for profiling without the consent of the data subject it should constitute an unacceptable infringement on his privacy.[146] The consent requirement should, however, not apply with regard to the prevention and detection of fraud.[147]

d) Where consent must be provided for, "implied" consent may particularly be feasible, but the law should then clearly provide for information to the public, when and how this process will operate in practice.[148]

---

142 Internet Service Providers Association.

143 Strata.

144 Eskom Legal Department.

145 SABC.

146 ENF for Nedbank.

147 SAFPS.

148 Financial Services Board.

5.2.19 On the other hand, those who felt that information profiling was a natural part of conducting business argued as follows:

a) The development of credit scores within the credit information system should be allowed with the knowledge of the data subject, but without a consent requirement. Alternatively, the use of credit information to develop credit scores should be defined as a legitimate use /purpose.[149]

b) Information profiling is a statutory requirement in terms of FICA and banks adhere to the requirements of this Act. It is further used for fraud prevention and behavioural scoring within the banking industry.[150] It was argued that information profiling for marketing purposes can and should be a natural element of marketing practices as long as it is done within defined parameters and subject to an 'opt out' consent option. The banking industry, for example, has access to clients' financial records, spending patterns, and as such is able to compile profiles of clients. Use of this information to curb and prevent fraud, enhance services and products, introduce services and products, manage relationships with clients, extend or deny credit facilities, etc should be encouraged, but subject to the provision that the use/storage of such information does not constitute an unreasonable act and if appropriate, is consented to by the client.

c) Information profiling is a reality in the law enforcement community that provides valuable input in respect of a suspect's modus operandi and assists the law enforcement agency in planning and conducting operations.[151]

d) Information profiling is essential in the long-term insurance industry. The industry has to deal with population demographics in order to revise the morbidity and mortality tables. These tables are based upon underlying information, and unless the industry is able to retain and use this type of information, the industry will be unable to determine the risks involved and no objective criteria for the determination of risk will

149 Credit Bureau Association. .

150 The Banking Council.; Nedbank.

151 SAPS.

be possible.[152]

e) Profiling is a natural part of conducting business. Profiling assists, for instance, in targeting those customers who are or may be interested in a product.

5.2.20 It was further stated that the true nature of the potential threat to the constitutional privacy of an individual posed by new information technology is not the processing of contact information and legitimately gathered credit information, but rather the ability of organisations to build up profiles of information technology users through the use of information tracking tools such as cookies ie data that allows for detecting Web pages viewed by a user on a given site or set of sites. This type of information can be collected to create user profiles.[153]

5.2.21 In so far as automated decision making, specifically, is concerned, the following comments were received:

a) All banks engage in active profiling of its clients, including for fraud and credit scoring and in order to create marketing or credit profiles. Many of these processes are automated and would be covered by the provisions of section 68 to the Bill.[154] Information scoring, whether automated or manual, should be allowed, but should be subject to restrictions to prevent abuse by unscrupulous parties and prevent vulnerabilities to spamming and excessive use which is not fair or reasonable in the circumstances, while at the same time allowing for profiling tools and methodologies to be used to assist businesses in continuing to operate their businesses effectively. Requirements to protect the consumer are covered in the National Credit Act and in the Electronic Communications and Transaction Act. However, the Commission should ensure that no loopholes exist between these pieces of legislation and this Act. Codes of conduct are required in this regard.

---

152 LOA; Some Life Offices have established specific information centers, which collates information regarding data subjects, so that financial advisers assisting data subjects with their financial planning can obtain the information necessary to do a financial need analyses. Such operations will also be impacted, to clients' potential detriment.

153 DMA.

154 Nedbank.

b) Banks use a substantial amount of information to do predictive modelling, which is extremely important to the business of the bank.[155] The predictive modelling is done in a number of ways and for a number of reasons. An example is where information relating to the bank's entire customer base is used to make projections and where the information of individual data subjects is used for profitability modelling. This processing is done firstly for reasons which revolve purely around effectively and competitively conducting the bank's business and secondly with a view to identifying specific data subjects as possible clients for additional products (lead generation). In the first example processing is done without reference to, or interest in the identity of the data subject, and in the second this is an important factor.

c) An important consideration in this area involves distinguishing between the further processing of information purely for the internal management of the business of a bank and the further processing of information for the purpose of "lead generation". While in the context of "lead generation" it is understandable that the Commission may want to keep some control over the further processing of information, and has therefore specifically allowed that authorization for further processing of information can be applied for. However in the context where a bank may need to process information further in order to maintain a competitive business edge and to be able to forecast with some degree of certainty, the further processing of information should be allowed in the context where it will not prejudice the data subject. An exemption which entrenches this would be preferable to having to apply for authorization.

d) A bank also utilises what it would view as "historical data" to develop score cards relating to certain products, historical data is also used to monitor a client's conduct on an account and to increase credit limits if in the opinion of the Bank the client's conduct has been suitable. This will impact both on what the legislature will regard as historical information and also on whether the concerns regarding lead generation already discussed, will be addressed.

---

155 Banking Association.

c) Recommendation

5.2.22 After evaluating the comments received, the Commission's recommendations regarding profiling can be summarised as follows:

a) There is no objection to the compiling of statistical information and profiles of personal information, provided it is not possible to trace the information to an identifiable data subject.

b) The legitimate interests of business should, furthermore, be appropriately accommodated. In ordinary circumstances marketing profiles should not be regarded as detrimental to a data subject.

c) The ordinary principles, exceptions, exclusions and exemptions set out in Chapter 3 and 4 of the Bill are applicable as is Chapter 7 dealing with sector specific codes of conduct.

d) Section 43(1) (k) and section 44 (3) of the proposed Bill make provision for the supervision of information matching legislation.

e) Marketing practices are currently being dealt with in the National Credit Act.[156] Special provision has, furthermore, been made for unsolicited electronic communications in section 66 of the Bill.

f) Restrictive measures need to be put in place that will ensure that data subjects are not unreasonably affected to their detriment by the profiling of their personal information.

5.2.23 The Commission, therefore, confirms its original proposals and recommends that a section should be included in the proposed Bill to provide for the prohibition of unreasonable automated decision making. The inclusion of this section will ensure that data subjects are not deprived of a significant counterweight to the ongoing expansion, intensification and refinement of automated profiling practices. However, provision has also

---

156 See in this regard Part C Credit Marketing Practices (sections 74-77) of the NCA.

been made for exceptions to this principle, where it is clear that the legitimate interests of the data subjects are protected.

5.2.24 The legislative enactment of this provision will read as follows:

Automated decision making

68.(1) Subject to subsection 2, no one may be subject to a decision to which are attached legal consequences for him or her, or which affects him or her to a substantial degree, that has been taken solely on the basis of the automated processing of personal information intended to provide a profile of certain aspects of his or her personality or personal habits.

(2) The provisions of subsection (1) do not apply if the decision -

(a) has been taken in connection with the conclusion or execution of a contract, and -

(i) the request of the data subject in terms of the contract has been met; or

(ii) appropriate measures have been taken to protect the data subject's legitimate interests; or

(b) is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

(3) The appropriate measures, referred to in subsection 2(a)(ii), must -

(a) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and

(b) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of subsection (a).

5.3 Credit reporting

a) Proposals in Discussion Paper

5.3.1 Credit reporting involves providing information about an individual's credit worthiness to banks, finance companies and other credit providers, such as retail businesses that issue credit cards or allow individuals to have goods or services on credit.[157]

5.3.2 Credit reporting is generally conducted by specialised credit reporting agencies (credit bureaux) that collect and disclose information about potential borrowers, usually in order to assist credit providers to assess applications for credit.[158] Before giving a person credit, credit providers (lenders) such as banks, loan companies, catalogue companies and shops want to be confident that the consumer will repay the money they lend.[159]

5.3.3 Credit bureaux collect personal information about consumers (data subjects) from credit providers and publicly available information. This information is stored in central data bases for use in generating credit reporting information for credit providers. In assessing credit applications, this information augments information obtained directly from a consumer's (data subject's) application form and the credit provider's own records of past transactions involving the consumer.

---

157 ***ALRC Discussion Paper*** at 1325.

158 Ibid.

159 Information Commissioner's Office UK ***Credit Explained*** accessed at www.ico.gov.uk on 20 August 2008 .

5.3.4 The information contained in credit reporting data bases may be used in credit scoring systems. Credit scoring may be described as the use of mathematical algorithms or statistical programmes that determine the probable repayments of debts by consumers, thus assigning a score to an individual based on the information processed from a number of data sources.[160]

5.3.5 It has been stated[161] that credit reporting is an understandable response to a modern, interconnected world containing billions of people and where word of mouth is insufficient to assess reputation.

5.3.6 While the major purpose of credit reporting is to provide information to assist credit providers to assess applications for credit, credit reporting may also be seen as serving the associated purpose of facilitating responsible lending. That is, the information provided by credit reporting to credit providers may help to prevent consumers becoming financially overcommitted. Credit reporting also assists in trade and mortgage insurance and in debt collection.

5.3.7 In practice, credit bureaux, in compiling credit information files, obtain most of that information from credit providers themselves. This creates a two-way flow of personal information between credit bureaux and credit providers.[162]

5.3.8 In terms of POPIA both credit providers and credit bureaux are defined as "responsible parties" and are consequently jointly responsible for the protection of the personal information of data subjects during various stages of the credit reporting cycle.

Credit bureaux

---

160 ***ALRC Discussion Paper*** at 1326.

161 ***ALRC Discussion Paper*** at 1326 in a reference to a comment by Professor Daniel Solove published in Solove, D "A Taxonomy of Privacy" (2006) 154 (3) ***University of Pennsylvania Law Review*** 477 at 507-508.

162 ***ALRC Discussion Paper*** at 1350.

5.3.9 In South Africa there are currently eleven known credit bureaux,[163] the oldest operating since 1901. All are privately owned.[164]

5.3.10 As the name indicates, the main object of credit bureaux is to collect and furnish information concerning the creditworthiness of people.[165] Credit bureaux collect consumer credit information (as defined in section 70(1) of the National Credit Act, 2005("NCA"). The information may be grouped into the following types:[166]

(a) Identifying Information: This is personal information such as name, address, identity number (same as social security number), employment details, marital status and telephone numbers.

(b) Court Record Information: Judgments and bankruptcies received from court records, which are public domain information. This information is obtained from the Magistrates Court and the High Court.

(c) Default Information: This information is provided by the subscribers to the bureaux who report on how their customers have performed on their financial obligations with the subscriber. This is only negative information.

---

163 The larger credit bureaux are:

a) Trans Union Credit Bureau.
b) Experian, who deals exclusively with consumer credit information, is British owned and is associated with Kreditinform and Snyman & Vennote.
c) Kreditinform, who deals exclusively with commercial credit information and who are South African owned.

The smaller bureaux are:

a) Snyman & Vennote Credit Profile Bureau, a consumer bureau, which focuses on small to medium size businesses as subscribers. They are linked to a debt recovery agency and are South African owned.
b) CIA, who deals exclusively with commercial information. CIA's main shareholder is Trans Union.
c) Medinform, a consumer information bureau who deals mainly with medical information and who is combined with a debt recovery agency, that is South African owned.
d) Creditwatch, that is a consumer bureau dealing only with the medical profession, and is South African owned.
e) Micro Lenders Credit Bureau, a consumer bureau dealing with the micro loans industry, that is South African owned.
f) Compuscan, a consumer bureau dealing with the micro loans industry, that is South African owned.

164 Kraus E ***The Legal Framework : Governing Public & Private Credit Information Registries: The South African Experience*** Credit Bureau Association, South Africa (hereafter referred to as "Kraus") at 3.

165 See ***Neethling's Law of Personality*** at 297; Cf also Faul ***Bankgeheim*** at 525-526. With regard to juristic persons, it is in particular information on their creditworthiness which is also the subject of data processing.

166 Kraus at 5.

(d) Closed User Group Information: The Credit Providers Association (CPA)[167] represents 80% to 90% of the larger retailers, telecommunications, debt recovery agencies and the banks. Members of this association supply both positive and negative information on the monthly payment details of the accounts that are held with the member.

(e) Information received from insurance companies and other sources other than credit providers.[168]

5.3.11 It has been argued that credit bureaux may be capable of disclosing a complete record, not only of someone's creditworthiness, but also of his entire personal life.[169] In this regard it would seem that South African credit bureaux generally restrict their activities to information on creditworthiness. The National Credit Regulations, 2006[170] now prohibits the collection of consumer credit information relating to specified subjects such as race, political affiliation etc.

5.3.12 Credit bureaux have an important role to play in providing consumers with access to credit facilities. They help lenders identify good borrowers which improves risk management, enables lenders to increase the amount of lending, reduces default rates and enables borrowers to develop credit profiles.[171] As the primary collectors and users of credit information both the credit providers and the bureaux also recognise the need to give effect to data subjects' rights to privacy and their responsibility to supply accurate, correct and valid data.[172]

5.3.13 However, owing to the fact that it is often difficult to identify data subjects positively from newspaper or court reports, the real possibility exists that data reports on persons in credit bureaux

---

167 The CPA shares information on payment performance of consumers through the credit bureaux.

168 See Regulation 18 of the National Credit Regulations below.

169 See McQuoid-Mason ***CILSA*** at 197 fn 9.

170 Regulations 18 and 19.

171 Credit Information Industry Code of Conduct , 2006.

172 Ibid.

may contain misleading or incorrect information.[173] It is important to note that although the information stored by credit bureaux is often available only to its clients,[174] the possibility exists that other individuals, private corporations or even the state may have access to such information.[175] In the USA the Federal Trade Commission receives more complaints about credit bureauxs than about any other industry. [176]

5.3.14 Errors are not always the fault of the credit bureau - it might be from one of its sources (mostly credit providers). The credit bureau's responsibility to its customers is to give an accurate reflection of what is in a public record, but that record may itself be inaccurate.[177]

5.3.15 Regardless of the origin of such errors, clear lines of responsibilty for correcting the record should be established. This would mean that protection of the information should be ensured throughout the credit reporting cycle, not only while the information is being processed by the credit bureau. If not, the victim's life may descend into a "Kafkaesque nightmare".[178]

5.3.16 In 1989 the then Credit Bureau Association (CBA) drew up a self-regulatory code of conduct, as a result of increasing pressure from various consumer groups to protect consumers against possible credit bureau abuses. In 1994 the CBA, in association with the Business Practices Committee (BPC) of the Department of Trade & Industry (DTI), formalised the code, which applied to all credit bureaux in South Africa. The BPC included various principles from the Fair Credit Reporting Act (USA) in the code. In 2006 a revised Code was published, the Credit Information

---

173 For examples from case law, see ***Informa Confidential Reports (Pty) Ltd v Abro*** 1975 (2) SA 760 (T); ***Pickard v SA Trade Protection Society*** (1905) 22 SC 89. Also in ***Kritzinger v Perskorporasie van Suid-Afrika (Edms) Bpk ea*** 1981 (2) SA 373 (O) 386 it was acknowledged that credit bureaux may distribute incorrect information.

174 Cf eg ***Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd*** 1968 (1) SA 209 (C).

175 See Neethling 1980 ***THRHR*** 144.

176 Piller at 2.

177 Piller at 2 referring to Steve Metlitz, general counsel of the Information Industries Association, which represents about 500 companies that gather and resell data in the USA.

178 Piller at 2. It has been noted that although a credit bureau may in theory be easily accessible to consumers, callers have been known to wait in line for more than an hour without being able to reach a credit bureau by phone.

Industry Code of Conduct,2006 (CII Code). The Code reflected various laws[179] and international best regulatory practice principles[180] applicable to the credit information industry.

5.3.17 The CII Code makes provision for the following with respect to protecting the consumer:[181]

– Credit bureaux have a duty to treat subscribers and consumers as fairly and impartially as possible. In addition, credit bureaux may only contract with subscribers who warrant that they have a bona fide risk management reason for accessing the information and who agree not to disseminate the information to any person other than the consumer concerned.

– Bureaux must follow reasonable procedures to ensure that the information they obtain is accurate, relevant and unbiased. Furthermore, the source of information received and the subscribers who access the information must be recorded.

- A bureau must upon request and presentation of positive identification, provide consumers with credit reports during normal business hours and on reasonable notice.

- If a consumer disputes the accuracy of any item of information in his file, the bureau must investigate the accuracy of such information. It must provide the consumer with credible evidence supporting the challenged information. If the information is found to be inaccurate or can no longer be verified, it must be deleted.

– In the case of a dispute between the bureau and a consumer on the accuracy or relevancy of information, the consumer has recourse to the Credit Information Ombudsman or the National Credit Regulator.

– Bureaux must take into account consumers' interests regarding the length of time for which information is retained, so that consumers are not prejudiced by stale information about long past credit defaults. See the provisions for retention in the NCA.

---

179 National Credit Act 34 of 2005; Promotion of Access to Information Act 2 of 2000; Financial Intelligence Centre Act 38 of 2001.

180 Internationally accepted Information Protection Principles.

181 See also section 72 of the NCA.

- The code only applies to consumer information recorded by the bureaux and not to business information.
- That subscribers shall warrant, subject to Regulation 18(4) of the Consumer Credit Regulations, 2006, via their subscription agreement to the services of a bureau, that they have obtained the necessary consent from their customers to access bureau information, and that the consumer has been informed in writing of the subscriber's intention to supply such information to the bureaux.

National Credit Act

5.3.18 In South Africa the National Credit Act[182] regulates the credit industry. Implementation of specified sections commenced on 1 June 2006.

5.3.19 The purpose of the National Credit Act[183] is to promote a credit market that is fair, transparent, accessible and responsible. It also aims to promote a market that is competitive and sustainable. However, the overriding objective of the Act is to protect consumers. It specifically prohibits practices such as reckless lending and automatic increases in credit limits, and regulates interest and fees. The Act covers all forms of consumer credit, including bank loans, credit cards, store cards, pawn transactions, furniture finance and motor vehicle finance.

5.3.20 The Act empowers the Regulator to deal with any contraventions on existing loan and credit agreements. Although the National Credit Act replaces the Usury Act and Credit Agreements Act, the Regulator will be able to assist consumers with problems that fall under these previous Acts, and to investigate complaints that fall under these Acts.

5.3.21 The National Credit Regulator is created to enforce the Act and to regulate credit providers,

---

182 National Credit Act 34 of 2005.

183 The Department of Trade and Industry South Africa "Introducing the National Credit Regulator" 2 June 2006 accessed at http://www.thedti.gov.za/article on 3 September 2008.

credit bureaux and debt counsellors. It further receives and investigates complaints, and educates consumers of their rights under The Act.

5.3.22 The Act is augmented by the National Credit Regulations, 2006.[184][185]

---

184 National Credit Regulations, 2006 Published under GN R489 in GG 28864 of 31 May 2006, as amended.

185 Regulation 18 (7) reads as follows:

18 Maintenance and retention of consumer credit information by credit bureaux

(1)-)6).....

(7) In addition to the sources of consumer credit information contemplated in section 70(2) of the Act, a registered credit bureau may receive consumer credit information in respect of a consumer from any person, provided the originating source of the information is one of the following persons:

(a) An organ of state, a court or judicial officer;

(b) Any person who supplies goods, services or utilities to consumers, whether for cash or on credit;

(c) A person providing long term and short term insurance;

(d) Entities involved in fraud investigation;

(e) Educational institutions;

(f) Debt collectors to whom book debt was ceded or sold by a credit provider;

(g) Other registered credit bureaux.

19 Submission of consumer credit information to credit bureau

(1) The information submitted to a credit bureau must contain the following information in respect of a consumer:

(a) Initials and surname or full names and surname;

(b) SA identity number, or if the consumer does not have an identity number, the passport number and date of birth;

(2) In as far as it is available, the following information should be included when consumer information is submitted to a credit bureau:

(a) Residential address and telephone number;

(b) Details of employer and place of work, if self employed or unemployed, a statement to that effect.

(3) All sources of information as set out in section 70(2) of the Act and Regulation 18(7) must take reasonable steps to ensure that the information reported to the credit bureau is accurate, up-to-date, relevant, complete, valid and not duplicated.

(4) All sources of information as set out in section 70(2) of the Act and Regulation 18(7) must give the consumer at least 20 business days notice of its intention to submit the following adverse information concerning that person to a credit bureau:

(a) classification of consumer behaviour, including classifications such as 'delinquent', 'default', 'slow paying', 'absconded' or 'not contactable';

(b) classifications related to enforcement action taken by the credit provider, including classifications such as handed over for collection or recovery, legal action, or write-off.

5.3.23 It should be noted that, in terms of an interim arrangement between the Dti and the Department of Justice, the Act and Regulations also partly regulates the protection of personal information of consumers during credit reporting. See Part B of Chapter 4 of the Act.[186]

(5) No source of information as set out in section 70(2) of the Act and Regulation 18(7) may submit information to a credit bureau that has prescribed in terms of the Prescription Act 68 of 1969.

Part B

Consumer rights (reg 20)

20 Right to access and challenge credit records and information

(1) When a consumer requests a credit report, the report must disclose the same information that will be displayed to other parties when such report is provided.

(2) If the accuracy of the consumer credit information has been challenged by a consumer in terms of section 72(3)(a) and (b) of the Act, the person to whom the challenge has been made must take the steps set out in section 72(3) within 20 business days after the filing of the challenge.

(3) If the information is removed in terms of section 72(3)(b), the credit bureau must inform the consumer and all parties to whom the information has been reported in the previous 20 business days as well as all other registered credit bureaux.

186

Part B

Confidentiality, personal information and consumer credit records (ss 67-73)

68 Right to confidential treatment

(1) Any person who, in terms of this Act, receives, compiles, retains or reports any confidential information pertaining to a consumer or prospective consumer must protect the confidentiality of that information, and in particular, must-

(a) use that information only for a purpose permitted or required in terms of this Act, other national legislation or applicable provincial legislation; and

(b) report or release that information only to the consumer or prospective consumer, or to another person-

(i) to the extent permitted or required by this Act, other national legislation or applicable **provincial** legislation; or

(ii) as directed by-

(aa) the instructions of the consumer or prospective consumer; or

(bb) an order of a court or the Tribunal.

(2) Failure by a credit bureau to comply with a notice issued in terms of section 55, in relation to this section, is an offence.

[Date of commencement of s. 68: 1 September 2006.]

70 Credit bureau information

(1) In this section, 'consumer credit information' means information concerning-

(a) a person's credit history, including applications for credit, credit agreements to which the person is or has been a party, pattern of payment or default under any such credit agreements, debt re-arrangement in terms of this Act, incidence of enforcement actions with respect to any such credit agreement, the circumstances of termination of any such credit agreement, and related matters;

(b) a person's financial history, including the person's past and current income, assets and debts, and other matters within the scope of that person's financial means, prospects and obligations, as defined in section 78 (3), and related matters;

(c) a person's education, employment, career, professional or business history, including the circumstances of termination of any employment, career, professional or business relationship, and related matters; or

(d) a person's identity, including the person's name, date of birth, identity number, marital status and family relationships, past and current addresses and other contact details, and related matters.

(2) A registered credit bureau must-

(a) accept the filing of consumer credit information from any credit provider on payment of the credit bureau's filing fee, if any;

(b) accept without charge the filing of consumer credit information from the consumer concerned for the purpose of correcting or challenging information otherwise held by that credit bureau concerning that consumer;

(c) take reasonable steps to verify the accuracy of any consumer credit information reported to it;

(d) retain any consumer credit information reported to it for the prescribed period, irrespective of whether that information reflects positively or negatively on the consumer;

(e) maintain its records of consumer credit information in a manner that satisfies the prescribed standards;

(f) promptly expunge from its records any prescribed consumer credit information that, in terms of the regulations, is not permitted to be entered in its records or is required to be removed from its records;

(g) issue a report to any person who requires it for a prescribed purpose or a purpose contemplated in this Act, upon payment of the credit bureau's fee except where the Act explicitly provides that no fee be charged;

(h) not draw a negative inference about, or issue a negative assessment of, a person's creditworthiness merely on the basis that the credit bureau has no consumer credit information concerning that person; and

(i) not knowingly or negligently provide a report to any person containing inaccurate information.

(3) In addition to-

(a) the consumer credit information contemplated in subsection (2), a credit bureau may receive, compile and report only other prescribed information in respect of a consumer; and

(b) the sources of consumer credit information contemplated in subsection (2), a credit bureau may receive consumer credit information in respect of a consumer only from other prescribed persons.

(4) The Minister may prescribe-

(a) standards for the filing, retention and reporting of consumer credit information by credit bureaux, in addition to, or in furtherance of the requirements set out in this section; and

(b) maximum fees that may be charged to a consumer for accessing consumer credit information concerning that person.

(5) For the purpose of monitoring the consumer credit market to detect apparent patterns of reckless credit granting and over-indebtedness, researching the accessibility and use of credit by persons contemplated in section 13 (a), and otherwise exercising its mandate to research consumer credit issues and to investigate and enforce compliance with this Act, the National Credit Regulator may-

(a) require any credit bureau to provide periodic synoptic reports of aggregate consumer credit information in the prescribed manner and form to the National Credit Regulator, but any such report must not identify any particular consumer or relate a particular consumer to any information so reported; and

(b) make further reasonable requests for information from a credit bureau related to the information contemplated in paragraph (a); and

Protecting the processing of personal information for purposes of credit reporting can be seen as a secondary object of the Act.

Credit reporting legislation in other jurisdictions

5.3.24 Internationally, credit reporting is generally regulated within privacy laws except where regulation of credit reporting preceded the enactment of privacy laws,[187] or where there is no comprehensive privacy or data protection legislation.[188] The substance of credit reporting regulation is fair information handling, which places it squarely in the area of data protection or information privacy law.

5.3.25 In the United States credit reporting is regulated by the Federal Trade Commission under the Fair Credit Reporting Act, 1970.[189] Credit bureaux receive information from credit providers and others, generally every month, and update their credit files within one to seven days of receiving new information. It should be noted that the stated purpose of the Fair Credit Reporting Act is restricted to ensure that credit reporting agencies (credit bureaux) exercise their role in assembling and evaluating credit information with fairness and respect to the consumer's right to privacy.[190] The Act does not regulate the credit industry per se.

5.3.26 In the United Kingdom, the activities of credit bureaux are regulated by both the Consumer Credit Act 1974 (UK) and the Data Protection Act 1998 (UK). The United Kingdom Information Commissioner deals with credit reporting complaints, and credit reference agencies are bound by the Data Protection Act. In contrast to the US Act the Consumer Credit Act regulates the credit industry itself and provides limited protection to the individual's rights of access to, and correction

---

(c) analyse information provided to it under this section or section 69.

(6) Failure by a credit bureau to comply with a notice issued in terms of section 55, in relation to this section, is an offence.

[Date of commencement of s. 70: 1 September 2006.]

187 Eg the United Kingdom. See discussion below.

188 ***ALRC Discussion Paper*** at 1370.

189 Note that the United States does not have a federal information protection regulator.

190 Section 602.

of, credit information about them.[191]

5.3.27 The Consumer Credit Act requires certain businesses to obtain consumer credit licences. It protects individuals receiving credit. The Consumer Credit Act sets out rules for:

a) The form and content of agreements;

b) Credit advertising;

c) The method of calculating the Annual Percentage (APR) of the Total Charge for Credit;

d) The procedures to be adopted in the event of default, termination, or early settlement; and

e) Extortionate credit bargains.

5.3.28 The Consumer Credit Act 2006 reformed the 1974 Act by enhancing consumer rights and redress by empowering them to challenge unfair lending and by creating more effective options for resolving disputes; improving the regulation of consumer credit businesses by ensuring fair practices and making regulation more appropriate for different types of consumer credit transaction by extending protection to all consumer credit and by creating a fairer regime for business.[192]

5.3.29 Credit reporting, on the other hand, is primarily dealt with under the Privacy Act and enforced by the Information Commissioner. This position came about when the Data Protection Act was enacted in 1998. It amended sections 158 and 159[193] of the Consumer Credit Act to make

---

191 Sections 157-160 of the Consumer Credit Act 1974 (UK).

192 Clear Start UK Limited ***Consumer Credit Legislation*** 2008 accessed on 20 August 2008.

193 Section 159 of the Data Privacy Act reads as follows (section 62 amendments indicated):

159.—(1) Any individual (the objector) [consumer] given (a) information under section 7 of the DPA Act 1998 by a credit reference agency or (b) information ito section 158, who considers that an entry in his file is incorrect, and that if it is not corrected he is likely to be prejudiced, may give notice to the agency requiring it either to remove the entry from the file or amend it.
(2) Within 28 days after receiving a notice under subsection (l), the agency shall by notice inform the objector [consumer] that it has—
(a) removed the entry from the file, or
(b) amended the entry, or
(c) taken no action,
and if the notice states that the agency has amended the entry it shall include a copy of the file so far as it comprises the amended entry.
(3) Within 28 days after receiving a notice under subsection (2), or where no such notice was given, within 28 days after the expiry of the period mentioned in subsection (2), the objector [consumer] may, unless he has been informed by the agency that it has removed the entry from his file, serve a further notice on the agency requiring it to add to the file an accompanying notice of correction (not exceeding 200 words) drawn up by the consumer, and include a copy of it when furnishing information included in or based on that entry.
(4) Within 28 days after receiving a notice under subsection (3), the agency, unless it intends to apply to the relevant authority [Director] under subsection (5), shall by notice inform the consumer that it has received the notice under subsection (3) and intends to comply with it.
(5) If—

provision for the Data Protection Commissioner (as he then was called) to enforce the privacy provisions in the Act. All the other appeals under the Consumer Credit Act stayed with the Office of Fair Trading.

5.3.30 Under the Data Protection Act, a "data controller" must comply with the data protection principles set out in the Act. These include for eg Data Protection Principle 3 which provides that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

5.3.31 In New Zealand and Canada credit reporting is regulated by these jurisdictions' Privacy Commissioners under the Privacy Act 1993 (NZ) and the Personal Information Protection and Electronic Documents Act 2000 (Canada), respectively.

5.3.32 In Australia the Privacy Act of 1988 is currently being reviewed. It contains a section on credit reporting. In 2006 a report prepared for MasterCard Worldwide (the MasterCard CIE/EDC Report)[194] summarised the key features of the regulatory systems for credit reporting in more than a dozen countries. Although a more comprehensive credit reporting regime is envisaged and it has been considered whether this regime should be dealt with within the context of the privacy legislation or not, the preliminary decision is that credit reporting will remain within the Privacy Act and the Privacy Commission.

b) Evaluation

Written comments

(a) the consumer has not received a notice under subsection (4) within the time required, or
(b) it appears to the agency that it would be improper for it to publish a notice of correction because it is incorrect, or unjustly defames any person, or is frivolous or scandalous, or is for any other reason unsuitable, the consumer or, as the case may be, the agency may, in the prescribed manner and on payment of the specified fee, apply to the relevant authority [Director], who may make such order on the application as he thinks fit.

(6) If a person to whom an order under this section is directed fails to comply with it within the period specified in the order he commits an offence.

(7) The Data Protection Commissioner may vary or revoke any order made by him under this section.

(8) In this section "the relevant authority" means:

a) where the objector is a partnership or other unincorporated body or person,the Director,and

b) in any other case, the Data Protection Commissioner.

194 Centre for International Economics and Edgar Dunn and Company "Options for Implementation of Comprehensive Credit Reporting in Australia" (Prepared fro MasterCard Worldwide) 2006 as referred to in ***ALRC Discussion Paper*** at 1428.

5.3.33 Two aspects were clear from the comments received. First of all, that the credit bureaux fulfilled an important function in the economy of South Africa, but secondly, that there was great dissatisfaction amongst consumers with regard to the way in which the bureaux were being operated.

5.3.34 In this regard, on the one hand, it was emphasised that credit bureaux, world wide, are an indispensable component of the granting of credit. It was stated:[195]

> ..we cannot emphasise enough that the legislators should not introduce any restrictive measures that will have the effect of curtailing the services available from the credit bureaux to credit providers. It is of utmost importance that the system of information sharing be allowed to continue as this is vital to the continued health and sustainability of the banking industry as a whole. If banks are not able to assess and share information relating to defaulting clients, the general public would be detrimentally affected, as the requirements and procedures which banks would have to implement to take on new clients and carry out screening will be costly and much more time consuming than is the practice.

5.3.35 However, on the other hand, individual consumers indicated problems with the credit bureaux centering around the accuracy of the information, the opportunity for correction of data held, openness and transparency regarding the process of collecting the information, and the periods for which the information was held.

5.3.36 Commentators also referred the Commission to the overlap of POPIA with the requirements of the National Credit Act and accordingly reminded it of the necessary amendments to the Act or to the National Credit Act, as the case may be, that would be required to be effected to ensure certainty.[196]

Interim nature of NCA privacy provisions

5.3.37 During the development and drafting of the National Credit Act an agreement was

---

195 Banking Council.

196 Nedbank.

entered into between the Department of Trade and Industry, the Department of Justice and the Commission to the effect that the privacy provisions in the NCA would be regarded as an interim arrangement until the Protection of Personal Information Bill is enacted. This arrangement was formalised in the Dti's policy documents, their submissions to NEDLAC and Cabinet and the report presented to Parliament.[197]

5.3.38 The arrangement is in accordance with similar arrangements with the Department of Communications (ECT Act), the Dti (Consumer Protection Bill) and the Ministry for Intelligence (Protection of Information Bill).

5.3.39 It should, however, at the outset be noted that although POPIA will, in general, be the primary piece of legislation dealing with the protection of personal information, it will not, necessarily, be the only legislation dealing with privacy protection. It is envisaged that the legislative framework for privacy protection will be composed of POPIA, in conjunction with sectoral legislation, codes of conduct and regulations. Of utmost importance is, however, that any other applicable legislation will also have to comply with the international prescripts for the adequate protection of personal information and that compatibility of the various legislative instruments will have to be ensured.

Relationship between privacy principles and other legislation

5.3.40 POPIA has been drafted with the object of providing South Africa with an EU adequacy rating in order to ensure the free flow of transborder information.[198] Articles 25 and 26 of the EU

---

197 Department of Trade and Industry in para 3.12 to 3.15 of its Policy Framework for Consumer Credit stated as follows:

> .....It is recognised that there is a need for the much more extensive regulation of credit bureaux. However, the Department of Justice, through the Law Commission, has initiated a process to draft new privacy legislation, which will also capture the regulation of credit bureaux and credit information. In order to minimise potential duplication and regulatory conflict, the more extensive regulation of these institutions will be left to privacy regulation. It is further envisaged that provisions concerning credit bureaux in new credit legislation will eventually be taken over in new privacy law.

The regulatory scheme for credit bureaux were expanded during the legislative process due to the concern that there should be adequate interim regulation of credit bureaux. However, the interim nature of the provisions was once again confirmed by the Deputy-Director General: Consumer and Corporate Regulation of the DTI in a letter to the Office of the State Law Adviser, dated 15 May 2005.

198 For further discussion see Chapter 6 below.

Directive stipulate that personal information should only flow outside the boundaries of the European Union to countries that can guarantee an "adequate level of protection" (or the so-called safe-harbour principles).

5.3.41 POPIA, therefore, embodies a set of eight internationally accepted privacy protection principles. Both the European Union and the Organisation for Economic Co-operation and Development (OECD) require compliance with these principles. The Act is applicable to both the public and the private sector and all regulatory aspects of personal information of data subjects (consumers) will be dealt with by an Information Regulator appointed in terms of the Act. [199]

5.3.42 The question arises how the privacy principles dealing with the processing of all personal information should relate to sectoral legislation that deals with particular types or aspects of privacy protection such as credit reporting. Should credit reporting therefore be regulated by a one size fits all model in the privacy principles or by sectoral legislation tailored to credit reporting, or a combination of both.

5.3.43 There are in essence three possibilities for reform:

a) First, credit reporting could be excluded from POPIA in terms of section 4 given that it is being dealt with elsewhere.
b) Secondly, the privacy protection sections in the National Credit Act could be repealed with POPIA then providing the sole form of regulation in respect of all forms of credit reporting.
c) Thirdly, the privacy principles could regulate credit reporting except to the extent that more specific sectoral legislation, the NCA, covers particular aspects of credit reporting.

5.3.44 In evaluating these options the following aspects will have to be considered irrespective of which option is chosen:

a) All the privacy principles have to be accommodated in legislation;
b) All the responsible parties involved in the sector have to be covered by the legislation;
c) Compliance with paras (a) and (b) should both be ensured at every stage in the process.

---

199 See a discussion of the Privacy Principles in Chapter 4 above.

5.3.45 The Credit Bureau Association has indicated in their submissions that the privacy principles contained in POPIA, when given effect to within the credit information system, would place certain obligations upon the credit granting industry (subscribers of the bureaux) and the credit bureau industry. The principles would place the following obligations on credit providers who are the source and primary users of personal information within the credit information industry:

a) To obtain the data directly from the data subject where possible;
b) At the time of collection, which would be on application of credit, the credit grantor would have to, through the credit application form, notify the data subject of the collection, the specified purpose/s of the collection, the uses the data may be put to and to whom it will be disclosed. Provision will then be made for "opt-out" consent;
c) The credit provider will have to ensure that the data supplied to the credit bureaux is valid (that is information in respect of valid debts), accurate, up-to-date, relevant (in relation to the purpose/s for which it is collected) and complete;
d) The credit provider will have to give 20 days notice to a data subject prior to transferring default (adverse) information on the data subject to a credit bureaux;
e) The credit provider will have to guarantee the security of the information and take responsibility for its destruction when necessary.

5.3.46 The Credit Bureau industry will then have the following obligations:[200]

a) Ensuring that data is accurate, complete and up-to date as is necessary for the purposes it was collected for, through effective and high quality data processing systems ; and to ensure that data is processed for the legitimate specified purposes;
b) Giving access to data subjects to their credit reports to give effect to the rights of verification and objection;
c) Ensuring high quality data security systems;
d) Ensuring that the data is removed from display and not used for assessing credit risk once the data retention period has lapsed;[201]
e) Providing a statement of their functions and activities for inspection by the data protection

---

200 Credit Bureau Association.

201 The information may be kept for statistical analyses and score card development past the display period.

authority, because of competition and legitimate business this information cannot be made public knowledge; and

f) Reporting to the data protection authority on the results of the independent audit of its data processing and data security systems.

5.3.47 In considering the privacy provisions set out in the NCA and Regulations and comparing them with the obligations for credit providers and credit bureaux in terms of the privacy principles set out directly above, it is clear that the legislation falls short in all the categories mentioned in par 5.3.43 above.

5.3.48 The NCA and Regulations do not, for instance, deal effectively, or in some instances, at all, with the collection limitation principle (Principle 2), purpose specification (Principle 3),[202] further processing (Principle 4), openness (Principle 5) and accountability of responsible parties (Principle1) principles. [203] Neither trans-border transfer of information (section 69 of POPIA) nor automated decision making (section 68 of POPIA) has been addressed.

5.3.49 The Act, itself, is, furthermore, only applicable to credit bureaux in so far as privacy protection is concerned, and even in the Regulations, only limited provision has been made for the accountability of credit providers. The NCA jurisdiction over juristic persons is, furthermore, limited to a threshold of R1 million turnover. All other juristic persons will not be covered by the NCA which creates a loophole.[204]

---

202 Principles 2 and 3 of POPIA deal with "purpose specification". Information must be collected for a specific purpose of which the consumer must be aware at the time and may not be processed further for a purpose that would be incompatible with the purpose for which it was originally collected. Further processing is therefore linked to the original purpose of collection and not necessarily to consent.

203 For eg, in section 68 four privacy principles have been condenced into one short section, only mentioning issues that have been dealt with in detail in the POPIA. The manner of collecting of personal information with the permission or knowledge of the data subject is, for instance, an important principle in data protection which has not been dealt with at all. POPIA refers to the "processing"of information and this definition, set out in section 2 of the Bill, includes the collection, recording, organisation, storage, updating, modification, retrieval, consultation, use, dissemination, distribution, merging, linking, blocking, erasure and destruction of information. Section 68 only refers to a person which "receives, compiles, retains or reports" information. "Receiving" and " compiling" of information already refers to the secondary processing of information. The limitations with regard to "receiving" and "compiling" information are accordingly concerned only with this secondary purpose and processing for the "primary purpose" of collection is by implication allowed unchallenged. In terms of section 68 it is therefore not necessary to protect the confidentiality of information where it is being collected or destructed. Although a half-hearted attempt has been made in the Regulations to rectify the situation, this has not been successful and many regulatory gaps exist.

204 Service providers such as Vodacom may not be subject either.

5.3.50 In so far as the third category referred to in para 5.3.43 is concerned, the drafters of the credit legislation seems not to have taken cognisance of the fact that the credit information cycle that needs to be protected, starts off with the collection of personal information by credit providers when they first apply for credit.

5.3.51 The NCA does not, therefore, comply with international prescripts for the protection of personal information and will not be able to operate independently without POPIA if the objects of the Act is to ensure proper privacy protection for consumers in the credit industry and an EU adequacy rating for South Africa.

5.3.52 Repealing the privacy protection sections in the NCA and depending exclusively on POPIA for protection of credit information is a possibility. However, it is not in line with the spirit of the Bill which makes provision for POPIA to be a generic Act being implemented in conjunction with sector specific legislation and codes of conduct.

5.3.53 It, therefore, seems as though option 3 (a dual regulatory system including both the NCA and POPIA) would be the appropriate choice. However, aspects of such a dual protection system that should be considered are the following:

a) First, there may be overlapping rules where a responsible party subject to the NCA also falls within the ambit of POPIA. When using information contained in a credit report, a bank, finance company or other credit provider must comply with both NCA and POPIA. Banks, finance companies and other credit providers would have to deal with two statutory privacy regimes - that is, specific rules in relation to credit reporting and the generic rules set out in POPIA in relation to other aspects of handing personal information.
b) On the other hand, the handling of other personal information relevant to credit worthiness by a credit provider, such as that obtained solely from the credit provider's own records, may be covered only by POPIA.
c) Difficulties in regulating credit reporting as an industry matter rather than regulating the handling of personal information used in credit reporting may include inconsistency and fragmentation, increasing the complexity of privacy regulation, varying levels of privacy protection and regulatory gaps.
d) POPIA is, furthermore, much more comprehensive than the NCA. POPIA makes extensive

provision for education of responsible parties (credit providers and bureaux) and data subjects (consumers), mediation and conciliation of disputes between opposing parties (credit providers, bureaux and consumers), prior assessments (of credit bureaux before they are allowed to start operations, especially where they do not subscribe to a code of conduct), disclosures (where security has been breached - this has been found to be more effective than criminal sanction) , enforcement notices etc.

c) Recommendation

5.3.54 It is the Commission's recommendation that POPIA should set out general requirements with respect to credit reporting. However, these requirements should be able to be displaced by more specific legislation that deals with the particular aspect of privacy protection found in credit reporting. This would allow for the prescripts in POPIA to operate alongside the more specific provisions of the NCA and its Regulations. This arrangement is also in accordance with similar arrangements in other sectors such as direct marketing information, health information, electronic communications. etc.

5.3.55 It is therefore recommended that no exclusion should be provided for the credit reporting industry in terms of section 4 of POPIA and that the credit reporting industry should fall within the ambit of POPIA. The NCA should be scrutinised to ensure that any discrepancies with POPIA (and accordingly with the internationally accepted privacy principles) are remedied in consequential amendments to the NCA. (An initial evaluation of the sections in the NCA seems to suggest that it is not so much any discrepancies that may result in problems, but rather the fact that the NCA does not deal comprehensively enough with the privacy provisions.) Note should be taken that the NCA should only particularise and complement the privacy principles.[205]

5.3.56 The Commission acknowledges that the creation of a multiplicity of processes and regulators for the protection of personal information will not be cost-effective and will create uncertainty for consumers (data subjects) to know where their remedies lie. A situation where

---

205 See discussion in par 5.3.17 and further.

one set of circumstances gives rise to various remedies in terms of different pieces of legislation and where the consumer has to approach more than one regulator in order to address each aspect of his or her problem, has to be avoided.

5.3.57 It is therefore proposed that the UK example be followed and that section 55 of the NCA be amended to distinguish between compliance notices issued, on the one hand, for failure to implement privacy protection provisions and, on the other, for non-compliance of the other provisions of the Act. The Information Protection Regulator to be given the authority to issue notices in terms of section 55 where the protection of privacy is at stake.

5.3.58 Finally, it should be noted that the National Credit Regulator will be accountable in terms of POPIA, in so far as its duties and obligations as the responsible party, processing information for the National Credit Register, is concerned.

CHAPTER 6: CROSS-BORDER INFORMATION TRANSFERS

6.1 Globalisation, the growth of the Internet and falling communication costs dramatically increase the amount of personal information flowing across borders.[1] This increase in transborder information flows benefits both organisations and individuals by lowering costs, increasing efficiency and improving customer convenience. At the same time, these personal information flows elevate concerns about privacy, and present new challenges with respect to protecting individual's personal information.[2]

6.2 Since cross-border information transfers by definition refers to the movement of personal information across national borders, it is to be expected that every time goods are ordered from a merchant outside the country, some personal information crosses the border– or crosses borders. More and more, however, personal information also crosses borders during business transactions conducted in a country, internally. For example, where an email is sent across town, it's likely to reach its recipient having first travelled outside the country, perhaps even around the world. To take another example, if a credit card is used to buy something from a bricks-and-mortar merchant in one country, the card issuer may well ship one's personal information abroad for processing. The central question is, therefore, "what privacy standards should apply to the transfer of personal data, and to its use and protection, wherever the data might end up?"[3]

---

1 ***ALRC Disussion Paper*** at 816 refers as follows to Sainty K and Ailwood A "Implications of Transborder Data Flow for Global Business" (2004-2005)1 ***Privacy Law Bulletin*** 101: Modern business is increasingly borderless. The communications revolution and the reduction in international trade barriers has allowed business to globalise and for regions to specialise. The call centre answers the phone in India, the product is designed in Europe, made in China and it is all managed from the USA. But these business units must share information, information about employees, customers and suppliers.

2 OECD ***Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*** 12 June 2007 (hereafter referred to as "***OECD Cross-border Recommendation***"). Recommendation developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP).

3 Loukidelis D "Transborder data flows & privacy—an update on work in progress" 7th Annual Privacy & Security Conference Victoria BC February 10, 2006.

a) Proposals in the Discussion Paper

International Instruments

6.3 The importance of harmonising the laws of different countries dealing with the protection of information was already acknowledged in the eighties. The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the Council of Europe Convention for the protection of Individuals with regard to the Automatic Processing of Personal Data, 1981 were the first international instruments to make provision for a set of internationally accepted privacy principles to be incorporated in national legislation.[4]

6.4 The OECD Guidelines were designed to promote international harmonisation of privacy protection while protecting the free flow of personal information. They expressly acknowledged the growth of transborder data flows and their implications for both privacy and commerce. They explicitly recognized the need to forestall inappropriate barriers to transborder data flows and thus economic activity. These features of the Guidelines are illustrated by the following quote from the preface to the Guidelines:

> .....there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance. For this reason OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data.

6.5 In 2007 the OECD also published a recommendation,[5] inter alia advising member countries and their privacy enforcement authorities to co-operate with each other to address cross-border aspects arising out of the enforcement of laws protecting privacy. It indicated that such co-operation may be facilitated by appropriate bi-lateral or multi-lateral enforcement arrangements.

---

4 See discussion in Chapters 1 and 4.

5 OECD ***Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*** 12 June 2007.

6.6 The CoE Convention, which has been initiated from a human rights perspective, also promotes the harmonisation of laws by providing for privacy principles to be incorporated in national legislation. The effect of the OECD Guidelines and the Convention principles are, in principle, the same. However, the Convention only made specific provision for the institution of provisions for cross-border transfers in 2001 when an Additional Protocol was adopted for this purpose. [6]

6.7 See also Principle 9 of the UN Guidelines. The latter differ in some respects from the other instruments in their terminology - employing the (undefined) criteria of "comparable" and "reciprocal" protection - though they probably seek to apply essentially the same standards as the criteria of "equivalency" and "adequacy". At the same time, while the Convention and OECD Guidelines have been primarily concerned with regulating flow of personal data between the member states of the CoE and OECD respectively, the UN Guidelines seek to regulate information flows between a broader range of countries.[7]

6.8 However, as was indicated in the Discussion Papers, the ease with which electronic data flows across borders lead to a concern that information protection laws could be circumvented by simply transferring personal information to other countries, where the national law of the country of origin does not apply. This information could then be processed in those countries, frequently called "information havens", without any limitations.

European Directive

6.9 In order to amplify and give substance to the Convention, the European Commission adopted Directive 95/46/EC on data protection which, by coordinating the laws of members states, aimed to ensure that the cross-border flow of personal data is regulated in a consistent manner and the possibility of "information havens" minimised.

Article 25 of the Directive

---

6 See discussion in Chapter 4 above.

7 See Bygrave ***Data Protection*** at 8.

6.10 Article 25 of the European Directive[8] imposes an obligation on member states to ensure that any personal information relating to European citizens is protected by law when it is exported to, and processed in, countries outside Europe (so-called "third countries").

6.11 As a first step, the European Union and all its trading partners have been required to have adequate information protection regimes, conforming to the European Data Protection Directive, with effect from 24 October 1998.

6.12 Article 25, paragraph (1), furthermore, sets out the principle that member states shall only allow a transfer to take place if the third country in question ensures an adequate level of protection. Paragraph (2) explains that "adequacy"should be assessed on a case by case basis "in light of all the circumstances surrounding a data transfer operation or set of data transfer operations". Paragraph (6) provides that the Commission may determine that certain countries offer adequate protection.[9]

6.13 The Directive does not define "transfer", but the ordinary meaning of the word is transmission from one place, person, etc to another.[10] In order to decide whether a "transfer"

---

8 The following clauses from the Directive govern the transfer of information:
CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES
Article 25
Principles
1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.

9 European Union Art 29 Working Party ***Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*** WP 12 Working Document adopted by the Working Party on 24 July 1998 (DG XV D/5025/98) (hereafter referred to as "WP12") at 3.

10 Information Commissioner ***Data Protection Act 1998: The Eighth Data Protection Principle and International Data Transfers*** 30 June 2006 (hereafter referred to as " ***ICO Data Protection Act***") at 5; See also ***ALRC Discussion Paper*** at 826 for distinction between 'transfer", "use" and "disclosure".

has taken place one must determine whether information has been sent to a recipient in another country. This is not the same as the transit of information through a country. If personal information is, for eg, transferred from country A to country B via a server in country C and no access to or manipulation of the information happens in country C, then the transfer is only to country B. Putting personal information on a web site will often result in transfers to countries outside the EU. The transfers will take place when the web site is accessed by someone outside the country of origin. [11]

6.14 In the case **Bodil Lindqvist v Kammaraklagaren**,[12] the European Court of Justice held that there was no transfer of personal data to a third country where an individual loaded personal data onto an internet page in a member state using the internet hosting provider in that member state, even though the page was accessible via the internet by people based in a third country. A transfer was only deemed to have taken place where the internet page was actually accessed by a person located in a third country. However, where data is loaded on the internet with the *intention* that the data be accessed in a third country, this will usually lead to a transfer and the principle in **Lindqvist** will not apply. It is also important to note that even where no access has taken place, responsible parties will still need to ensure that the processing complies with all the other Information Protection Principles.[13]

6.15 A decision of whether or not there is adequacy may be based on a Community finding of adequacy or after assessment of adequacy made by the responsible party itself. [14]

6.16 In terms of Article 25(6) the Article 29 Working Party may determine that certain third countries ensure an adequate level of protection.[15] A positive finding should not in principle be limited to countries having horizontal data protection laws, but should also cover specific sectors within countries where data protection is adequate, even though in other sectors the same

---

11 See Information Commissioner ***International Transfers of Personal Information: General Advice on How to Comply with the 8th Data Protection Principle*** Data Protection Guidelines 31 August 2007 (hereafter referred to as "***UK Guidelines on International Transfers***") at 2.

12 ***Bodil Lindqvist v Kammaraklagaren*** (2003) (Case C-101/01) as referred to in ***ICO Data Protection Act*** at 5 .

13 ***ICO Data Protection Act*** at 6.

14 ***ICO Data Protection Act*** at 7.

15 Where a country is not found to have adequate protection, this need not imply that the country is implicitly or explicitly "blacklisted". The public message would rather be that no general guidance regarding that particular country is yet available.

country's protection may be less than adequate. [16]

6.17 Where the European Commission has made a finding that a third country does or does not ensure adequacy, any question as to whether there is adequacy during transactions will be determined in accordance with that finding.[17] In July 2007, the EU and the USA signed an agreement to legitimise and regulate the transfer of passenger name record information (PNR)[18] from the EU Airlines to the US Department of Homeland Security.[19]

6.18 In practice the transfer of information from the EU to both private and governmental bodies will normally only be permissible with countries which have acceptable information protection legislation or self regulation covering the information protection principles outlined in Chapter 4 above.[20]

6.19 However, where the data protection regime in the third country has not been subject to a Commission finding of adequacy, it may be possible for the responsible exporting party to assess adequacy in a way that is consistent with the Directive. [21]

6.20 All the circumstances surrounding the data transfer must be taken into account. Factors that must be given particular consideration are the nature of the data; the purpose and duration

---

16 WP12 at 27.

17 ***ICO Data Protection Act*** at 7; The following countries are considered adequate: Argentina, Canada, Guernsey, Isle of Man, Switserland; Safe harbor arrangement of the USA.

18 PNR's are the records about each airline passenger that will be used for the USA government's Secure Flight (formerly named "CAPPS-II) passenger surveillance and profiling system and "no fly" lists, and compiled into the Passenger and Aviation Security Screening Records (PASSR) database of the Transportation Security Agency (TSA), a division of Homeland Security. PNR's are airline records, but few airlines host their own databases. Most airlines store their PNR's in a "virtual partition" in the database of a Computerised Reservation System (CRS). There are only four major CRS's worldwide: SABRE travel Network, Galileo/Apollo, Amadeus and Worldspan. CRS's have the same relationship to travel data that credit bureaux have to financial data: they centralise and store vast amounts of information about persons, but they get the information through intermediaries; they remain in the background and they have minimal direct contact with people on whom they keep files. CRS's don't just store data, they also are the centre of travel networking. They connect airlines to each other, to travel agencies, car rental companies, hotels, cruise lines, tour operators and other providers of travel services. Whenever a person makes a reservation, a PNR is created. If you are a regular traveller with an airline or travel agency, your account information is typically stored in a "profile" in the CRS. The profile may include all the credit cards you regularly use, alternate addresses, phone numbers, emergency contacts, names and other information on your family members, business associates who sometimes travel with you, your tastes and preferences ("prefers king-size bed", prefers "room on low level of hotel", "wont' fly on Jewish sabbat", "always requests halaal meal", "uses wheelchair, can control bowels and bladder", etc. Information from many different sources is gradually added to the profile through different channels over time. Advance Passenger Information (API) is one of the categories of data in the PNR.

19 ***UK Guidelines on International Transfers*** at 4.

20 See also DMA Submission on Open Democracy Bill.

21 ***ICO Data Protection Act*** at 8.

of the proposed processing operation ; the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question; and the professional rules and security measures which are complied with in that country.[22]

6.21 According to the Article 29 Working Party[23] any meaningful analysis of adequate protection must comprise two basic elements:

a) an assessment of the content of the rules applicable (information protection principles); and

b) an assessment of the means for ensuring their effective application (procedural enforcement mechanisms).[24]

6.22 A core of data protection content principles can be identified, compliance with which could be seen as a minimum requirement for protection to be adequate. These principles are the following:[25]

a) The purpose limitation principle;

b) The data quality and proportionality principle;

c) The transparency/openness principle;

d) The security and confidentiality principle;

e) Rights of access, rectification and opposition;

f) Restrictions on onward transfers;

g) Sensitive data;

h) Direct marketing; and

i) Automated individual decision making.

6.23 In so far as the enforcement mechanisms are concerned, the objectives of a data

---

22 Article 25 (2).

23 WP12 at 5.

24 The UK Commissioner's Office suggests the following questions to determine compliance with the UK's 8th data protection principle:
(a) Is it possible to fulfil your objectives without transferring personal information;
(b) Is there actually a transfer of personal information taking place;
(c) Is the destination country outside the EEA;
(d) Has the country been confirmed as "adequate" by the European Commission;
(e) Are there other ways to achieve adequacy;
(f) Do any of the exemptions apply.
See ***UK Guidelines on International Transfers*** at 1.

25 For a discussion on each of these principles see Chapters 4 and 5 above.

protection system are essentially threefold:[26]

a) to deliver a good level of compliance with the rules;

b) to provide support and help to individual data subjects in the exercise of their rights; and

c) to provide appropriate redress to the injured party where rules are not complied with.

6.24 It should be noted[27] that Article 25 requires an adequate level of protection, not a comparable level or similar level.[28]

6.25 Information sharing now takes place on an international scale and involves a tremendous amount of personal information. Information regarding credit transactions, for example, flows routinely from the country where charges are incurred to the country where the bill is ultimately settled. A broad ban on the transfer of information to third countries would therefore be disruptive and expensive. In light of these economic realities, the Directive provides certain exemptions to the provisions of Articles 25 and 26. In terms of these exemptions adequacy is determined in each individual case or with regard to individual bodies.

Article 26 of the EU Directive

6.26 Article 26 identifies the circumstances under which an EU member nation can authorise transfer in the absence of an adequate level of information protection.[29] It, therefore, makes

---

26 WP12 at 7.

27 Fisher R Excerpt from ***Privacy of Personal Information and the National Information Infrastructure*** as referred to in a fax received from ITC Consumer Liaison (hereafter referred to as "Fisher excerpt").

28 See Roos A "Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position" ***SALJ*** Vol 124 Part 2 2007 400 (hereafter referred to as "Roos ***SALJ*** 2007") at 411 and reference to the criticism noted by European commentators of the "adequacy standard" since it sets a more lenient standard for countries outside the EU than for member states.

29 Art 26 provides as follows:

provision for derogations (exemptions) from Article 25.

6.27 Article 26 (1) provides for instances where wider protection of personal information is not necessary such as where the data subject has unambiguously given consent to the transfer (it is not clear whether assent is required, or if notice with the opportunity to opt out is sufficient).

6.28 Article 26 (2) makes provision for instances where wider protection is not available, but where alternative protection is provided for eg. where the company receiving the information establishes privacy rights through appropriate contractual clauses.[30]

Article 26(1) exemptions

6.29 Article 26(1) of the Directive sets out a limited number of situations in which an exemption from the "adequacy" requirement for third country transfers may apply. These

---

Article 26 Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) 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
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) 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.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces 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; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).
Member States shall take the necessary steps to comply with the Com mission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

30 See further Bygrave ***Data Protection*** at 82; Bennett CJ "Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada" August 1997 available at http://web.uvic.ca/~polisci/bennett/research/iso.htm at 9.

exemptions mostly concern cases where the risks to the data subject are relatively small or where other interests (public interests or those of the data subjects themselves) override the data subject's right to privacy. As exemptions form a general principle, they must be interpreted restrictively.[31]

6.30 The first exemption covers cases where the data subject gives his or her consent unambiguously to the proposed transfer. The consent must be freely given, specific and informed.[32]

6.31 The second and third exemptions cover transfers necessary either for the performance of a contract between the data subject and the responsible party or for the conclusion of a contract concluded in the interest of the data subject between the responsible party and a third party. These exemptions appear potentially quite wide, but their application in practice is likely to be limited by the "necessity " test: all the information transferred must be necessary for the performance of the contract. It will be applicable, for eg. to those transfers necessary to reserve an airline ticket for a passenger or to transfers of personal information necessary for the operation of an international bank or credit card payment.[33]

6.32 The fourth exemption has two strands. The first covers transfers necessary or legally required on important public interest grounds. A simple public interest justification for a transfer does not suffice, it must be a question of important public interest. Recital 58 suggests that information transfers between tax or customs administrations or between services responsible for social security will generally be covered.[34] This is a high threshold to meet.[35]

6.33 On this point the drafters of the Directive clearly did envisage that only important public interests identified as such by the national legislation applicable to responsible parties

---

31 WP 12 at 24; Where these exemptions are used there is not necessarily any protection in place in relation to the information being transferred. Instead, these provisions reflect the fact that there are instances where it will be justifiable to transfer information even though there will be a lower level of protection given to these information. As such, in interpreting these provisions, the exemptions should be narrowly construed. See ***ICO Data Protection Act*** at 22; See also ***ALRC Discussion Paper*** at 821: Where one of the conditions in (a) to (f) is satisfied, the responsible party transferring the information is not liable for subsequent privacy breaches. It is important, therefore, that these conditions are sufficiently stringent to prevent transfers that create unwarranted privacy risks.

32 WP 12 at 24.

33 WP 12 at 24.

34 WP 12 at 25.

35 ***UK Guidelines on International Transfers*** at 12.; ***IOC Data Protection Act*** at 25. It is the public interest in the UK that should be considered, not that of the third country.

established in the EU are valid in this connection. Any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in the Directive.[36]

6.34 The second strand concerns transfers taking place in the context of international litigation or legal proceedings, specifically transfers that are necessary for the establishment, exercise or defence of legal claims.[37]

6.35 The fifth exemption concerns transfers necessary in order to protect the vital interests of the data subject. An obvious example would be the urgent transfer of medical records to a third country where a tourist had previously received medical treatment in the EU and has suffered an accident or has become dangerously ill. Recital 31 of the EU Directive interprets "vital interest" fairly narrowly as an interest "which is essential for the data subject's life". This would therefore exclude for eg, financial, property or family interests. [38]

6.36 The sixth exemption concerns transfers made from registers intended by law for consultation by the public, provided that in the particular case the conditions for consultation are fulfilled. Recital 58 makes it clear that entire registers or entire categories of data from registers should not be permitted to be transferred under this exemption.[39]

6.37 Where responsible parties use operators in third countries to carry out processing on their behalf, they will remain the responsible parties in terms of the privacy legislation. They will therefore be responsible to comply with all the provisions of the applicable legislation in the country from where the information is transferred. The responsible party's liability remains unchanged, even where the processor subcontracts the processing of the information to another processor.[40]

6.38 When applying the exemptions, exporting responsible parties should be aware that even

---

36 European Union Article 29 Data Protection Working Party ***Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*** Adopted on 22 November 2006 WP128 (01935/06/EN) at 24.

37 WP 12 at 25.

38 WP 12 at 25.

39 WP 12 at 25.

40 ***IOC Data Protection Act*** at 30.

though they may be exempted from the section dealing with transborder information flows, the Information Protection Principles will still be applicable.[41]

Article 26(2) (Contracts)

6.39 It is therefore possible to protect the privacy of information transferred to countries that do not provide "adequate protection" by relying on a private contract[42] containing standard information protection clauses.[43] This kind of contract would bind the responsible party to respect fair information practices such as the right to notice, consent, access and legal remedies. In the case of information transferred from the European Union, the contract would have to meet the standard "adequacy" test in order to satisfy the EU Directive.[44]

6.40 The requirements for a contractual solution correspond to the requirements for an adequate legislative solution set out above. The contract should therefore contain a series of basic data protection principles[45] together with certain conditions necessary to ensure their effectiveness.[46]

6.41 The same criteria set out for determining the effectiveness of a data protection system apply. However, providing a legal remedy to a data subject by way of contract between the transferer of the data and the recipient is not a simple question. Much will depend on the nature of the contract law chosen as the national law applicable to the contract. The applicable law will generally be that of the member state in which the transferer is established. The contract law of some member states permits the creation of third party rights, whereas in other member

---

41 See ***IOC Data Protection Act*** at 22.

42 Article 26(2). However, the idea of using contracts as a means of regulating international transfers of personal information was not invented by the Directive. Already in 1992 the Council of Europe, the International Chamber of Commerce and the European Commission were jointly responsible for a study of the issue. See "Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum" Strassbourg 2 November 1992 as referred to in WP 12 at 15.

43 Article 26(4) gives a power to the EU Commission, acting in accordance with the procedure laid down in Article 31, to decide that certain standard contractual clauses offer the sufficient guarantees envisaged in Article 26(2).

44 EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 16. In intra-Community flows of data, contracts could also be used to determine how the responsibility for data protection compliance is split between two parties where more than one responsible party is involved. See WP 12 at 16.

45 In some situations additional principles relating to sensitive data, direct marketing and automated decisions must be applied.

46 WP 12 at 17.

states this is not possible.[47]

6.42 As a general rule, the more the recipient is limited in terms of his freedom to choose the purposes, means and conditions under which he processes the transferred data, the greater will be the legal security for the data subject. The preferred solution will, therefore, be to provide the recipient of the transfer with no autonomous decision-making power in respect of the transferred data. The recipient is bound to act solely under the instructions of the transferer, and while the information may have been physically transferred outside the EU, decision making control over the data remains with the entity who made the transfer. The law of the member state in question will, therefore, continue to apply to the processing carried out in the third country.[48]

6.43 However, where the recipients have rented or bought the information to use it for their own benefit and purpose this solution will not work. Some legal systems allow third parties to claim rights under a contract to which they are not parties and this could be used to create data subject rights under a contract. Another possibility is for the transferer to enter into a separate contractual agreement with the data subject stipulating that the transferer will remain liable for any damage or distress caused by the failure of the recipient of a data transfer to comply with the agreed set of basic data protection principles. The data subject is, therefore, granted a means of redress against the transferer.[49]

6.44 A specific difficulty with the contractual approach is the possibility that the general law of a third country may include requirements for the recipient of a data transfer, in certain circumstances, to disclose personal data to the state (the police, the courts and the tax authorities, for eg) and that such legal requirements may take precedence over any contract. Under the Directive certain limitations are set out which would provide a specific context within which the state's ability to require the provision of personal information from companies and other organisations to operate. Similar limitations may not be in place in third countries. The contract may therefore be too frail an instrument to offer adequate information protection safeguards and transfers to certain countries should not be authorised.[50]

6.45 Contractual solutions would probably be best suited to large international networks

---

47 WP 12 at 17.

48 WP 12 at 18.

49 WP 12 at 19.

50 WP 12 at 22.

(credit cards, airline reservations) characterised by large quantities of repetitive data transfers of a similar nature, and by a relatively small number of large operators in industries already subject to significant scrutiny and regulation.[51]

Model/Standard contractual clauses

6.46 In the absence of global data protection standards, standard contractual clauses provide an important tool allowing the transfer of personal data from all member states under a common set of rules.[52] Commission Decision 2001/497/EC[53] under Directive 95/46/EC therefore lays down a model set of standard contractual clauses which ensures adequate safeguards for the transfer of information to third countries.[54]

6.47 Since the adoption of this Decision, a coalition of business associations[55] has submitted a set of alternative, additional standard contractual clauses designed to provide a level of data protection equivalent to that provided for by Decision 2001/497/EC while making use of different mechanisms (more flexible auditing requirements and more detailed rules on the right to access). These recommendations have been incorporated in Commission Decision 2004/915/EC[56] and it therefore amends Decision 2001/497/EC accordingly. [57]

---

51 WP 12 at 23.

52 A number of model clauses that could be included in such a contract were outlined in a 1992 joint study by the Council of Europe, the European Commission and the International Chamber of Commerce. Joint Study of the Council of Europe and the Commission of the European Communities (1992), available at http://www.coe.fr/dataprotection/Etudes_Rapports/ectype.htm; See also "Model clauses for use in contracts involving transborder data flows" prepared by the Working Party on Privacy and Data Protection of the Commission on Telecommunications and Information Technologies of the International Chamber of Commerce.

53 European Commission Decision 2001/497/EC on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries 15 June 2001.

54 The model clauses contain obligations on both the data exporter and data importer to ensure that the transfer complies with the standards required by the Directive and the data subject has a right to directly enforce its rights under them. Under the Set I controller-controller model clauses, the data exporter and data importer are jointly and severally liable to the data subject for any damage it suffers of a breach by either party of those of the model clauses under which the data subject is a beneficiary. ("third part beneficiary clauses").

55 The International Chamber of Commerce (ICC),Japan Business Council in Europe (JBCE), European Information and Communications Technology Association (EICTA), EU Committee of the American Chamber of Commerce in Belgium (Amcham),Confederation of British Industry (CBI), International Communication Roundtable (ICRT) and the Federation of European Direct Marketing Associations (FEDMA).

56 European Commission Decision amending Decision 2001/497/EC as regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (2004/915/EC) 27 December 2004.

57 In terms of Set II controller-controller (responsible party-responsible party) model clauses the data subject can only enforce its rights against the party who is responsible for the relevant breach. The Set II clauses also give the data importer greater discretion in deciding how to comply with data protection laws and how to respond to subject access requests.

6.48 Commission Decision 2002/16/EC[58] furthermore makes provision for approved model clauses for transfers from responsible parties in the EEA to data processors (referred to as "operators" in POPIA) outside the EEA.[59]

6.49 Data exporters may choose which set of clauses they want to use, if any.[60] However, as each set forms a model, it is not possible to amend these sets or totally or partially merge them in any manner.[61] A data exporter who uses these model clauses does not need to make a separate assessment of adequacy in relation to the transfer.[62]

6.50 This approach to data protection to some extent represents a shift away from traditional models of centralized, state-driven enforcement. Under the contract clauses approach, businesses involved in a data transfer will look to the contract clauses for the rules that regulate their behaviour. They will also look to the contract for dispute resolution mechanisms. Dispute resolution of this kind is more and more the province of massive global law firms brought in by the parties to arbitrate a dispute. This does not by any means displace data protection authorities' role. In fact, it will often be a data protection authority investigation that triggers the dispute between the parties to the transfer, who will look to the contract to sort out responsibility as between themselves.

Binding corporate rules

6.51 Similar observations can be made about what are known as binding corporate rules, or global privacy codes. Under this approach, internationally active companies like Microsoft, Oracle or Procter and Gamble, doing business in multiple countries, are able to develop a global privacy code for the corporation and then commit to implementing it at the global level.[63]

---

58 European Commission Decision 2002/16/EC on Model Clauses for Transfers from Responsible Parties in the EEA to Data Processors dated 27 December 2001.

59 Under the controller-processor (responsible party-operator) model clauses, the data exporter is liable to the data subject for any breach by either party of the third party beneficiary clauses except in limited circumstances. However, if the breach was caused by the data importer, the data importer is required to indemnify the data exporter to the extent of its liability to the data subject.

60 The model clauses are attached as an annexure to the EC Decisions of adequacy which approve their use and can be found on the web site at www.europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm.

61 ***UK Guidelines on International Transfers*** at 7.

62 ***ICO Data Protection Act*** at 16.

63 Wugmeister M, Retzer K & Rich C "Codes of Conduct: The Solution for International Data Transfers?" ***Morrison & Foerster Legal Updates & News*** July 2003 (Article first published in WDPR, June 2003, reprinted with permission of publisher) accessed at http://www.mofo.com/tools/print.asp?mofo_dev/news/updates/files/update1170.html

The key is to have the code acknowledged, or even certified, by data protection authorities as meeting local requirements. Given the growing number of cross-border information transfers, the idea of relying on global rules for all cross-border information transfers is attractive.

6.52 The Directive initially, already made provision for and encouraged members to make use of codes of conduct. The primary obstacle to using codes of conduct for cross-border transfers was that there was no streamlined mechanism for approving enterprise-wide codes.

6.53 A solution to this problem was found in 2003 by the Article 29 Working Party in its working document on binding corporate rules.[64]

6.54 Note should also be taken of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of June 2007 that makes provision for member countries to cooperate across borders in the enforcement of laws protecting privacy.

Accountability

6.55 It has been noted that it is very difficult to impose legal responsibility on an out of the country recipient of personal information to process that information in a manner that is consistent with the privacy principles in the transferor's country. It is only possible to take action against the transferor.[65]

6.56 The APEC Privacy Framework makes provision that, once a responsible party has collected information, it remains accountable for the protection of that personal information even if the information changes hands or moves from one jurisdiction to another.[66] Responsible parties must therefore, mitigate their liability in contractual arrangements with the recipient of the personal information. The advantage of such a system is that the data subject may seek redress from a responsible party in his own jurisdiction if the recipient breaches the data

---

(hereafter referred to as Wugmeister et al ***Codes of Conduct***") at 3.

64 European Union Art 29 Working Party ***Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*** Working Document (WP 74) June 2003.

65 See also discussion on Article 26(2).

66 Continuing liability can also be found where information is transferred to an operator for processing only.

subject's privacy.[67]

United States safe harbor agreement

6.57 Although the EU Commission never issued a formal opinion on the adequacy of privacy protection in the United States, there were serious doubts whether the United States' sectoral and self-regulatory approach to privacy protection would pass the adequacy standard set out in the Directive.

6.58 The European Union commissioned two prominent United States law professors, who wrote a detailed report on the state of United States privacy protections and pointed out the many gaps in United States protection.[68]

6.59 The United States strongly lobbied the European Union and its member countries to find the United States system adequate. In 1998, the United States began negotiating a "Safe Harbor" agreement with the European Union in order to ensure the continued transborder flows of personal information. The idea of the "Safe Harbor" was that United States companies would voluntarily adhere to a set of privacy principles worked out by the United States Department of Commerce and the Internal Market Directorate of the European Commission. These companies would then have a presumption of adequacy and they could continue to receive personal information from the European Union. Negotiations on the drafting of the principles lasted nearly two years and were the subject of bitter criticism by privacy and consumer advocates.[69]

6.60 The United States Department of Commerce and the European Commission in June 2000 announced that they had reached an agreement on the Safe Harbor negotiations that would allow United States companies to continue to receive information from Europe. On July

---

67 However, in evaluating this system the ALRC has recommended that a responsible party should not remain liable under all circumstances. Where the data subject has consented to the processing, where the recipient is subject to adequate privacy legislation or where the processing is necessary for law enforcement purposes, the responsible party should, for eg, not be liable.

68 See EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 17 and reference to Schwartz PM and Reidenberg JR ***Data Privacy Law*** Michie 1996.

69 EPIC and Privacy International ***Privacy and Human Rights Report 2002*** at 17 and reference to Public Comments Received by the United States Department of Commerce in Response to the Safe Harbor Documents April 5, 2000, available at http://www.ita.doc.gov/td/ecom/Comments400/publiccomments0400.html.

26, 2000, the Commission approved the agreement.[70] Over 200 companies have joined the Safe Harbor.[71]

6.61 The principles of the agreement require the following:

- All signatory organisations to provide individuals with "clear and conspicuous" notice of the kind of information they collect, the purposes for which it may be used, and any third parties to whom it may be disclosed.
- This notice must be given at the time of the collection of any personal information or "as soon thereafter as is practicable".
- Individuals must be given the ability to opt out of the collection of information where the information is either going to be disclosed to a third party or used for an incompatible purpose.
- In the case of sensitive information, individuals must expressly consent to (opt in) the collection.
- Organisations wishing to transfer information to a third party may do so if the third party subscribes to Safe Harbor or if that third party signs an agreement to protect the information.
- Organisations must take reasonable precautions to protect the security of information against loss, misuse and unauthorized access, disclosure, alteration and destruction.
- Organisations must provide individuals with access to any personal information held about them, and with the opportunity to correct, amend, or delete that information where it is inaccurate.

6.62 Privacy advocates and consumer groups both in the United States and Europe are critical of the European Commission's decision to approve the agreement, which they say will fail to provide European citizens with adequate protection for their personal information. The agreement rests on a self-regulatory system whereby companies merely promise not to violate their declared privacy practices. There is little enforcement or systematic review of compliance. The Safe Harbor status is granted at the time of self-certification. There is no individual right to appeal or right to compensation for privacy infringements. There is an open-ended grace period

---

70 Commission of the European Communities ***Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions*** issued by the United States Department of Commerce July 26, 2000 available at http://www.ita.doc.gov/td/ecom/Decisions_SECGEN-EN.htm.

71 Safe Harbor List http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+lis.

for United States signatory companies to implement the principles.

6.63 In February 2002 the European Commission issued a report on the practical operation of the European Union-United States Safe Harbor Agreement.[72] This was the first report to evaluate the success of the agreement. It concluded that all the essential elements of the agreement are in place and that a structure exists for individuals to lodge complaints if they feel their rights have been infringed. It did find, however, that there is not sufficient transparency among the organisations that have signed up to Safe Harbor and that not all dispute resolution providers relied on to enforce Safe Harbor actually comply with the privacy principles in the agreement itself.

South Africa

6.64 With the exception of the USA, the requirements set out in the EU Directive have resulted in growing pressure outside Europe for the passage of strong information protection laws. Those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive information.

6.65 It is also important to consider that the transfer of information to South Africa from Europe is governed from the European side by the Directive or country legislation that is implemented in terms of the Directive. This issue is obviously of concern to business in South Africa. See discussion of the written comments received from interested stakeholders, below.

b) Evaluation

6.66 Respondents to the Discussion Papers[73] were, in general, in favour of the principle that

---

72 European Commission Staff Working Paper, February 2002, available at http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf>.

73 The proposed clause in the Discussion Paper Bill reads as follows:

Transborder information flows

94. 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

care should be taken to ensure that the South African model will be regarded as adequate in terms of section 25. There was, however, a difference of opinion regarding the question whether adequacy necessarily implied a strong, regulatory information protection system.

6.67 Respondents who were in favour of ensuring adequate protection of information through a comprehensive general statute argued as follows:

* It is imperative that the South African Protection of Personal Information Bill ensures that the transfer of personal data between the European Union (esp. Germany and U.K.) and South Africa is approved by the EU without a hitch.[74]

* South Africa's international trade aspirations would be adversely affected by the adoption of a privacy model that is considered inadequate by international and EU standards.[75] This impact would not only be felt on a bilateral basis, but on the multilateral level. It would result in lost opportunities for database warehousing, and possible cross border trade in financial and telecommunications services. Moreover, as the SADC region moves towards a trade bloc in 2008, South Africa's policies should be a guiding best practice for the region and capable of adaptation by our regional trading partners. [76]

* It is noted that the Commission has so far recognized Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing "adequate

---

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 perfomance 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.

74 South African Insurance Association (SAIA); Land and Agricultural Development Bank; The Banking Council; Gerhard Loedolff; Nedbank; Eskom Legal Department;The Internet Service Providers Association; Society of Advocates of Kwa-Zulu Natal; Law Society; Nedbank; SA Medical Research Council.

75 Land and Agricultural Development Bank; The Banking Council; Gerhard Loedolff; Nedbank; Eskom Legal Department.

76 The Internet Service Providers Association; Society of Advocates of Kwa-Zulu Natal.

protection".[77]

* Currently, as South Africa does not have any information protection legislation in place, it has been impossible to meet the "adequate level of protection" standard required of countries within the European Union (in accordance with Article 25 of the applicable EU Directive). Nedbank 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.[78] Therefore, it is imperative that appropriate legislation is enacted urgently so that the business mentioned above and other similar South African businesses that process information emanating from offshore parent or affiliate companies or third party customers are not prevented from doing so. The bank is of the view that South Africa, as a country, could attract a substantial amount of information processing business from abroad should this legislation be in place. All the other factors which would make such a business option viable are already in place in favour of South African information processing businesses (such as the fact that we are an English speaking country, we have similar time zones to Europe, labour costs are reasonable etc.).[79]The bank further faces the practical difficulty that it is currently precluded from transferring personal information relating to its customers from its branches in London, Hong Kong, New York and other jurisdictions to its head office in South Africa, for the reason that South Africa has not yet adopted adequate information protection legislation. This has an impact on various aspects of the bank's business, including forensic investigations, monitoring activities in the context of money laundering legislation and other aspects. The bank reiterates that the new information protection legislation must be in line with and satisfy the "adequate protection" requirement of the EU Directive. If it fails to satisfy this requirement, the bank is of the view

---

77 Nedbank.

78 Nedbank.

79 Nedbank.

that such legislation would be inadequate in that it will not assist local banks at all, either in their international business processing operations nor in their local banking operations vis a vis their offshore branches and banking operations.[80]

* The nascent call centre industry in this country could be effectively cut off from a very large market if we do not adhere to or generally understand the import of the EU data privacy rules. We are not important enough to be granted the fig leaf of a " safe harbour" provision and should not, in any case, need to have any such provision made. We must follow best practice and the EU Directive's basic requirements have, we think, been met by the provisions of the proposed section 94.[81]

* An additional aspect of cross-border data flows which is of concern is the flow of information, especially information gathered in the course of research projects on groups of subjects, out of the country, without the possibility of access to that data within the country. It would be helpful if the proposed legislation, or associated guidelines for practice, could address this issue, in order to ensure that data flows out of the country do not jeopardise health care practice and/or research in South Africa.[82]

6.68 Commentators who were opposed to general privacy legislation[83] posed the following arguments:

* Article 25 (2) offers a measure of flexibility by its reference to "…the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measure which are complied with in these countries."[84] There is therefore a case for satisfying the adequacy provision through self-regulation and the courts. [85]

---

80 Nedbank.

81 Law Society of South Africa.

82 South African Medical Research Council.

83 Sanlam; SAFPS; Credit Regulator.

84 Sanlam Life; Legal Service.

85 Sagie Nadasen Legal Adviser : Sanlam Life Law Service.

* The Commission was referred[86] to Du Motier and Goemans[87] who suggest that the assessment of "adequate level of protection" is analyzed on the basis of two core elements, namely: the content of the rules applicable and the means for ensuring their effective application. On the basis of this approach, they contend that countries which have, for example, ratified the Council of Europe's Code 108/81 will benefit from a presumption to be allowed under Article 25(1), provided that additional enforcement mechanisms are in place and that the country in question is the final destination of transfer. Commenting on the Directive's reference to "…professional rules and security measures which are complied with in that country…" they observe that the Directive requires that regard be had to non-legal rules that may be in force in the third country in question, provided that these rules are complied with. In assessing these non-legal rules the applicable criteria are:

(a) an objective analysis of the content of the non-legal rule by reference to core information protection principles and the transparency of applicable codes, and

(b) an evaluation of the effectiveness of the self-regulatory instrument. In the view of the Working Party, the following three functional criteria for judging the effectiveness of the protection must be met:

(i) a good level of compliance which depends often on the awareness of the code's existence – a system of dissuasive and punitive sanctions is one way of achieving this while mandatory audits are another;

(ii) the existence of an impartial, independent support and help to data subjects who are faced with a problem involving the processing of their personal information. Accordingly, an easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate breaches of the code must therefore be in place; and,

(iii) appropriate redress in cases of non-compliance must be provided to obtain a remedy and compensation. [88] Possibilities exist for ad hoc measures where there are inadequate levels of protection. Thus, a contract between the information provider in the EU and the recipient in the third country can be

---

86 Ibid.

87 Du Motier and Goemans ***Data Privacy and Standardization*** 2000 as referred to in the submission of Sagie Nadasen.

88 Ibid.

concluded whereby additional safeguards for the data subject are provided due to the absence of an enforceable set of information protection rules. [89]

* Reference was also made to Carey[90] who notes that one must have regard to the following in respect of the "adequate:" requirement: (a) the nature of the personal information ; (b) the country or territory of origin of the information contained in the data; (c) the country or territory of final destination of that information; (d) the purposes for which and period during which the information are intended to be processed; (e) the law in force in the country or territory in question; (f) the international obligations of that country or territory; (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and (h) any security measures taken in respect of the information in that country or territory. Carey asserts that this list is not exhaustive and also refers to the possibility of a contract between the transferor and transferee – he contends that it is arguable that if the provisions of the contract are enforceable in the legal system of the transferee's legal system, then that country is in fact providing protection.[91] It was argued that both the contractual provisions concluded between South African and foreign companies (which provisions will ensure that core principles and procedures are adequately addressed) and the existing Constitutional protection of fundamental freedoms and rights are more than sufficient to meet information protection concerns of the regulatory authorities in the EU. South African companies must of course ensure that any audit will confirm they have requisite systems and processes in place to meet the EU requirement of "adequate level of protection"[92].

* The majority of African States, if not all, have no information privacy legislation in place and subjectively it is foreseen that with the problems of the continent being what they are, the introduction of such legislation will not be seen for some considerable time. South Africa is presently increasing its presence on the continent and many South Africa organisations have offices throughout Africa. In effect this will mean that South Africa would isolate itself from the rest of the continent in its attempt to blindly follow directives designed for economies far

---

89 Ibid.

90 Carey ***Data Protection Act*** 1998 as referred to in the submission by Sagie Nadasen.

91 Ibid.

92 Ibid.

removed from Africa and South Africa. However, having made this submission it is obviously necessary that the country must provide some form of "adequacy" in order to satisfy Article 25 and our major trading partners. It would therefore appear necessary to provide within the proposed legislation certain exemptions and to make submissions to the European Union in this regard.[93] Another commentator suggested a window period in order to get the necessary contractual commitments, consents or systems in place to ensure such compliance.[94]

* Section 94 of the Discussion Paper Bill should not be enacted in South Africa since cross border flow of both legal and illegal immigrants to and from South Africa to and from other parts of Africa needs to be carefully monitored. The majority of countries in Africa do not have, nor are likely to have in the near future, legislation as outlined in section 94(a) of the draft legislation. From a crime prevention perspective section 94 could create many difficulties to both public and private bodies.[95]

6.69 In May 2008 the Commission was contacted by the SARS Legal and Policy Division. They indicated that SARS has been allocated the responsibility of facilitating the large numbers of international travelers who will be making use of international airlines to attend the 2010 FIFA Soccer World Cup. In order to enforce proper customs control measures SARS needs to receive electronic Advance Passenger Information (API)[96] from the applicable international airlines. The airlines are, however, bound by their own national data protection and privacy legislation which basically holds that the transfer of such personal information is only permitted in certain circumstances and only to such parties that offer the same or higher level of privacy protection.

---

93 SAFPS; Credit Bureau Association.

94 Nedbank.

95 South African Fraud Prevention Service (SAFPS).

96 Advance Passenger Information (API) is one of the categories of data in PNR's. See the discussion on PNR's above. API data is collected, stored and forwarded to governments (typically to the immigration authorities of the destination countries of international flights, to expedite customs and immigration processing by allowing destination countries to start reviewing the passenger manifest while the flight is still in the air. The collection of API data (unlike PNR data) serves no business purpose for airlines. It is solely passenger surveillance and immigration law enforcement carried out by the airlines on behalf of governments. Airlines have therefore resisted the imposition of this unfunded mandate to carry out passenger surveillance and monitoring on government's behalf. In 2004 the EU published Council Directive 2004/82/EC on the Obligations of Carriers to Communicate Passenger Data dated 29 April 2004. It provides for member states to introduce provisions laying down obligations on air carriers transporting passengers into the territory of the member states to transmit the necessary information to destination countries. However, the members states must take the necessary measures to comply with the Directive in this regard.

They inquired as to whether it would be possible to expedite the privacy legislation. Alternatively, they would consider implementing emergency measures which include inserting the provisions of the Bill in the Customs and Excise Act,1964.

6.70 Since POPIA is a comprehensive piece of legislation that has to be considered in depth, it was not possible to expedite it. As an interim arrangement, SARS, therefore, submitted a draft Revenue Laws Second Amendment Bill, 2008 to Parliament in September 2008. It proposes that Sections 7A and 101B (clauses 23 and 37) be included in the Customs and Excise Act. These clauses are more or less a summary of the most important sections of POPIA. The Department of Home Affairs is experiencing the same problem. They have tried to solve the problem by choosing a contractual solution, but have now realised that legislation will be the best option and are considering similar amendments to those of SARS for the Immigration Act. However, SARS dealt with API only, whereas Home Affairs will include APP and PNR.[97]

6.71 The amendments referred to above are regarded as interim measures. The adequacy of these amendments are in doubt and the enactment of POPIA before 2010 may still be the best way to ensure a problem-free World Cup.

6.72 The following technical issues regarding clause 94 of the Discussion Paper Bill were raised:

* In clause 94(c) and (e)(i) and (iii) of the Discussion Paper Bill should refer to "data subject" rather than "individual";[98]
* Clause 94 of the Discussion Paper Bill should gain more prominence and become a Chapter on its own in the Bill. The EU Directive 95/46/EC in its GENERAL PROVISIONS devoted a specific Chapter, viz. Chapter IV to the transfer of personal data to third countries. In the Discussion Paper Bill transborder information flow is listed as one item under Chapter 10, Miscellaneous which gives the impression that South Africa is not giving the same amount of importance or attention to this aspect of data transfer as is the EU.[99]
* Chapter 3 sets out the principles that would enable South Africa to meet the

---

97 See the discussion on PNR above.

98 Department of Communication.

99 South African Insurance Industry (SAIA).

"adequate level of protection" requirements of the EU. However, Chapter 3 does not address the issue of transborder information flow. Chapter 3 does not, therefore, prohibit the transfer of information to third countries which do not have adequate levels of protection. This means that a responsible party in South Africa will be able to forward information received from another party in the EU to a country that has similar protection principles to our Draft Bill in place, and the receiving country could then forward the information to a country that has no data protection whatsoever. It was, therefore, suggested that Chapter 3 should incorporate the transborder information flow prescripts. Including this qualification is important in order to meet the "adequate level of protection" requirement as set out in the EU Directive.[100]

c) Recommendation

6.73 If a country wants to compete in the international market, it will have to ensure that it provides adequate information protection in terms of international standards. If, indeed, personal data intensive industries such as call centres, financial services and tourism industries are going to be promoted, and a market such as the EU targeted, South Africa's proposed data protection legislation will have to ensure that it complies with the EU's "adequate level of protection" requirements.

6.74 Although the international community (as well as the Directive) is not prescriptive as to the way in which these standards are to be met, it is safe to say that having an appropriate comprehensive statute that meets the requirements of Article 25 of the Directive, with an independent regulatory authority to champion this cause, [101]will be a big step in the right direction. This will mean that adequacy will not have to be assessed in the context of each particular transfer, but rather on a per country basis. It is obvious that this will ease the way for South African companies interested in international exposure as well as for international companies wishing to trade in South Africa.

6.75 However, the fact that the Directive makes provision for other ways in which to acquire adequacy contradicts the argument that South Africa will be adversely affected,

---

100 SAIA; Lucien Pierce.

101 See discussion in Chapter 7 below.

in so far as its trade with African countries are concerned, should it comply with Article 25. Trade with African countries will be more difficult than with Europe since adequacy will have to be established in each particular transfer. This is, however, the status quo at the moment and this position can not be ascribed to the effects of the information protection legislation. The legislation will however, improve the country's position regarding countries that do have proper legislation in place, which include all our major trading partners in Europe, North America and Australasia.

6.76 It is therefore the Commission's opinion that a general comprehensive law making provision for adequate information protection should be instituted. This will be achieved by making provision for the inclusion of the information protection principles as well as for the means to ensure their effective application.[102]

6.77 The Bill will furthermore, in clause 69, stipulate that information will not be transferred to another country if proper safeguards for the protection of the information has not been made in that country. Clause 69 closely mirrors the provisions set out in Articles 25 and 26 of the EU Directive as explained above.[103]

6.78 Clause 94 of the Discussion Paper Bill has now been incorporated in clause 69 of the Bill and forms a separate Chapter (Chapter 9,Transborder Information Transfers) in order to provide a proper indication of its importance in the context of the Bill.

6.79 Subclause 69(a)(ii) has been inserted to ensure that the laws regulating the protection of personal information in the recipients's country will also prevent the onward transfer of information to countries without adequate protection as stipulated in the Directive.

6.80 The legislative enactment, including the amendments necessitated by the submissions received, will read as follows:

---

102 See the proposed Protection of Personal Information Bill included as Annexure C herewith.

103 See discussion above.

CHAPTER 9

TRANSBORDER INFORMATION FLOWS

Transfer of personal information outside the Republic

69. A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless -

(a) the recipient of the information is subject to a law, binding code of conduct or contract which -

(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles; and

(ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

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

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

(e) the transfer is for the benefit of the data subject, and -

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

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

CHAPTER 7: MONITORING AND SUPERVISION

7.1 Introduction

7.1.1 An essential aspect of any privacy protection regime is oversight. The effectiveness of information protection provisions in protecting an individual's personality rights will depend largely on how they are applied and interpreted in practice.[1]

7.1.2 It has been argued[2] that the rules for information protection come from three distinct perspectives, namely political, economic and technological:

a) In Europe, information protection is an inherently political right and focuses on legal mechanisms to guarantee respect for a fundamental human right to privacy.

b) By contrast, in the United States, information privacy is left to the marketplace and the desire to have market-based protection for consumers. Information protection is a question of economic power rather than political right.

c) Across these two policy models of information protection, technological rules and defaults define information practices for network interactions.

7.1.3 The rules found in information protection laws furthermore usually belong to two main categories:[3]

a) rules concerned directly with regulating the processing of personal information (so-called Information Protection Principles)[4]; and

b) rules concerned primarily with monitoring and enforcing the first set of rules.[5]

---

1 Roos 1998 ***THRHR*** at 505 in referring to the data protection provisions as they were then in the Open Democracy Bill.

2 Reidenberg J "Technologies for Privacy Protection" Presentation delivered at the 23rd International Conference of Data Protection Commissioners, Paris Sept 2001(hereafter referred to as "Reidenberg presentation 2001") at 2 and the references made therein.

3 Bygrave ***Data Protection*** at 84.

4 See discussion of Data Protection Principles in Chapter 4.

5 The subject of discussion in this Chapter.

7.1.4 The first category of rules can in turn be sub-divided into two main sub-categories:

a) Rules regulating the manner and purposes of information processing. These rules ensure that the processing of information occurs with the participation of the data subject. Information processing should therefore be authorised, publicised and rectifiable.

b) Rules relating to the quality of personal information.

7.1.5 The second main category of rules can also be broken down into two main sub-categories:

a) Rules that facilitate monitoring and enforcement functions (supervision).

b) Rules directly concerned with monitoring and enforcement functions (enforcement).

7.1.6 Four models, embodying the abovementioned rules for privacy protection, were identified in Issue Paper 24:[6]

a) Comprehensive laws

In many countries around the world, there is a general law that governs the collection, use and dissemination of personal information by both the public and private sectors. The overwhelming majority of countries with information protection laws also have established special authorities (information protection authorities) to oversee specifically the implementation of these laws.[7] A variation of these laws, described as a co-regulatory model, was adopted in Australia. Under this approach there is a comprehensive law, but industry may develop rules for the protection of privacy that are enforced by the industry and overseen by the privacy oversight agency.[8]

---

6 EPIC and Privacy International ***Privacy and Human Rights Report*** 2002 at 3.

7 In most cases the authorities are empowered to issue legally binding orders. In some jurisdictions, however, the authorities either do not have such a competence at all, or they do not have it in relation to certain sectors.There is evidence to suggest that the recommendations of an Ombudsman can sometimes be equally as effective as orders. See Bygrave ***Data Protection*** 70 fn 277 and the references made therein. Notable exceptions are the USA and Japan. Repeated attempts to set up a data protection authority at the federal level in the USA have stranded largely on account of America's deep-seated antipathy to regulation by governmental agencies. See Bygrave ***Data Protection*** at 70.

8 EPIC and Privacy International ***Privacy and Human Rights Report*** 2002 at 4.

b) Sectoral laws

Some countries, such as the United States, have avoided enacting general information protection rules for the private sector in favour of specific sectoral laws governing eg. credit reporting, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. With this approach, new legislation has to be introduced with each new technology - so protections frequently lag behind. The lack of legal protections for individual privacy on the Internet in the USA is a striking example of its limitations. There is also the problem of a lack of an oversight agency dealing specifically with privacy protection. In some countries, sectoral laws are, however, used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.[9]

c) Various forms of self-regulation

Information protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of conduct and engage in self-policing. However, in many countries, and especially in the private sector in the United States, these efforts have been disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries provide only weak protections and lack enforcement. This is currently one of the policies promoted by the governments of the United States and Singapore.[10]

d) Technologies of privacy

With the recent development of commercially available technology-based systems, privacy protection has also moved into the hands of individual users. Users of the Internet and of

---

9 EPIC and Privacy International ***Privacy and Human Rights Report*** 2002 at 4.

10 EPIC and Privacy International ***Privacy and Human Rights Report*** 2002 at 4.

some physical applications can employ a range of programs and systems that provide varying degrees of privacy and security of communications.[11] These include encryption, anonymous remailers, proxy servers and digital cash.[12] While technology has made our personal lives more transparent, privacy and technology are therefore not inherently antagonistic.[13] Technology by itself is neither a privacy enhancer nor a privacy threat. This is to be determined by its uses.[14] Technology will become a privacy enhancer if appropriate awareness, education, management processes/business models are developed.[15] Some argue that new technologies may prove to be one of the most potent forces driving the right to informational self-determination.[16]

---

11 Privacy Enhancing Technologies (PETs) have been defined with reference to the definition of Herbert Burkert in fn 288 in Froomkin AM "The Death of Privacy?" ***Stanford Law Review*** Vol 52:1461 May 2000 (hereafter referred to as "Froomkin 2000 ***Stanford Law Review")*** at 1529 as technical devices organisationally embedded in order to protect personal identity by minimising or eliminating the collection of data that would identify an individual or a legal person. In addition to PETs embedded in organisations there are also a number of closely related technologies that people can use for self-help, especially when confronted by organisations that are not privacy friendly. One such device is the Platform for Privacy Preferences (P3P) which seeks to reduce the transaction cost of determining how much personal data should be surrendered in a given transaction. The P3P project provides a standard way for web sites to communicate about their data practices. Developed by the World Wide Web Consortium (W3C) P3P specification includes a standard vocabulary for describing a website's data practices, a set of base data elements that web sites can refer to in their privacy policies and a protocol requesting and transmitting website privacy policies. P3P enabled web sites make information available on how sites handle personal information about its users. P3P enabled browsers can then "read" this information automatically and compare it to the consumer's own set of privacy preferences; Froomkin 2000 ***Stanford Law Review*** at 1529.

12 EPIC maintains a list of privacy tools at http://www.epic.org/privacy/tools.htm.

13 Valeri L "Is Technology a Privacy-enhancer or Privacy Threat? Some Thoughts" Presentation delivered at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002 (hereafter referred to as "Valeri presentation 2001"). Technology has already alleviated many everyday intrusions: airport x-ray units have made hand searchers of luggage rare. Magnetic markers in books and clothing makes searches unnecessary. Encryption software makes computer files infinitely more secure than paper documents in locked cabinets.

14 Valeri presentation 2001 at 8.

15 Technology solutions:
- Privacy enhancing technologies.
- Anonymous and pseudonymous browsing, email, remailing systems.
- Platform for Privacy Preferences or P3P.
- Privacy policy generators.
- Smart cards/public key infrastructures.
- Biometric solutions readers, software etc.
- Cookie managers.

16 Piller ***Macworld*** at 7; Mark Heyink, in his submission to the Commission stressed that It is, however, increasingly clear that questions of information security, often thought to be the domain of the technologists and technologies that they create, have proved to be far more dependent on people and processes than on the technologies which support the processes. While the role of privacy enhancing technologies may be important in future, it is likely that these privacy enhancing technologies will be driven by issues of compliance with legislation rather than the interests of markets to build technologies with this capacity. Further, it is unlikely in the foreseeable future, that privacy enhancing technologies

7.1.7 It was noted in the Discussion Papers that, depending on their application, these models/instruments could be complementary or contradictory. In most countries several are used simultaneously. In the countries that protect privacy most effectively, all the instruments are used together to ensure privacy protection. [17]

7.1.8 This fact was confirmed in collating the responses to the Discussion Papers. It became clear that the different options to be evaluated in drafting privacy legislation for South Africa did not so much turn on the specific models or instruments used, but rather on the degree of regulation involved in each case. Three supervisory systems were identified through which the privacy principles could be implemented. These systems included all of the abovementioned models/instruments or parts thereof.[18] They were identified as regulatory, self-regulatory and co-regulatory systems.

7.2 Supervisory systems

a) Proposals in Discussion Paper

7.2.1 Each option will be discussed in this section (para 7.2 (a)) with the comments it elicited in each case discussed in para 7.2(b) below.

(i) Regulatory system (eg. UK, New Zealand, the Netherlands, Canada)

---

implemented without also addressing human behaviour and establishing processes within which the technologies would be used, would work.

17 Bennett ***Government Foundation Paper*** 2001at 28; Bennett CJ "The Data Protection Authority: Regulator, Ombudsman, or Campaigner?" Presentation delivered at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, September 9-11,2002 (hereafter referred to as "Bennett presentation 2002") further note that the data protection statute is just one influence on the behaviour of the data protection authority. The data protection authority is furthermore just one policy instrument in the 'privacy toolbox", others are self-regulatory instruments, privacy enhancing technologies and international instruments. See also Bennett CJ and Raab CD ***The Governance of Privacy - Policy Instruments in Global Perspective*** Ashgate Publishing Aldershot Hamshire 2003 (reprinted in 2004) (hereafter referred to as ""Bennett and Raab ***The Governance of Privacy***") at 165.

18 It is interesting to note that there has been a continuing process of convergence and harmonisation of ideas to the extent that one can now speak of a global approach to privacy protection. At the same time the range of possible policy instruments has expanded.

Comprehensive law

7.2.2 A regulatory system makes provision for a comprehensive Act setting out the Principles of Information Protection[19] as well as provisions dealing with the monitoring and enforcement of these principles.

Sectoral laws

7.2.3 As stated above, the regulatory system may also include sectoral laws. These specific laws may precede the national adoption of general information protection legislation or may be passed after general legislation comes into force. Examples of countries with both general and sectoral laws are The Netherlands, Belgium, Germany, Austria, Finland, Norway, Sweden and Denmark. Taken together, these laws cover a wide range of information-processing fields, including the census, public service "one stop shops", public order, telecommunications, video surveillance, sensitive information registers, credit cards, public archives, the media, information matching in the field of taxation, genetic information and the collection of personal information for payroll wage-deduction.[20]

7.2.4 It is important to note, though, that as with comprehensive statutes, their oversight and implementation will remain the key to their effectiveness.[21]

Oversight agencies

7.2.5 As seen above, most countries with an omnibus information protection or privacy Act, have an official or agency that oversees enforcement of the Act.[22] The powers of these officials -

---

19 See Chapter 4 above.

20 Bennett and Raab ***The Governance of Privacy*** at 106.

21 Ibid.

22 Bennett and Raab ***The Governance of Privacy*** at 108 refer to OECD countries with Data Protection Supervisory Authorities: Office of the Federal Privacy Commissioner, Australia; Buro der Datenschutzkommission, Austria; Commissie Voor De Bescherming van de Persoonlijke Levenssfeer, Belgium; Privacy Commissioner of Canada; Office of Personal Data Protection, Czech Republic; Datatilsynet, Denmark; Der Bundesbeauftragte fur den Datenschutz, Germany; Hellenic Data Protection Authority, Greece; Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary; Personuvernd, Iceland; Data Protection Commissioner, Ireland; Garante per la Protezione dei dati Personali, Italy; Commision a la Protection des Donnees Nominatives, Luxembourg; College Bescherming

Commissioner, Ombudsman or Registrar - vary widely by country. A number of countries, including Germany and Canada, also have officials or offices on a state or provincial level.

7.2.6 The most detailed treatment of the competence and functions of information protection authorities is found in the EU Directive. Article 28(1) states that each EU Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Members States pursuant to the Directive. [23]

7.2.7 In contrast to the EU Directive, the OECD Guidelines have little to say about the need for, and competence of, national information protection authorities. Indeed, they do not require such authorities to be established. A similar situation has pertained up until recently with the CoE Convention. However, an additional Protocol to the Convention was adopted on 23 May 2001[24] by the CoE Committee of Ministers replicating in Article 1 the basic thrust of Article 28 of the Directive.[25]

7.2.8 The UN Guidelines specifically address the need to establish national data protection authorities that are "impartial", "independent" and "technically competent".[26]

7.2.9 The Commonwealth guidelines make provision for the establishment of an independent

---

Persoonsgegevens, Netherlands; Privacy Commissioner, New Zealand; Datatilsynet, Norway; Bureau of the Inspector General for the Protection of Personal Data, Poland; Comissao Nacional de Protecao de Dados, Portugal; Commissioner for the Protection of Personal Data, Slovak Republic; Agencia de Proteccion de Datos, Spain; Data Inspection Board, Sweden; Federal Data Protection Commissioner, Switzerland; Information Commissioner, United Kingdom. OECD countries without supervisory authorities are Japan, Korea, Turkey and the United States.

23 Bygrave ***Data Protection*** at 71; Article 28(1) of the EU Directive reads as follows:

Article 28
Supervisory authority

1.Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

24 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) Regarding the Supervisory Authorities and Trans-border Data Flows, ETS No 179, open for signature 8.11.2001.

25 Bygrave ***Data Protection*** at 73.

26 Bygrave ***Data Protection*** at 73 referring to para 8.

Privacy Commission, but on an optional basis. It recognises that small and developing countries may not be able to create such an office and may need to rely on courts or tribunals only to deal with allegations of damage caused by breach of the privacy law.[2728]

Codes of conduct

7.2.10 Some Commissioners have explicit responsibilities to negotiate privacy codes of conduct. Some countries' laws make specific provision for industries, professions, etc to draw up sectoral

---

27 Commonwealth Model Law for Private Bodies at 2. In terms of this Model Law the office of Privacy Commissioner is established by the appointment of a full-time Privacy Commissioner by the President upon the recommendation of the Minister, for five years subject to such terms and conditions as may be specified in the instrument of appointment. The Commissioner shall receive and investigate a complaint from any person in respect of any matter relating to -
(a) the collection, retention or disposal of personal information by a public authority; or
(b) the use or disclosure of personal information held by a public authority; and have the powers to carry out an investigation in this regard.
With regard to private bodies the Privacy Commissioner shall have similar powers and duties. Parliament shall appropriate annually, for the use of the Privacy Commissioner, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Commissioner, of his or her powers, duties and functions under this Act.

28 The functions of the Privacy Commissioner would be -
(a) to monitor compliance by public authorities of the provisions of this Act;
(b) to provide advice to public authorities on their obligations under the provisions, and generally on the operation, of this Act;
(c) to receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;
(d) to inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby;
(e) for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner;
(f) to make public statements in relation to any matter affecting the privacy of the individual or of any class of individuals;
(g) to receive and invite representations from members of the public on any matter affecting the privacy of the individual;
(h) to consult and co-operate with other persons and bodies concerned with the privacy of the individual;
(i) to make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interests of the privacy of the individual;
(j) to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring;
(k) to examine any proposed legislation (including subordinate legislation or proposed policy of the Government that the Commissioner considers may affect the privacy of individuals, and to report to the Minister the results of that examination;
(l) to report (with or without request) to the Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of the individual;
(m) to report to the Minister from time to time on the desirability of the acceptance, by [name of country] of any international instrument relating to the privacy of the individual;
(n) to gather such information as in the Commissioner's opinion will assist the Commissioner in discharging the duties and performing the functions of the Commissioner under this Act;
(o) to do anything incidental or conducive to the performance of any of the preceding functions; and
(p) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

codes of conduct/practice on information protection in co-operation with information protection authorities.[29] An increasing number of schemes for the development of such codes is likely, given that the EU Directive requires Member States and the Commission to "encourage" the drafting of sectoral codes of conduct at national and community level, in pursuance of the measures contemplated by the Directive.[30]

7.2.11 Codes of conduct are primarily instruments of self-regulation and will also be discussed below in paras (ii) and (iii), dealing with the co- and self-regulatory systems. They do, however, also offer some clear advantages in a legislated information protection regime. The procedure of negotiating codes may enhance the understanding of the privacy problem within different sectors. Codes are flexible instruments and once negotiated can be adapted to changing economic and technological developments.[31]

7.2.12 There are three different models that have evolved in those countries that use privacy codes. The first, and in many ways most stringent, is represented by the system under the New Zealand Privacy Act.[32] The crucial aspect of the New Zealand approach is that codes of practice negotiated under the Privacy Act have the force of law. A breach of a ratified code of practice is as serious as a breach of the information privacy principles expressed in the law, which would then trigger the complaints and enforcement procedures in the legislation. The second, slightly more flexible regime, exists in the Netherlands. Although the Dutch system is similar in most respects to that in New Zealand, the codes are not formally binding on the courts. If an organisation can prove that it has met the requirements of its code, it will have a strong case. Conversely, a complainant's demonstration that the provisions of the code have been breached constitutes prima facie evidence of liability under the law. Codes therefore, have indirect, rather than direct legal effect. In other countries, such as the UK and Canada, the law simply empowers the Commissioner concerned to encourage the development of codes as a further instrument of compliance with the

---

29 See eg Parts VI-VII of the New Zealand Act; section 51(3)-(4) of the United Kingdom Act; Part III AA of the Australian Act; and Article 25 of the Netherlands' Act.

30 Bygrave ***Data Protection*** at 74 referring to Article 27; See discussion on codes of conduct below in para 7.4 below.

31 Bennett and Raab ***The Governance of Privacy*** at 113.

32 See Part VI of the New Zealand Privacy Act.

law. Indeed, this is all that is expected by the EU Directive. [33]

7.2.13 Where a formal ratification process is laid out, as in New Zealand and the Netherlands, this can bureacratise a process that, in theory, is supposed to allow the flexibility of self-regulation. Submission of the codes in some sectors are, furthermore, hindered by competition within the sector, and by unclear boundaries and overlaps that weaken the claim that the association submitting the code is sufficiently "representative".[34]

Other agencies

7.2.14 It should also be noted that information protection authorities are not alone in monitoring, encouraging and enforcing the implementation of information protection laws. A great number of other bodies are involved to varying degrees in one or more of the same tasks, even if their participation is not always formally provided for in information protection instruments.[35]

7.2.15 On the international plane, notable examples of relevant bodies are the expert committees on information protection and information policy formed under the umbrella of the CoE and OECD. A variety of other inter- and non-governmental organisations are also emerging to play a role in the setting of information protection standards. These include the World Trade Organisation (WTO), World Intellectual Property Organisation (WIPO) and the World Wide Web Consortium (W3C). Many of these bodies will approach information protection from a market-oriented rather than a human rights perspective.[36] At a national level, obvious examples of relevant bodies are those charged with hearing appeals from the decisions of information protection authorities. Other examples are parliamentary committees, ombudsmen and national auditing offices.

Independence

7.2.16 The EU Directive requires that oversight authorities must act with complete independence

---

33 Bennett and Raab ***The Governance of Privacy*** at 113.

34 Ibid.

35 Bygrave ***Data Protection*** at 73.

36 Bygrave ***Data Protection*** at 74.

in exercising the functions entrusted to them.[37] The reference to "complete independence" means that great care must be taken in ensuring that the authorities' inevitable *administrative* dependence on other bodies (eg through budget and personnel allocations) does not undermine the functional independence they are otherwise supposed to have. It also means that administrative and legal frameworks which leave open even a small possibility of an information protection authority being instructed by another administrative body on how to exercise its functions, most probably do not satisfy the criterion of Article 28(1).[38] However, they are clearly not judicial bodies and usually closely linked to the Ministry of Justice. Perhaps the best way to describe them is as "independent administrative agencies".[39]

7.2.17 This criterion of independence boils down to the capacity for an information protection authority to arrive at its own decision in a concrete case without being given case-specific instructions by another body as to what line it should take. Yet, insofar as such a decision is legally binding, it will usually be subject to political and legal review.[40] Moreover, decision making by an authority will be steered at a more general level by laws and regulations laid down by other bodies.[41]

7.2.18 Many authorities are appointed in special procedures, often involving Parliament - although some are appointed by the Government (in the UK by the Queen acting on the advice of Government) or, indeed, the Minister of Justice (the Netherlands).[42]

7.2.19 The independence of privacy and information protection regulators is therefore a complex variable that is affected as much by processes of appointment and financing, as by the formal lines of authority stipulated in law. In the UK the Information Commissioner reports to Parliament and

---

37 Article 28(1).

38 Bygrave ***Data Protection*** at 71.

39 Korff ***Comparative Study*** at 200.

40 Korff ***Comparative Study*** at 201 argues that the very existence in Member States under the Rule of Law, of the above-mentioned kinds of almost discretionary powers in the hands of non-judicial bodies must raise questions. At the very least, the exercise of such powers should be subject to judicial overview and indeed, in appropriate cases, to prior judicial authorisation (such as the issuing of a search warrant).

41 Bygrave ***Data Protection*** at 70.

42 Korff ***Comparative Study*** at 203.

not to a government minister, and is generally regarded as well insulated from direct political interference. [43]

7.2.20 The Directive contains several provisions which will stimulate an internationalisation, at least within the EU, of supervisory and monitoring regimes in the field of information protection.[44] Further, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereafter referred to as "Data Protection Working Party") has been established pursuant to Article 29. This body is mainly composed of representatives from each Member State's data protection authority. It acts independently from the Commission and other EU organs, and has advisory competence only. Its purpose is to provide advice on issues relating to the uniform application of national measures adopted pursuant to the Directive; data protection afforded by non-Member States; possible changes to the Directive and other instruments affecting data protection; and codes of conduct drawn up at Community level.[45]

7.2.21 At the 23rd International Conference of Data Protection Commissioners[46] an accreditation procedure (for recognising the credentials of data protection authorities for the purposes of the International Conference) was established.[47] The following rules were set: the information protection authority must be a public authority implemented by legal purview; the authority must have the benefit of guarantees of autonomy and independence; the authority must dispose of effective competence, and it should not only have a consultative role, but must also dispose of a power of surveillance which includes legal or administrative consequences. [48]

Monitoring

---

43 Bennett and Raab ***The Governance of Privacy*** at 175 and 176.

44 See Article 28(6) in this regard.

45 Bygrave ***Data Protection*** at 73.

46 Held in Paris, France 24-26 September 2001.

47 Accredited members would have a legitimately full share in the resolutions which may be adopted.

48 The document was prepared by the delegations from New Zealand, the United Kingdom and France who also formed the first accreditation committee in terms of the rules.

7.2.22 Most information protection laws lay down special rules to enhance the ability of information protection authorities to monitor the practices of responsible parties. While information protection laws expound similar core principles, there are numerous differences between them in terms of the monitoring and supervisory regimes they establish:[49]

a) One category requires responsible parties simply to **notify** information protection authorities of certain planned processing of personal information.[50] Upon notification, processing is usually allowed to begin. [51] Most information protection laws, including the EU Directive (the other three main international information protection instruments, however, refrain from specifically laying down requirements for notification or for other control schemes) operate with this sort of requirement, though the ambit of their respective notification schemes has varied.[52]

b) Occasionally, the notification requirement is formalised as a system for **registration**. [53] Under this sort of system, responsible parties must, as a general rule, apply to be registered with the information protection authority, registration being a necessary pre-condition for their processing of personal information. Once application for registration is lodged, the controller is legally able to begin processing.[54] The UK used to be an example of the registration model.

c) Another category of control/oversight requires that responsible parties must apply for and receive specific authorisation (in the form of a **licence)** from the relevant

---

49 Bygrave ***Data Protection*** at 75.

50 See eg section 36 of Sweden's Personal Data Act. The notification requirement does not apply where the data controller has appointed an internal data protection officer.

51 Article 19(1) of the EU Directive stipulates the types of information to be notified to include "at least" the identity of the data controller and his/her representative; the purposes of the data processing; the categories of data subject and data held on the latter; the categories of recipients of the data; and proposed transfers to third countries and a general description of adopted security measures for the processing.

52 Bygrave ***Data Protection*** at 75.

53 Repealed ss 4-9 of the UK Data Protection Act of 1984.

54 Bygrave ***Data Protection*** at 75.

information protection authority prior to establishing a personal register or engaging in a particular information-processing activity. Only a minority of information protection authorities operate, or have operated with comprehensive authorisation/licencing regimes, France being an example in so far as its public sector is concerned. It has been more common for countries to reserve a licencing requirement for certain designated sectors of business activity such as credit reporting or for overseas transfers of personal information or for the matching of information.[55]

Other functions[56]

7.2.23 Apart from monitoring the practices of responsible parties, agencies may also have other duties. Some examples are as follows:[57]

a) Governments may consult the body when the government draws up **legislation** relating to the processing of personal information; they would accordingly also take part in hearings in Parliamentary commissions.[58]

b) The bodies have the power to conduct **investigations**[59] and have a right to access

---

55 Bygrave ***Data Protection*** at 76.

56 See Article 28(2) and (5) of the EU Directive.

57 Lopez JMF "The Data Protection Authority: The Spanish Model" Presentation delivered at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, September 9-11 2002 (hereafter referred to as "Lopez presentation 2002").

58 Korff ***Comparative Study*** at 205 explains as follows: Governments and legislators often follow the authorities' advice; at the very least, their opinions ensure that the issues concerned are properly aired and debated. In several national systems, the providing of "opinions" furthermore formally or effectively becomes a part of enforcement. Thus, In France, the issuing of "favourable opinions" on the required regulations for proposed public-sector processing operations has in practice become a pre-condition. In the Netherlands a positive opinion, by the data protection authority is required before a sectoral code of conduct can play its intended role in the data protection compliance system.

59 Such investigations can arise, in particular, out of doubts about a proposed processing operation as described in a ("full") registration form, or out of specific complaints from individual data subjects . Korff ***Comparative Study*** at 206. Action taken by data protection authorities on the basis of complaints from individual data subjects follows the same pattern: the authority gets in touch with the data user (responsible party) concerned, "advises" and act as a conciliator, and tries to reach an amicable solution to the dispute. In many cases, the issues are straight-forward and easily resolved on the basis of clear legal principles. For instance, a data user refusing to grant a data subject access to his or her data may need only to be "reminded" by the authority of his duty to allow such access. Other cases however are more complex, and in those the authority tries to reach a compromise acceptable to both the data user and the data subject. Again, this approach is almost always "successful" in the sense that the authority does not need to use formal enforcement measures: the authorities in the Member States only resort to "hard" enforcement measures in a minute proportion of complaints. Korff ***Comparative Study*** at 207-208.

information relevant to their investigations; impose **remedies** such as ordering the destruction of information or ban processing, and start legal proceedings, hear complaints and issue reports.[60]

c) The agency is generally responsible for public **education** and raising awareness actions, speeches, organisation and participation in symposiums, courses and seminars, publication of an annual report and the drawing up of information documents for citizens such as brochures, manuals and recommendations.

d) **Liaison** both on international as well as national level which entails cooperation with various entities such as ombudsmen, the public prosecutor, universities, autonomic information protection authorities, chambers of commerce and professional organisations.

e) In a number of countries, this official also serves as the enforcer of the jurisdiction's **Freedom of Information Act**. These include Mexico, Hungary, Estonia, Thailand, Ireland, and the United Kingdom.[61] On the sub-national level, many of the German Lund Commissioners have recently been given the power of information commissioner, and most of the Canadian provincial agencies handle both information protection and freedom of information.

7.2.24 The contemporary role of the Information Protection Authority is therefore that of ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer and international ambassador**.**[62]

7.2.25 A number of countries that do not have a comprehensive Act still have a commissioner. The major duty of these officials is to focus **public attention** on problem areas, even when they do not have any authority to fix the problem. They can do this by promoting codes of conduct and encouraging industry associations to adopt them. They can also use their annual reports to point

---

60 Korff ***Comparative Study*** indicates that criminal prosecutions are an extreme rarity, reserved for the most obstinate or crass law breakers such as companies which continue to maintain unregistered databases in spite of repeated warnings, or which export data in spite of such warnings or formal notices, or people who knowingly flout the law by selling confidential personal information (eg policemen who obtain access to criminal records or other confidential information on behalf of unauthorised third parties).

61 The UK Commissioner has opted for a systemic solution to the problem in that the mechanism for enforcing the provision of its access regime and its data protection regime is one and the same – a Commissioner who regulates both.

62 Bennett Conference Paper 2002.

out problems.

7.2.26 Examples of the work done by Privacy Commissioners in other countries are as follows -

a) In Canada both the Privacy Act and PIPEDA are overseen by the independent Privacy Commissioner of Canada:

– Under the Privacy Act[63] the Commissioner has:

- The power to investigate, mediate, and make recommendations, but cannot issue orders or impose penalties.
- During the course of an investigation the Commissioner may subpoena witnesses and compel testimony, and enter premises in order to obtain documents and conduct interviews.
- The Commissioner is also charged with conducting periodic audits of federal institutions to determine compliance with the Privacy Act, and to recommend changes where necessary.
- The Commissioner can initiate a Federal Court review in limited circumstances relating to denial of access to records.

– The Commissioner's powers under PIPEDA [64]are very similar to those under the Privacy Act.

- The Commissioner has powers of recommendation only with regard to complaints submitted under the Act. Once a complaint is received, the Commissioner assigns an investigator to look into the matter. The investigator then submits his findings to the Commissioner who then

---

63 The office received a total of 1,713 complaints under the Privacy Act between April 1, 2000, and March 31, 2001, an almost ten percent increase from the previous year. Office of the Privacy Commissioner of Canada ***Annual Report to Parliament 2000-2001, Part One–Report on the Privacy Act*** December 2001. The office closed 1,542 investigations, again an increase of 10 percent from the previous year. 339 of these cases related to issues of collection, use, disclosure, or disposal, 630 related to access, and 573 to time limits. Since November 2001, the office has received more than 8,047 requests for information concerning the Privacy Act. (E-mail from Dona Vallieres, Senior Director General, Communications and Policy, Privacy Commission of Canada to Nicole Anastasopoulos, Research Assistant, Electronic Privacy Information Center, July 10, 2002 (on file with the Electronic Privacy Information Center).

64 The Office of the Privacy Commissioner began receiving complaints under PIPEDA on January 1, 2001. By January 17, 2001, it was reported that the office had already received four formal requests for investigations and numerous telephone inquiries.Tyler Hamilton, "Confidentiality Fears Swamping Privacy Watchdog," ***The Toronto Star***, January 17, 2001. As of November 2001, the Office had received more than 8,859 E-mail from Dona Vallieres, Privacy Commission of Canada, to EPIC supra, 496 requests for information concerning PIPEDA, 95 formal complaints (half of which involved banks) and initiated 198 investigations. Office of the Privacy Commissioner of Canada ***Annual Report to Parliament 2000-2001, Part Two– Report on the Personal Information Protection and Electronic Documents Act***, December 2001, available at<http://www.privcom.gc.ca/information/ar/. The Commissioner's office completed and issued findings and recommendations on 27 complaints.

considers the case and issues a report with recommendations.

- He can also request the organisation in question to submit, within a specified period of time, notice of any action taken or proposed to be taken to implement these recommendations.[65]
- However, if the Commissioner is satisfied that there are reasonable grounds to investigate a matter under the Act, he may initiate his own complaint.[66]
- The Commissioner is also authorised to conduct broad research into privacy issues and promote awareness and understanding of privacy issues among Canadians.

b) In the UK[67] the Information Protection Commissioner is appointed in terms of section 6(2) of the Data Protection Act of 1998 by the Queen by Letters Patent. Paragraph 1(2) confirms that the Commissioner, officers and staff of the Commissioner are not to be regarded as servants or agents of the Crown. Tenure of office is for a period of five years but the Commissioner may be reappointed. The powers and functions of the Commissioner can be classified as follows;

- duties to promote good practice and compliance;
- dissemination of information;
- involvement in respect of drawing up codes of practice;
- dissemination of Community findings in relation to transfers to third countries;
- assessing processing with the consent of responsible parties;
- laying reports and codes of practice before each House of Parliament;
- assisting individuals where processing is for special purposes; and
- participating in international co-operation.

7.2.27 The Data Protection Act 1998 furthermore follows a twin track approach (as it did with the 1984 Act) by giving the Commissioner powers of enforcement whilst also providing for a number of criminal offences under the Act. The Commissioner therefore has powers and functions

---

65 See generally Office of the Privacy Commissioner of Canada ***Your Privacy Responsibilities: A Guide for Business and Organizations*** December 2000.

66 Perrin S, Black H, Flaherty D and Rankin TM ***The Personal Information Protection and Electronic Documents Act: An Annotated Guide*** Toronto, 2001.

67 Bainbridge ***Data Protection*** at 143 and 217.

pertaining to notification, enforcement, prosecution of offenders and powers of entry and inspection all set out in the relevant sections of the Act.

7.2.28 The Act also makes provision for the Data Protection Tribunal. The purpose of the Tribunal is primarily to hear appeals from data controllers/responsible parties in respect of notices served by the Commissioner or determinations made by the Commissioner as to whether processing is for special purposes. A data subject, however, does not have a right to appeal to the Tribunal against a decision of the Commissioner.

7.2.29 In reality the information protection authorities in the EU Member States see themselves much more as advisers, facilitators and conciliators than as policemen: referees rather than Rambos. As the UK information protection authority once put it:[68]

> Powers of enforcement are vital but our approach is to seek to anticipate complaints by providing adequate advice, or where they arise to proceed by agreement and negotiation only taking formal action where action to achieve compliance cannot be agreed.[69]

Challenges

7.2.30 Challenges experienced by *oversight agencies* in giving effect to information legislation are as follows:

a) A major problem with many agencies around the world is a lack of resources to adequately conduct oversight and enforcement. Some are burdened with licensing systems, which use much of their resources. Others have large backlogs of complaints or are unable to conduct a significant number of investigations. Many that started out with adequate funding find their budgets cut a few years later.[70]

---

68 Korff ***Comparative Study*** at 206.

69 Annual Report 1996 at 32.

70 In 1995 in South Africa, the Task Group on Open Democracy compiled its *Policy Proposals* on the basis of preliminary consultations undertaken by the Task Group late in 1994; Task Group on Open Democracy ***Open Democracy Act for South Africa: Policy Proposals 1995*** at 18. They identified principles, rather than rules to serve as the basis for further consultations early in 1995. In so far as costs and fees of implementation of legislation are concerned, the Task Group,

b) Independence is also a problem. In many countries, the agency is under the control of the political arm of the government or part of the Ministry of Justice and lacks the power or will to advance privacy or criticise privacy invasive proposals. Finally, in some countries that do not have a separate office, the role of investigating and enforcing the laws is done by a human rights ombudsman or by a parliamentary official.

c) The authorities also pride themselves on the effectiveness of their "conciliatory" approach, pointing out that they have to resort to "hard" enforcement measures in only a very limited number of cases. This conciliatory approach by the information protection authorities may, however, reinforce the idea on the part of many responsible parties that information protection is "soft law".[71]

7.2.31 On the other hand, the enactment of comprehensive legislation may have the following negative implications for *responsible parties* -

a) The information base owners may face additional costs in having to comply with whatever legislation is passed;[72]

b) Responsible parties may be liable for stringent penalties for poor or non-compliance; and

c) List brokers may suffer loss of business if third party lists are withdrawn until these are compliant. This could put companies out of business. The implication of not being able to do business should not be underestimated.[73]

---

in their proposal in terms of the Open Democracy Act made the following interesting remarks when the affordability of the Open Democracy Bill was discussed (At the time the Open Democracy Act also included sections pertaining to privacy protection. These were removed to form a separate Privacy Act. See discussion above in Chapter 1).

The question of cost is an important one, but it must be evaluated in a context which takes account of all the material considerations.....Cost estimates can be exaggerated: there is general tendency for officials confronted with new legislation to fear it, and consequently to exaggerate the likely cost. For these reasons, there is a need to evaluate cost estimates cautiously, alert to the factors which tend to exaggerate them. Despite this it is clear that the administration of the Act will compete for resources urgently needed elsewhere and that it is the responsibility of the Task Group to make recommendations which will minimise the cost to Government of the Act.

71 Korff ***Comparative Study*** at 207.

72 The USA is also debating the merits of privacy legislation and a major part of the debate concerns the costs to business.

73 It was argued that ways should rather be found to guide these companies and make things work in a practical way instead of finding ways to make life difficult and in the same process put people out of work. Barnard F "Informal Notes from the DMA to the Law Commission re a possible new Data Privacy Act for SA" 14 September 2001 at 6.

Sanctions and remedies[74]

7.2.32 All information protection legislation stipulate a variety of sanctions and remedies for breach of their provisions. Provision is usually made for a combination of penalties (fines and imprisonment), compensatory damages and where applicable, revocation of licences and deregistration.

7.2.33 In some jurisdictions, the enforcement of information protection laws rarely involves meting out penalties in the form of fines or imprisonment. A variety of other means of remedying recalcitrance - most notably dialogue and, if necessary, public disclosure via the mass media - seem to be preferred instead. In other words, information protection laws often work by persuasion, is enforced by shame and punished by blame.[75]

7.2.34 The topic of sanctions and remedies is dealt with only in very general terms by the CoE Convention, OECD Guidelines and UN Guidelines. The EU Directive is more specific. It requires that data subjects be given the right to a "judicial remedy" for "any breach" of their rights pursuant to the applicable national data protection law.[76] It also stipulates that decisions by a data protection authority which give rise to complaints "may be appealed against through the courts".[77]

(ii) Self-regulatory system (eg USA)

7.2.35 The private sector in the United States is a good example of the second category of

---

74 See discussion in Chapter 8 below.

75 Bygrave ***Data Protection*** at 79 and references therein.

76 Article 22.

77 Article 28(3).

enforcement systems since it is dealt with by a self-regulatory system.[78] Industries in the private sector are encouraged to self-regulate. The law only intervenes on a narrowly targeted basis to solve specific issues where the marketplace is perceived to have failed. [79]

7.2.36 American privacy policies are derived in part from the Constitution, in part from federal laws, in part from state law and in part from the common law. Ad hoc sectoral statutes, thus, address only an eclectic set of problems. In addition, voluntary policies adopted by companies and trade associations are significant influences.[80]

7.2.37 Sectoral laws can be regarded as a patchwork of laws that regulate the collection and dissemination of different types of personal information in different ways, depending on how it is acquired, by whom, and how it will be used. Although these laws provide some level of privacy protection, they are not comprehensive in the sense that they do not apply uniformly to all service providers. [81]

7.2.38 For instance, in the USA, Congress has created specific statutory rights to privacy for oral and electronic communications;[82] financial, educational and credit information;[83] criminal history,[84] and even video rental records.[85] All of these laws were passed following collaboration among civil liberties-, consumer-, and industry groups.[86]

---

78 The Privacy Act of 1974,5 U.S.C. regulates the public sector.

79 Reidenberg presentation 2001 at 2.

80 Ibid.

81 US Department of Commerce ***Privacy and the NII: Safeguarding Telecommunications-related Personal Information*** 23 October 1995 (NTIA Privacy Report) (hereafter referred to as the "US Department of Commerce ***Privacy Report"***) at 11.

82 Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510 et seq (1995).

83 The Right to Financial Privacy Act, 12 U.S.C. 3401 (1978); the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g (1974); and the Fair Credit Reporting Act, 15 U.S.C. 1681 (1970).

84 Privacy Act of 1974, 5 U.S.C. 552a (1974); Freedom of Information Act, 5 U.S.C. 552 (1966).

85 The Video Privacy Protection Act 1988, 18 U.S.C. 2710.

86 Goldman ***Brandeis Lecture*** at 2 and references therein to the abovementioned legislation.

7.2.39 However, the eclectic statutory response illustrates the limitations of this method. Few meaningful legal privacy protections exist for some important categories of records, for example, marketing information.[87] Sectoral regulations are reactive and inconsistent. Furthermore, credit reporting agencies providing credit history information in connection with credit eligibility decisions are regulated, but direct marketing organisations providing similar information for pure marketing purposes are not. Drug abusers for example, have stronger protection than web users and video rental titles must be held confidential, though medical records can be disclosed.[88]

7.2.40 This statutory gap-filling approach also leaves many areas of information processing untouched and runs counter to the cross-sectoral nature of modern information processing.[89]

7.2.41 Since there is no comprehensive privacy legislation, there is also no oversight agency dealing specifically with information privacy. As a result, individuals with complaints about privacy must pursue expensive lawsuits, or they may have no recourse at all. Also, foreign governments do not have an accessible forum to bring concerns about disparate privacy regulation.[90]

7.2.42 In the USA there is general distrust of state control of economic and social matters, accompanied by scepticism towards legislative regulation of the private sector except where there are proven to exist flagrant imbalances of power between private parties which cannot be corrected otherwise than by legislative intervention. Industries have therefore been encouraged to self-regulate. [91]

---

87 Gellman RM "Data Privacy Law (book review)" ***Government Information Quarterly*** Vol 14 No 2 1997 at 215-217 in a review of the book by Scwartz PM and Reidenberg JR ***A Study of United States Data Protection*** Charlottesville, VA Michie 1996; see, however, the discussion on the new CAN-SPAM Act of 2003 in Chapter 5 above. This Act deals with unsolicited marketing but is not in compliance with the EU Directives published in this regard.

88 Reidenberg presentation 2001 at 2.

89 Reidenberg presentation 2001 at 5.

90 Gellman book review supra.

91 Froomkin ***Stanford Law Review*** 2000 at 1525.

7.2.43 It is often overlooked that self-regulation is nothing new, but actually nothing more or less than the default position of the way in which most problems are solved in an orderly society. If legislation or other forces do not intervene, it is self-regulation by which individuals and organisations handle their interests.[92]

7.2.44 The incentives for self-regulation can be described as moral persuasion, the desire to avoid adverse publicity and the seeking of a competitive advantage through regulating privacy practices.[93]

7.2.45 However, since the economic incentive to provide strong privacy protection is either weak, nonexistent, or at least non-uniformly distributed among all participants in the marketplace, most serious proposals for self-regulation among market participants rely on the threat of government regulation if the responsible parties fail to regulate themselves sufficiently.[94]

7.2.46 In a more positive sense, self-regulation is often advanced as a means of experimenting and to prepare for regulation in a positive way. Self-regulation may also serve as a sector-specific way to implement legislation and to avoid too much detail in the legislation itself. A last option is that self-regulation can serve as a way to provide solutions beyond the scope of the existing legislation, which may or may not result in a new cycle of policymaking along the lines mentioned above.[95]

7.2.47 In order for institutions to regulate themselves four interrelated policy instruments may play a role,[96] namely privacy statements, privacy codes, privacy standards and privacy seals.

---

92 Hustinx PJ "Co-regulation or Self-regulation by Public and Private Bodies - the Case of Data Protection" Published in Freudendesgabe fur Alfred Bullesbach 2002 Umbruch von Regelungssystemen in der Informationgesellschaft accessed at http://www.dutchdpa.nl/documenten/enon 11/11/07 (hereafter referred to as "Hustinx") at 2.

93 Bennett ***Government Foundation Paper*** 2001 at 23; Raab C D "Privacy Protection: The Varieties of Self-regulation" Paper delivered at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002 (hereafter referred to as "Raab presentation 2002").

94 Froomkin 2000 ***Stanford Law Review*** at 1525.

95 Hustinx at 2.

96 Raab presentation 2002 at 1.

Privacy commitments/ statements

7.2.48 Privacy commitments perform no other function than to indicate to clients, consumers and regulators that the orgnisation has considered privacy protection at some level, and believe that it would be good policy to state a set of commitments. They place on record what the organisation believes it does with a consumer's or a client's personal information. Many examples can be found in the privacy statements on contemporary public and private sector websites.[97] It is brief pledges intended for external consumption rather than to affect internal organisational functions. It rarely reflects any deep organisational culture and is often symbolic in nature. It may, however, be useful in stating the company's policies in a brief, open and "user friendly" manner.[98]

Codes of conduct

7.2.49 Codes offer a flexibility and can be adapted to the specific economic, technological and regulatory contexts of different sectors.[99] 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.[100]

7.2.50 The successful implementation of privacy policy is inextricably linked to the ways in which that policy is developed. Before any codification takes place, a central question should be posed: Should the policy merely reflect existing business approaches, or should it reflect goals for which the organisation might strive in future. The correct answer is that it should reflect a thorough

---

97 Bennett ***Government Foundation Paper*** 2001 at 17.

98 Bennett presentation 2002 at 18.

99 See discussion on codes of conduct below.

100 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.univ.za/polisci/bennett accessed on 29/10/2002 (hereafter referred to as Bennett Evaluation of Privacy Codes" at 4.

understanding of existing practices, as well as a commitment to improve.[101]

7.2.51 In short, the organisation should be prepared to implement any policy it codifies. The term "code of conduct" should be reserved for codified policies that not only state commitments to the outside world, but also bind employees to these obligations.

7.2.52 Many codes are developed in the absence of a regulatory framework in order to avoid or anticipate further regulatory intervention.[102] The debate about personal privacy protection for the private sector is often couched as a choice between the "voluntary" code and legislation. This is a false dichotomy. The range of possible incentives for compliance falls along a complicated continuum. At the one end is the purely voluntary code in which there is neither internal nor external compulsion to develop, adopt or implement privacy standards. At the other is the code existing within a full set of statutory obligations and liabilities. Some codes, for example that of the Canadian banking industry, fall in the middle of this continuum where a complicated and fluctuating range of incentives and sanctions are continuously at work.[103]

7.2.53 Five kinds of privacy code can be identified[104] according to their scope of application: organisational code[105], the sectoral code,[106] the functional code[107], the professional code[108] and the

---

101 Bennett Evaluation of Privacy Codes 1997 at 16.

102 In contrast to codes that are developed to implement or supplement legislation as is the case within the framework of statutory data regimes.

103 Bennett Evaluation of Privacy Codes 1997 at 21.

104 Raab presentation 2002 at 9-11. See also Bennett and Raab ***The Governance of Privacy*** at 123-126.

105 This applies to one agency that is bound by a clear organisational structure.

106 The defining feature of a sectoral code is that there is a broad consonance of economic interest and function and a similarity in the kinds of personal information collected. Examples are the banking industry, life insurance etc.

107 This code is defined less by the economic sector and more by the practice in which the organisation is engaged, for example direct mail and marketing. The Direct Marketing Association in South Africa represents businesses in a wide number of sectors.

108 Codes developed for those directly involved in information processing activities eg market researchers and health professionals.

technological code[109].

Privacy standards

7.2.54 Privacy standards extend the self-regulatory code of practice in some important ways. Standards imply that a process exists through which an organisation's claims that they are adhering to privacy rules can be objectively tested. Technical standards may, for instance, include both a code of practice for computer security and a standard specification for security management systems, which includes a risk analysis for the different categories of information stored by the organisation.[110]

7.2.55 The idea of a more general privacy standard[111] that could incorporate the entire range of privacy protection principles was negotiated in Canada.[112] In this case the federal government announced its intention to introduce federal legislation based on the standard shortly after the standard was published, so there was never a pure test of whether a market mechanism alone would encourage registrations. General standards, similar to that of Canada's CSA, were also negotiated in Australia and Japan.[113]

7.2.56 The Centre Europeanne de Normalisations (CEN), responsible for the negotiation of standards within Europe, and supported by the Article 29 Working Party, has begun to study the feasibility of an international privacy standard. This would comprise a general information protection standard which would set out practical operational steps to be taken by an organisation in order

---

109 As new potentially intrusive technologies have entered society, codes have developed to deal with their specific application.

110 Bennett presentation 2002 at 22. See in this regard the British Standard, BS7799.

111 Bennett presentation 2002 at 23.

112 The Model Code for the Protection of Personal Information was passed in September 1995 and was subsequently approved as a "National Standard of Canada" by the Standards Council of Canada.

113 In 1999 the Japanese Standards Association released JIS Q 15001. In Australia a set of National Privacy Principles were issued in 1998 by the Privacy Commissioner. The idea was to get Australian business to adopt these Principles in a formal manner. As in Canada, this initiative was overtaken by a more general legislative approach.

to comply with relevant information protection legislation, a series of sector specific initiatives in key areas such as health information and human resource management and task specific initiatives mainly related to the online environment. [114]

Privacy seals

7.2.57 One logical corollary of any standard is a commonly understood mark, symbol or cachet that can be awarded to any organisation that is successfully certified or registered. The development of a specific "mark" or "seal" for privacy protection has, however, proliferated on the Internet. These programmes are built on the premise that consumers should be able to have consistent disclosure of privacy practices from all sites with which they interact.

7.2.58 To build consistency, these licencing programmes require participating websites to post a privacy policy disclosing their online information-gathering and dissemination practices. A cornerstone of these programmes is an online branded seal displayed by member websites and which is only awarded to sites that adhere to established privacy principles and agree to comply with ongoing oversight and dispute resolution procedures.[115]

7.2.59 What is needed therefore is a granting organisation responsible for examining private enterprises' applications for the privacy mark and then certifying them. The enterprise must also have a compliance programme complying with the previously set guidelines (based on the guidelines of the business to which the enterprise belong). It must also demonstrate that personal information is appropriately managed based on the compliance programme or that a feasible structure has been established. The certification is then in existence for a specific period, for example two years.[116]

---

114 Bennett presentation 2002 at 24.

115 Bennett presentation 2002 and references therein.

116 Supra at 25.

7.2.60 Current seal programmes have not, however, inspired great confidence.[117] Furthermore, the more privacy seal programmes in existence, the more the consumer will be confused, and the more difficult it will be for any one system to achieve a reputation as the methodology by which privacy protective practices can be claimed and assured. [118]

7.2.61 Ideally these four instruments (commitments, codes, standards and seals) should be cumulative. The self-regulatory process should involve:[119]

a) an agreement and statement of organisational policy;

b) a codification of that policy throughout the oganisation or sector;

c) a verification of those practices through some external and independent conformity assessment process; and

d) the assignment of a "seal of good housekeeping".

7.2.62 More often than not, however, public claims are made without adequate internal analysis, or external auditing. And privacy seals are invariably awarded without proper codification and verification of organisational practices. Therefore, the number of organisations that have engaged in privacy self-regulation in this cumulative and logical manner are very few.[120]

7.2.63 A more generic problem with self-regulatory schemes is that they regulate only those motivated or principled enough to take part in them.[121]

---

117 See discussion in Froomkin 2000 ***Stanford Law Review*** at 1525 as to the actions of the trustmarkholder TRUSTe. It became clear that firms licence the trustmark and some corporate sponsors contribute huge sums of money in support. If the trustmarkholder would start suspending trustmarks it would lose revenue; if it were to get a reputation for being too aggressive towards clients, they may decide they are better off without the trustmark and the attendant hassle.

118 Bennett presentation 2002 at 26.

119 Ibid.

120 Bennett presentation 2002 at 26.

121 Froomkin 2000 ***Stanford Law Review*** at 1528.

7.2.64 In 1998 the Department of Commerce in the USA was requested to report to the President on industry efforts to establish self-regulating regimes to ensure privacy online and to develop technological solutions to protect privacy.[122] In this document it was stressed that to implement meaningful, consumer-friendly, self-regulatory regimes to protect privacy, self-regulation must do more than articulate broad policies or guidelines. Effective self-regulation also involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from non-compliance.

7.2.65 A self regulatory privacy regime should, therefore, include mechanisms to assure compliance with the rules and appropriate recourse to an injured party when the rules are not followed. Such mechanisms are:

a) Consumer recourse mechanisms: mechanisms through which complaints and disputes can be resolved. They should be readily available and affordable.

b) Verification Procedure: This provides attestation that the assertions businesses make about their privacy practices have been implemented as represented. Because verification may be costly for business, appropriate cost-effective ways must be found to provide companies with the means to provide verification.

c) Consequences: Failure to comply with fair information practices should have consequences. Examples of such consequences include cancellation of the right to use the certification seal or logo, posting the name of the non-complier on a “bad actor” list, or disqualification from membership in an industry trade association. Non-compliers could also be required to pay the costs of determining their non-compliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion.

---

122 National Telecommunications and Information Administration, Department of Commerce United States of America ***Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy*** Notice and request for public comment RIN 0660-AA13 dated 6 May 1998 (hereafter referred to as “ NTIA Commerce Report”) at 1.

(iii) Co-regulatory system (eg Australia)

7.2.66 The third system identified is the co-regulatory system. This concept refers to self-regulation by an industrial association with governmental oversight and ratification.[123] It has been argued that this mixture of legislation and self-regulation may provide the optimum solution, offering advantages of flexibility and low-compliance of self-regulatory systems with the rights, obligations and enforceable bottom line of legislative guarantees.[124]

7.2.67 In Australia a set of National Privacy Principles were issued for the private sector in February 1998 by the Privacy Commissioner. At this stage only the public sector was formally regulated. The overall aim was to get Australian business to adopt these Principles in a formal manner, and thus to produce greater consistency in the Australian marketplace.

7.2.68 In December 1998, the Commonwealth Government announced its intention to legislate to support these Privacy Principles. The Privacy Amendment (Private Sector) Act was passed in December 2000 and came into force a year later. The broad acceptance by business of a set of national standards eased the process by which information protection law could be introduced for the private sector.

7.2.69 In this co-regulatory system industry codes play a far more central role than in other countries.[125] It can be seen as a form of voluntary regulation within the confines of broader legislative provisions.

7.2.70 In Australia an organisation or industry registering a Privacy Code under the Australian

---

123 Bennett and Raab ***The Governance of Privacy*** at 184 notes that a distinction should be made between co-regulation and enforced self-regulation.

124 Parliament of Australia Senate Legal and Constitutional Committee **Privacy in the Private Sector** Chapter 7 The Co-regulation model 1999 accessed at http://www.aph.gov.au/senate/committee/legcon_ctte/ on 2005/04/25.

125 Bennett and Raab ***The Governance of Privacy*** at 129.

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.[126] Where a code is not established, the Privacy Principles set out in the Act automatically apply.

7.2.71 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. The Privacy Commissioner may also create and issue a Code, based on his or her own initiative or on the application of any other person. Legislation sets out the conditions subject to which a Commissioner may issue a Code. It may for instance stipulate that the code should provide for the appointment of an independent adjudicator to whom complaints may be made, the responsibilities and duties of such an adjudicator etc. It may also make provision for the review procedures of an adjudicator's decision under the approved privacy code.[127]

7.2.72 Caution should be exercised where a code of conduct exists in that the code should not create a lesser standard than that set out in the Privacy Principles and thereby fall below the adequacy standard set out in the EU Directive. Another aspect to be noted is that companies operating in two or more industries (eg media and communications) should not be subject to multiple codes.[128] The cost of compliance with these standards may, furthermore, out-weigh the cost of compliance with formal legislation.[129]

7.2.73 Relatively few Codes have so far been established. By far the greater number of businesses within the private sector, especially small to medium sized organisations rely solely on the Privacy Principles as set out in the Act, without feeling the need to develop a Code of Conduct.

---

126 Michalsons for IMS. In March 2003, the Internet Industry Association of Australia lodged an application for registration of their Privacy Code of Practice for member companies with the Federal Office of the Privacy Commissioner. Concurrently, they have sought a ruling from the EU regarding adequacy and it is expected to have a positive resolution for trans-border transfers once local ratification is complete.

127 See for example Part IIIA of the Australian Privacy Act 1988 as amended.

128 Senate Committee at 6.

129 Bennett and Raab ***The Governance of Privacy*** at 129.

(iv) A proposed information protection system for South Africa

7.2.74 In comparing different information protection laws, cross-national regulatory trends[130] can be identified.[131] Some of these are as follows:

* Increasing regulatory density, therefore more detailed discriminating provisions and requirements;
* Increasing concern to lay down procedural mechanisms for enforcing compliance with the information principles;
* A shift in regulatory focus, for instance the encouragement of sectoral codes of practice;
* A trend away from comprehensive licencing regimes to requirements for mere notification/registration of information-processing operations; and
* Enhancement of opportunities for participatory control.

7.2.75 A highly efficient information protection system would therefore comprise:[132]

* A strong and unambiguous law;
* An active and assertive regulatory authority;
* A strong commitment by responsible parties, reflected at least in the establishment of the requisite procedures for compliance and, in particular, by an effort to collect as little information as possible for the carrying out of legitimate activities;
* With respect to private sector compliance, a set of market incentives that drive companies to be pro-privacy and to implement those goals through strong self-

---

130 In data protection discourse it is popular to categorise these trends in terms of generations: ie first-, second- and third-generation data protection laws. See Bygrave ***Data Protection*** at 88.

131 Bygrave ***Data Protection*** at 88.

132 Bennett and Raab ***The Governance of Privacy*** at 207.

regulatory mechanisms;

* A vigilant, concerned and activist citizenry that is prepared to complain, to exercise access and correction rights, and to opt out of secondary uses of their information;

* The application, as far as possible at the outset of system development, of privacy-enhancing technologies to assist in the overall provision of privacy protection.

No a priori judgment can be made about the relative importance of each of these trends; all are necessary conditions for high quality information protection. None is a sufficient condition.

7.2.76 It is therefore clear that, though conceived as distinct rule sets, the legal, technological and market models of fair information practices are interdependent as tools for effective information protection. The different models or instruments need to be channelled in the same direction so that the rules support rather than frustrate each other.[133] PET's (privacy enhancing tools) is furthermore to be regarded as a useful complement to existing regulatory and self-regulatory approaches.[134]

7.2.77 The Commission's proposal in the Discussion Paper was, therefore, that a comprehensive Act should be instituted with or without sectoral legislation and codes of conduct, to be implemented within a regulatory system. The regulatory system should be implemented by a statutory regulatory authority, with wide-ranging duties and responsibilities, working in conjunction with regulatory authorities in individual sectors. [135]

---

133 Reidenberg presentation 2001at 3.

134 Bennett and Raab ***The Governance of Privacy*** at 153 referring to PISA's (Privacy Incorporated Software Agent) project specification which says that "rather than relying on legal protection and self-regulation only, the protection of consumer's privacy is more effective if transactions are performed by means of technologies that are privacy enhancing". See also Principle 6 dealing with security, section 18 of the proposed Act which refers to technical and organisational measures to be implemented by the responsible parties to secure information.

135 In the Discussion Paper the Commission therefore proposed that the information protection enforcement system be set out as follows:

CHAPTER 5

SUPERVISION

Part A
Information Protection Commission

Establishment of Commission

34. There is hereby established a body to be known as the Information Protection Commission.

Constitution of Commission and period of office of members

35. (1)(a)The Commission must consist of the following members, appointed by the State President -

(i) a chairperson known as the Information Commissioner;

(ii) two other persons known as ordinary members of the Commission.

(b) Members of the Commission must be appropriately qualified, fit and proper persons 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.

(c) The chairperson of the Commission must perform his or her functions under this Act in a full-time capacity and must not be employed in any other capacity during any period in which the person holds office as Information Commissioner.
(d) The other members of the Commission must be appointed in a part-time capacity.

(e) The Chairperson must direct the work of the Commission and the Secretariat.
(f) No person will be qualified for appointment as a member of the Commission if that person –

(i) is a member of Parliament;

(ii) is a member of a local authority;

(iii) is an unrehabilitated insolvent; or

(iv) has at any time been convicted of any offence involving dishonesty.

(2) The State President may appoint one or more additional members if he deems it necessary for the investigation of any particular matter or the performance of any duty by the Commission.

(3) The members of the Commission will be appointed for a period of not more than five years and will, at the expiration of such period, be eligible for reappointment.

(4) A person appointed as Information Commissioner may resign from office by writing under his or her hand addressed to the President and will in any case vacate office on attaining the age of seventy years.

(5) A member may be removed from office only for inability to discharge the functions of the office (whether arising from infirmity of body or mind or any other cause) or for misbehaviour.

Remuneration, allowances, benefits and privileges of members

36.(1) A member of the Commission who-

(a) is a judge of the Constitutional Court, the Supreme Court of Appeal or a High Court will, notwithstanding anything to the contrary contained in any other law, in addition to his or her salary and any allowance, including any allowance for reimbursement of travelling and subsistence expenses, which may be payable to him or her in his or her capacity as such a judge, be entitled to such allowance (if any) in respect of the performance of his or her functions as such a member as the President may determine;

(b) is not such a judge and is not subject to the provisions of the Public Service Act, 1994 (Proclamation103 of 1994), will be entitled to such remuneration, allowances (including allowances for reimbursement of travelling and subsistence expenses incurred by him in the performance of his functions under this Act), benefits and privileges as the Minister in consultation with the Minister of Finance may determine.

(2) The remuneration, allowances, benefits or privileges of different members of the Commission may differ according to -

(a) the different offices held by them in the Commission; or

(b) the different functions performed, whether in a part-time or full-time capacity, by them from time to time.

(3) In the application of subsections (1) and (2), the President or the Minister, as the case may be, may determine that any remuneration, allowance, benefit or privilege contemplated in those subsections, will be the remuneration, allowance, benefit or privilege determined from time to time by or under any law in respect of any person or category of persons.

Secretary and staff

37.(1) The secretary of the Commission and such other officers and employees as are required for the proper performance of the Commission's functions, will be appointed in terms of the Public Service Act, 1994 (Proclamation 103 of 1994).

(2) The Commission may, with the approval of the Minister in consultation with the Minister of Finance, on a temporary basis or for a particular matter which is being investigated by it, employ any person with special knowledge of any matter relating to the work of the Commission, or obtain the co-operation of any body, to advise or assist the Commission in the performance of its functions under this Act, and fix the remuneration, including reimbursement for travelling, subsistence and other expenses, of such person or body.

Funds

38. Parliament will appropriate annually, for the use of the Commission, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Commission, of its powers, duties and functions under this Act.

Powers and duties of Commission

39. (1) The powers and duties of the Commission will be---

education

(a) to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles;
(b) for the purpose of promoting the protection of personal information, to undertake educational programmes on the Commission's own behalf or in co-operation with other persons or authorities acting on behalf of the Commission;
(c) to make public statements in relation to any matter affecting the protection of the personal information of a person or of any class of persons;

monitor compliance

(d) to monitor compliance by public and private bodies of the provisions of this Act;
(e) to undertake research into, and to monitor developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of persons are minimised, and to report to the responsible Minister the results of such research and monitoring;
(f) to examine any proposed legislation (including subordinate legislation) or proposed policy of the Government that the Commission considers may affect the protection of the personal information of individuals, and to report to the responsible Minister the results of that examination;
(g) to report (with or without request) to the Minister from time to time on any matter affecting the protection of the personal information of a person, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the personal information of a person;
(h) when requested to do so by a public or private body, to conduct an audit of personal information maintained by that body for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles;
(i) to monitor the use of unique identifiers of data subjects, and to report to the Minister from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the personal information of a person;

(j) to maintain, and to publish, make available and provide copies of such registers as are prescribed in this Act.
(k) to examine any proposed legislation that makes provision for -
(i) the collection of personal information by any public or private body; or
(ii) the disclosure of personal information by one public or private body to any other public or private body, or both; to have particular regard, in the course of that examination, to the matters set out in section 40(3) of this Act, in any case where the Commission considers that the information might be used for the purposes of an information matching programme; and to report to the responsible Minister the results of that examination;

consultation

(l) to receive and invite representations from members of the public on any matter affecting the personal information of a person;
(m) to consult and co-operate with other persons and bodies concerned with the protection of information privacy;
(n) to act as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by one person in the interests of the protection of the personal information of another person;
(o) to provide advice (with or without a request) to a Minister or a public or private body on their obligations under the provisions, and generally, on any matter relevant to the operation, of this Act;

complaints

(p) to receive and investigate complaints about alleged violations of the protection of personal information of persons and in respect thereof make reports to complainants;
(q) to gather such information as in the Commission's opinion will assist the Commission in discharging the duties and carrying out the Commission's functions under this Act;
(r) to attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation;
(s) to serve any notices in terms of this Act and further promote the resolution of disputes in accordance with the prescripts of this Act;

research and reporting

(t) to report to the Minister from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a person;
(u) to report to the Minister on any other matter relating to protection of information that, in the Commission's opinion, should be drawn to the Minister's attention;

codes of conduct
(v) to issue, from time to time, codes of conduct, amendment of codes and revocation of codes of conduct;
(w) to make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct;
(x) to review an adjudicator's decision under approved codes of conduct;

general
(y) to do anything incidental or conducive to the performance of any of the preceding functions;
(z) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commission by or under this Act or any other enactment.

(2) The Commission may, from time to time, in the public interest or in the interests of any person or body of persons, publish reports relating generally to the exercise of the Commission's functions under this Act or to any case or cases investigated by the Commission, whether or not the matters to be dealt with in any such report have been the subject of a report to the responsible Minister.

Commission to have regard to certain matters

40. (1) The Commission is independent in the performance of its functions.

(2) In the performance of its functions, and the exercise of its powers, under this Act, the Commission must -

(a) have due regard to the protection of personal information as set out in the information protection principles; and
(b) have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way; and
(c) take account of international obligations accepted by South Africa, including those concerning the international technology of communications; and
(d) consider any developing general international guidelines relevant to the better protection of individual privacy.

(3) In performing its functions in terms of section 39(1)(k) of this Act with regard to information matching programmes, the Commission must have particular regard to the following matters -

(a) whether or not the objective of the programme relates to a matter of significant public importance;

(b) whether or not the use of the programme to achieve that objective will result in monetary savings that are both significant and quantifiable, or in other comparable benefits to society;

(c) whether or not the use of an alternative means of achieving that objective would give either of the results referred to in paragraph (b) of this section;

(d) whether or not the public interest in allowing the programme to proceed outweighs the public interest in adhering to the information protection principles that the programme would otherwise contravene;

(e) whether or not the programme involves information matching on a scale that is excessive, having regard to -

(i) the number of agencies that will be involved in the programme; and

(ii) the amount of detail about an individual that will be matched under the programme;

Programmes of Commission

41. (1) In order to achieve its objects the Commission must from time to time draw up programmes in which the various matters which in its opinion require consideration are included in order of preference, and must submit such programmes to the Minister for approval.

(2) The Commission may include in any programme any suggestion relating to its objects received from any person or body.

(3) The Commission may consult any person or body, whether by the submission of study documents prepared by the Commission or in any other manner.

(4) The provisions of sections 2, 3, 4, 5 and 6 of the Commissions Act, 1947 (Act 8 of 1947), will apply mutatis mutandis to the Commission.

Protection of Commission

42. No criminal or civil proceedings lie against the Commission, or against any person acting on behalf or under direction of the Commission, for anything done, reported or said in good faith in the course of the exercise or performance or purported exercise or performance of any power, duty or function of the Commission under this Act.

Meetings of Commission

43.(1) Meetings of the Commission must be held at the times and places determined by the chairperson of the Commission.

(2) The majority of the members of the Commission will constitute a quorum for a meeting.

(3) The Commission may regulate the proceedings at meetings as it may think fit and must keep minutes of the proceedings.

Reports of Commission

44.(1) The Commission must prepare a full report in regard to any matter investigated by it and must submit such report to the Minister for information.

(2) The Commission must within five months of the end of a financial year of the Department for Justice and Constitutional Development submit to the Minister a report on all its activities during that financial year.

(3) The report referred to in subsection (2) must be laid upon the Table in Parliament within fourteen days after it was submitted to the Minister, if Parliament is then in session, or, if Parliament is not then in session, within 14 days after the commencement of its next ensuing session.

Committees of Commission

b) Evaluation

7.2.78 Respondents to the Discussion Papers made the following specific comments

---

45.(1) The Commission may, if it deems it necessary for the proper performance of its functions-

(a) establish a working committee, which must consist of such members of the Commission as the Commission may designate;

(b) establish such other committees as it may deem necessary, and which must consist of-

(i) such members of the Commission as the Commission may designate; or

(ii) such members of the Commission as the Commission may designate and the other persons appointed by the Minister for the period determined by the Minister.

(2) The Minister may at any time extend the period of an appointment referred to in subsection (1) (b) (ii) or, if in his opinion good reasons exist therefor, revoke any such appointment.

(3) The Commission must designate the chairman and, if the Commission deems it necessary, the vice-chairman of a committee established under subsection (1).

(4) (a) A committee referred to in subsection (1) must, subject to the directions of the Commission, perform those functions of the Commission assigned to it by the Commission.

(b) Any function so performed by the working committee referred to in subsection (1) (a) will be deemed to have been performed by the Commission.

(5) The Minister or the Commission may at any time dissolve any committee established by the Commission.

(6) The provisions of sections 41(4) and 43 will mutatis mutandis apply to a committee of the Commission.

Part B

Information Protection Officer

Information protection officer to be appointed

46.(1) Each responsible party must ensure that there are, within that body, one or more information protection officers whose responsibilities include -

(a) the encouragement of compliance, by the body, with the information protection principles;

(b) dealing with requests made to the body pursuant to this Act;

(c) working with the Commission in relation to investigations conducted pursuant to Chapter 6 of this Act in relation to the body;

(d) otherwise ensuring compliance by the body with the provisions of this Act.

(2) Officers must take up their duties only after the responsible party or body which appointed them has registered them with the Commission.

regarding the systems identified above:

(i) Regulatory system

Comprehensive law[136]

7.2.79 Respondents in favour of the regulatory approach stated that a new privacy law is now urgently required.[137] The legislature must facilitate good practice in so far as the protection of privacy in general, and informational privacy in particular, are concerned and should, through the enactment of appropriate legislation, make provision for the mechanisms to facilitate this, including the appointment of a body responsible for the administration of such legislation with sufficiently defined powers and functions. Where these rights are not respected, the legislation should provide for judicial remedies which should be imposed on anyone, whether in the private or public sector, who fails to comply with the provisions of privacy and information protection legislation.[138]

7.2.80 Respondents agreed that the legislation enacted should follow the broad principles laid down in the OECD Guidelines and in the EU Directive and argued that to follow the self-regulatory approach, the sectoral law approach or even the co-regulatory approach, will not generally be sufficient to qualify such legislation within the "adequate protection" requirement of the EU Directive.[139]

7.2.81 It was argued that consolidated national information protection legislation will:

* Provide a consistent approach to privacy and information protection across all

---

136 The USA Department of Commerce was the only respondent not in favour of a comprehensive law. See discussion on self-regulation in Para 7.2.170 below.

137 Financial Services Board; ENF for Nedbank.

138 ENF for Nedbank.

139 Nedbank; See discussion in Ch 6 above regarding the adequacy requirement.

sectors of the economy based on the founding principles[140] listed in Chapter 4. [141]

* Go a long way in providing guidance and clarity in the regulatory and legislative environments pertaining to privacy and information protection. [142] The current legal situation is fraught with legal uncertainty (even as regards public sector rights to obligatorily demand disclosures from individuals), which must be clarified as soon as possible in the public interest.[143]

* Create an overall stable and investment-friendly regulatory and legislative framework, benefitting the South African economy and its people.[144]

* Give effect to both the South African common law and the Constitution of the Republic of South Africa in recognising and protecting the right to privacy (section 14 of the Constitution). [145]

* Ensure that South African organisations are able to compete in the international information-technology based services market through cross-border transactions.[146]

7.2.82 The objectives of an information protection system should essentially be:[147]

* To require compliance by responsible parties with the rules. A good system is generally characterised by a high degree of awareness among responsible parties of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an

---

140 Fair and lawful processing, Openness; Collection limitation; Use/Purpose specification; Disclosure limitation; individual participation; Data quality; Finality; Security safeguards; Accountability and Sensitivity.

141 Vodacom (Pty)Ltd.

142 Vodacom (Pty) Ltd.

143 Financial Services Board, Banking Council.

144 Vodacom (Pty) Ltd.

145 Eskom Legal Department; The Legislature forms part of the State and the latter must "*respect, protect, promote and fulfil the rights in the Bill of Rights"* (section 7(2) of the Constitution). In promoting the current type of new law, the State will be doing exactly what is so required.

146 ENF for Nedbank.

147 ENF for Nedbank.

important part in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

* To provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

* To provide appropriate redress to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which provides for compensation to be paid and sanctions imposed where appropriate.

* To create a balance between protection and use of information on the one hand and ensuring adherence to privacy principles of the data subject on the use of the information.

Regulatory agency for South Africa?

7.2.83 One of the South African Law Reform Commission's preliminary proposals set out in its Discussion Papers[148] dealing with privacy and information protection was that a statutory regulatory agency should be established. A flexible approach was, however, advised in which industries would develop their own codes of conduct which would then be overseen by the regulatory agency. Comment was invited on these proposals.

7.2.84 The Commission received a mixed reaction from respondents. Many of the comments received were in favour of a statutory agency,[149] but some differed as to the powers to be afforded to such an institution.[150] Some respondents expressed their opposition to the creation of an

148 SALRC Issue Paper 24; Discussion Paper 109.

149 Eg MFSA; SAHA; ENF for Nedbank; ISPA; IMS; SNO (Second National Operator); Law Society of South Africa; Cell C; Society of Advocates; Dr MDC Motlala; SA Medical Research Council; Department of Home Affairs; SAFPS.

150 SAFPS; FSB.

oversight agency.[151]

7.2.85 Before discussing these comments it should be noted that this problem was already discussed in debates during consultations on the Open Democracy Bill about the necessity of a regulating agency to ensure enforcement of this Act (which of course included privacy provisions at that stage).[152] The following interesting viewpoints were held:

(a) The *SA Human Rights Commission (SAHRC)*[153] noted that the Open Democracy Bill did not establish an information protection authority as such, but used the Human Rights Commission to perform some of the functions of such an authority. The Bill furthermore set out internal appeal procedures. Should these be exhausted, and an aggrieved applicant (or respondent) remained dissatisfied, the Bill made provision for the High Court as the forum for relief.[154] The HRC believed the High Court to be an inappropriate forum since it is inaccessible to ordinary people, both geographically, and in terms of costs, and it does not present a speedy remedy. It also lacks flexibility around issues of procedure, thereby preventing a development of sound jurisprudence, particularly on the question of the exemptions. The HRC stressed that this was particularly relevant to access to information, where there is no existing precedent, and a body of jurisprudence needs to be developed from scratch. The HRC submitted that an effective and appropriate enforcement mechanism would be crucial to the successful implementation and functioning of the Bill and referred to various options which could replace the use of the High Court, and the court system. These included the creation of a tribunal system, or the use of an ombudsman or Information Commissioner to resolve disputes. The HRC stressed that these options needed careful consideration, with emphasis on the short-term cost implications of setting up new bureaucracies, and the long term cost

151 Eg. Vodacom; SABC; LOA; CAPES; MTN; SAPS.

152 The Bill subsequently became known as the Promotion of Access to Information Act 2 of 2002. The Act did not establish an information or data protection authority. The Justice Portfolio Committee has, however, now requested the Department of Justice to investigate the possibility of establishing an office for an Information Commissioner.

153 Submission to the Open Democracy Bill.

154 PAIA eventually made provision for Magistrates' Courts and magistrates to be specifically designated by the Minister of Justice in terms of section 1 and 91A of the Act as a forum for relief. To date, this has not happened yet.

implications of clogging up the court system even further.[155]

(b) The *Open Democracy Lobby Group*[156] agreed with the HRC and proposed the consideration of the introduction of an interim procedure between the internal and external review by the courts. Such a procedure would be directed towards conciliation and mediation, with the view to facilitating settlements of matters, and would utilise an informal and inquisitorial procedure. It would, however, have authority to make a decision if settlement is not achieved. This could be introduced in the form of an Information Officer, some form of a tribunal, or an Ombudsman.

(c) In their submissions *IDASA and COSATU* made provision for the establishment of an Information Ombudsman appointed by the Minister, in consultation with the Portfolio Committee for Justice and Constitutional Affairs. The main object of the Ombudsman was stated to be to dispose of complaints lodged in terms of the Promotion of Access to Information Act in a procedurally fair, economical and expeditious manner.[157]

7.2.86 When PAIA was enacted it was decided not to institute a regulatory authority. This decision has subsequently been re-evaluated since it has been found[158] that PAIA was not

---

155 PAIA currently also assigns responsibility for promotional and related functions and for dispute-resolution to separate bodies, as did the draft Open Democracy Bill. Moreover, responsibility for dispute-resolution is itself currently split between the Public Protector, which deals with disputes over mal-administration and the courts, which deal with disputes over enforcement of substantive rights under PAIA. The Human Rights Commission devotes three full-time staff members to its PAIA responsibilities. The Head of Research and Documentation, of which the PAIA Unit is a part, also devotes significant time and energy to the unit. A committee called "PAIA.com" oversees the work of the PAIA Unit. Section 8 of the Human Rights Commission Act allows the Commission to attempt dispute-resolution through mediation, conciliation or negotiation and to rectify any act or omission regarding fundamental rights. It also has additional power conferred by other legislation. See further discussion below.

156 Submission to Select Committee on Security and Justice on 11 August 1998 (sponsoring organisations: Black Sash, Environmental Justice Networking Forum, The Human Rights Committee, Idasa, The Legal Resources Centre, The SA Catholic Bishops Conference, SA Council of Churches, SA NGO Coalition).

157 In order to achieve his or her main object, the Ombud: a) would investigate any complaint and may make the order which any court of law may make; (b) may, if it is expedient and prior to investigating a complaint, require any complainant first to approach an organization established for the purpose of resolving disputes, and approved by the registrar. After the Ombud has completed an investigation, he or she shall send a statement containing his or her determination and his or her reasons, signed by him or her, to all parties concerned as well as to the clerk or registrar of the court which would have had jurisdiction had the matter been heard by a court. Any determination of the Ombud shall be deemed to be a civil judgment of any court of law had the matter in question been heard by such court, and shall be so noted by the clerk or the registrar of the court, as the case may be. A writ or warrant of execution may be issued by the clerk or the registrar of the court in question and executed by the sheriff of such court after expiration of a period of six weeks after the date of the determination, on condition that no application contemplated in section 14 has been lodged. Any party who feels aggrieved by a determination of the Ombud may, within six weeks after the date of the determination, apply to the division of the Supreme Court which has jurisdiction, for relief, and shall at the same time give written notice of his or her intention so to apply to the other parties to the complaint.

158 Parliament of the Republic of South Africa ***Report of the ad hoc Committee on the Review of Chapter 9 and Associated Institutions*** A report to the National Assembly of the Parliament of South Africa Cape Town South Africa 31 July 2007 (hereafter referred to as "***Chapter 9 and Associated Institutions Report")*** at 173.

operating as the legislature had intended. Appeals to the courts to challenge decisions denying access to information undermine the effectiveness of the legislation. Recommendations have, therefore, been made for the institution of a regulatory authority of some kind to ensure the more effective implementation of this legislation. [159]

Written responses against the creation of a new independent regulatory authority:

7.2.87 Commentators who were against the creation of a regulatory authority stated that the need for a regulatory authority is questionable. Information privacy should be a matter regulated by law and contract. A Commission would create additional regulation and bureaucracy and little apparent benefit in respect of actual protection of a person's personal information.[160]

7.2.88 The idea was supported that self-regulation should be developed by sector players, founded on the general principles established in the legislation. This would enable sectors to tailor information protection regulation to the specific characteristics of the relevant sector, however, still done on the basis of the principles established in the legislation. It was acknowledged that the legislation should provide recourse for consumer complaints or disputes for failure to comply with the code of conduct in accordance with the principles of self-regulation. The principle of positive regulation should, however, prevail, i.e. regulatory intervention should only be considered for repeated failure to comply with the legislation, eg through the prescription of appropriate and proportionate penalties for repeated breach of information protection provisions. It was noted that the self-regulatory approach that is currently specified in the Electronic Communications and Transactions (ECT) Act could provide guidance in this regard, and re-course for appeal of decisions should remain with the High Court.[161]

7.2.89 It was, furthermore, argued that where recommendations are made for the establishment

---

159 See further discussion below.

160 CAPES.

161 Vodacom (Pty) Ltd.

of a single information privacy regulatory authority, the implication is that such regulatory authority should be well-funded, well-skilled, and well-resourced to perform its task. However, it is of paramount importance that role clarity and jurisdiction in terms of a dedicated information privacy regulatory authority versus a sector-specific regulatory authority is obtained.[162] By implication, any duplication or overlap in jurisdiction with sector-specific regulatory authorities must be avoided, since it will simply result in "forum shopping" or inconsistent approaches in dealing with privacy and information protection matters. [163]

7.2.90 Furthermore, the legislation will need to indicate clearly how co-operation with sector-specific regulatory authorities will occur, especially in dealing with customer complaints.[164]

7.2.91 As an alternative, a more efficient, practical and workable option might be to task sector-specific regulatory authorities with information privacy issues for each particular sector, subject to specifying their powers in the information protection legislation.[165] If this second approach is followed, it is important that sector authorities are sufficiently funded, skilled and resourced to perform this additional role.[166]

7.2.92 Having a sector-specific regulatory authority will ensure that there is an authority whose duty it is to ensure that information protection policies and legislation are adequate and in line with international practice. This will also ensure that there is proper and adequate policing of issues around privacy protection. Such a regulatory authority will also be better placed to make determinations as to whether there is a need for sectoral privacy laws and particularly whether there

---

162 The difference between a sector-specific regulatory authority (instituted by the state) and a self-regulatory adjudicator (instituted and funded by the particular industry) should be noted.

163 Vodacom (Pty)Ltd. In analogy, the current concurrent jurisdiction of ICASA and the Competition Commission can be considered.

164 Vodacom (Pty)Ltd.

165 See also the discussion below on the alignment of regulators.

166 Vodacom (Pty)Ltd.

is a need for specific privacy laws which apply specifically to state owned entities.[167] The existing regulatory bodies, which oversee the various industries, have adequate systems and insight to properly ensure compliance and make the need for an independent regulatory agency or authority unnecessary.[168]

7.2.93 In one submission the long-term insurance industry was cited as an example of a sector with an existing regulatory body. The Financial Services Board oversees the financial services industry and it was argued that they would be the most appropriate regulatory body to oversee the protection of information in long-term insurance.[169] It has insight into the industry and already has systems in place and is actively involved in monitoring compliance, which would minimise costs.[170] Members of an independent oversight agency will not have insight into the requirements and environment applicable to the long-term insurance industry. For instance, the types of products marketed and the processes in place in the long-term insurance industry usually are complex. An outsider may not easily be aware of all of the conflicting issues, if an outsider were to regulate the industry. [171] The long-term insurance industry is also regulated by the Life Offices' Association (LOA). The LOA has various Codes of Conduct which include the protection of registers and information. Add to this that legislation already exists that regulates this industry on this point (like the Policy Protection Rules and the Financial and Advisory Services Act) and it is clear that there is no room for a statutory regulatory agent. Moreover, one must also consider that such an agency will have virtually no experience in this industry and will be compelled to draw on the experience of the FSB or the LOA, creating a multiplicity of functions. Another example is the banking industry which has the Banking Council of South Africa, in addition to being regulated by the Financial Services Board. [172]

---

167 SABC.

168 LOA submission.

169 LOA.

170 LOA.

171 LOA.

172 LOA.

7.2.94 It was argued that it would be more sensible to amplify the functions of these bodies, rather than to create a new agency. Agencies are indeed administratively expensive and tardy and reliant on government to come to life. Government involvement at this juncture adds no value and will retard the process to the point where the law becomes meaningless. One needs only to look at the government initiatives in terms of the ECT Act which have not seen the light of day several years post promulgation to understand this statement.[173]

7.2.95 It was proposed that the envisaged legislation should rather lay down the criteria in terms of which information may be collected, kept and used and that the body which collected the information be the guardian of its information. Should the collecting body not meet the criteria of the legislation or refuse access to its information, an aggrieved party will have recourse to the courts. It is foreseen that a single statutory regulatory authority cannot control the databases of both the public and private sector in view of their vastly different roles and mandates. The creation of yet another statutory body will also be costly and may prolong the implementation of information protection laws.[174]

7.2.96 It was noted that Chapter 9 of the Constitution provides for state institutions to support Constitutional Democracy. The functions and powers of the SAHRC, which is one of the Chapter 9 institutions, encompass those envisaged for the Information Commission. The SAHRC should oversee both PAIA and POPIA.[175]

Respondents who were in favour of a regulatory authority, but only if such an authority had only mediating and educational and ombuds functions. Arguments were as follows:

7.2.97 The appointment of an information commissioner should be avoided, but an

---

173 Liberty.

174 SAPS.

175 MTN.

ombudsperson with legislative power should be considered.[176] The ombudsperson would be responsible for responding to complaints from consumers and other aggrieved persons who believe that their right to privacy has been infringed.[177] It is foreseen that there should be a number of Ombudsman offices in the main centres of the country and an electronic means of submitting complaints via an Internet website and fax on demand service. It is foreseen that the office of The Ombudsman would operate along similar lines to that of The Banking Adjudicator, but with legislative powers to enforce compliance.[178]

7.2.98 The appointment of a Commissioner to act as a policeman in ensuring compliance with information privacy legislation was, however, not supported. Any proposed legislation should, it was submitted, be based on the USA Safe Harbour style of enactment and that industry bodies would be required to ensure compliance by their members and associate organisations. The establishment of a massive bureaucracy to monitor information privacy legislation was not in the best interests of South Africa which, unlike first world countries, has neither the economy nor infrastructure to effectively operate such a system.[179]

7.2.99 It was, however, emphasised that an oversight body is necessary in South Africa to focus public attention on problem areas, even though they might not have the authority to fix the problem. They can for example promote codes of practice and encourage industry associations to adopt them.[180]

Respondents in favour of the creation of a regulatory authority argued as follows:

---

176 SAFPS; See also "What Price Privacy" ***Finance Week*** 26 November 65 where it is estimated by research agency Jupiter that by 2006 business spending on privacy and security issues will be five times that of 2001. This is considered a luxury that the fledgling South African economy and democracy simply cannot afford.

177 Ombudsman for Longterm Insurance Industry stated in an address delivered by the ombudsman, Judge PM Nienaber, at the International Conference of Financial Ombudsman held at the Mariott Downtown Eaton Centre, September 19-21, 2005 on the topic: "Privacy and its impact on dispute resolution": dealt with the reasons for confidentiality of an ombudsman in contracts to the openness in court proceedings. It was argued that a pragmatic (and not dogmatic) approach is needed.

178 SAFPS.

179 SAFPS.

180 MFSA.

7.2.100 It was noted that a key requirement of an adequate and effective information protection system is that an individual faced with a problem regarding his personal information is not left alone, but is given some institutional mechanism to assist in ensuring his problems are addressed. Effective privacy protection must therefore include mechanisms for assuring compliance with the information protection principles, recourse for individuals affected by non-compliance of the principles, and consequences for responsible parties in cases of non-compliance.

7.2.101 At a minimum, such mechanisms must include -

(a) readily available and affordable independent recourse procedures by which each individual's complaint or dispute is investigated and resolved by reference to the Principles;

(b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and correct and that privacy practices have been implemented as presented; and

(c) mechanisms to remedy problems arising out of responsible parties' failure to comply strictly with the principles.

Sanctions must be sufficiently rigorous to ensure that these mechanisms can operate effectively.[181] Relying on the court system is not an effective means of protecting consumer's rights.[182]

7.2.102 It was stated that the important role that over-arching privacy law has in establishing public policy objectives is acknowledged and a statutory regulatory authority as an essential part of an enforceable and comprehensive information protection regime, as set out above, is supported by research.[183] The establishment of a regulatory authority responsible for the enforcement of rights and resolution of disputes under the legislation, as well as the promotion, publicity, education, advice, assistance, monitoring and reporting to Parliament is therefore imperative.[184] An

181 ENF for Nedbank.

182 Nedbank.

183 IMS.

184 SAHA; Department of Home Affairs.

independent and accountable regulatory agency should also be responsible for the harmonisation of the roles, functions and powers of other regulatory bodies dealing with information issues.[185]

7.2.103 Of course, this does not mean that such an authority is the sole means of achieving this objective – but, rather, that it should be viewed as an essential cornerstone to a multi-faceted regime that provides the modern South African with the benefits of e-commerce, economic and telecommunication infrastructure growth, privacy-enhancing technologies and control over their personal information in this progressive environment.[186]

7.2.104 It was stated that the proposal that there be a mechanism (the Information Protection Regulator structure proposed by the SALRC) with overall responsibility for the implementation of the privacy legislation, and which complements the related activities and structures within specific domains ('industries' in the SALRC document), could work well in practice, for health research, and for health care practice in general. In terms of the health research domain, the existing MRC Health Research Ethics Guidelines and other health research ethics guidelines already in use, combined with a well-established national network of Health Research Ethics committees (as provided for in the National Health Act),[187] already provide for many of the functions envisaged in the proposed legislation. The proposed legislation, however, provides essential guidelines for the practical implementation of the privacy requirements which are central to health research and practice, but which are not all catered for at present.[188]

7.2.105 It should be kept in mind that the right to privacy is not absolute and may be limited in appropriate circumstances, provided due process is respected and transparent mechanisms are in place. This limitation, however, requires a properly resourced oversight body/person (such as a privacy commissioner/ ombudsperson/ regulator) to ensure that the rights granted to individuals can be enforced and to ensure that where these rights need to be suspended, that they are done so

185 SNO (Second National Operator) Telecommunications (Pty) Ltd.

186 IMS.

187 National Health Act 61 of 2003.

188 SA Medical Research Council.

with the maximum respect for the right as a whole.[189]

7.2.106 To cultivate a privacy culture in South Africa, it is incumbent upon government to launch educational campaigns on the right to privacy and access to information. It is a fact that the vast majority of South African citizens are wholly ignorant of the mere existence of the right to access information entrenched in the Constitution and as further detailed in PAIA.[190] There is not currently sufficient championing of the right to access to information at higher levels of government.[191] It is also important to link privacy rights to increased usage of information and communication technologies. Many users of electronic communications do not trust these networks to secure their information. Where information gathering bodies are subject to codes of conduct, these should be publicised and users educated on the implications of a responsible party or gatherer violating such codes. [192] However, public relations and awareness campaigns require funds and, in an accountable government environment, require a quantifiable measurement of success in order to sustain access to these critical funds.[193]

7.2.107 It was, furthermore, emphasised that the legislation should have enough teeth to ensure that all responsible parties comply with the legislation, in particular companies who sell information, marketing information and the like. There should be sufficient enforcement mechanisms and suitable punishment for those who flagrantly do not comply with the requirements of the information protection legislation.[194] A separate regulatory authority to oversee compliance within South Africa should have sufficient ability to ensure effective enforcement of contraventions of such legislation.

---

189 ISPA.

190 ISPA.

191 SAHA.

192 ISPA; ISPA has a code of conduct for members and all their members have to clearly display their privacy policies on their Internet web sites and draw users attention to the existence and provisions of such policies. They believe that similar provisions should bind other entities.

193 IMS.

194 Nedbank.

7.2.108 It was argued that it would be important in an independent review mechanism to include provision for making binding orders. This would meet concerns expressed in numerous quarters that PAIA currently fails to provide for sufficiently cheap, accessible, quick, effective and authoritative dispute-resolution.[195]

7.2.109 Even in Canada it has been suggested that the Federal Information Commissioner should be better resourced and given the power to make binding orders in accordance with the position in the provinces.[196] Provincial Information Commissioners' order-making power encourages parties to settle their disputes before orders are made. Whilst Canada's Federal Information Commissioner is unable to issue binding orders, it operates in a long-standing democratic system characterised by an entrenched culture of governmental openness and accountability, a feature not yet present in South Africa's young democracy.[197]

7.2.110 It was suggested that the way in which the local procedures should operate should take into account the problems experienced in the EU with regard to enforcement, ie it should be clear whether a particular contravention would amount to a criminal offence or not. It is suggested that a robust system be put in place to assist data subjects, with the regulatory authority having sufficient power to curtail non-compliance.[198]

7.2.111 In a submission to the Commission received form the Human Rights Commission[199] they argued that, on the basis of international experience and current public experience in South Africa, there is a need for a public statutory regulatory body. There are long established bodies in other jurisdictions, which further illustrate the need. The PAIA Unit of the Human Rights Commission shares the COSATU position on this issue. It is furthermore necessary, when looking into the

---

195 SAHA.

196 See Roberts A "New Strategies for Enforcement of the Access to Information Act" (2002) 27 ***Queens Law Journal*** 647-682.

197 SAHA.

198 Nedbank.

199 PAIA Unit South African Human Rights Commission "Comments on the DATA Protection Document" 1 June 2004.

enforcement mechanism of the right to privacy in terms of the proposed Privacy Act, that such a platform has the capacity capabilities to achieve the purpose of the proposed Act.

Structure of regulator

7.2.112 The question has been posed internationally[200] whether information privacy should be regulated by an individual, independent regulator rather than a commission-style regulatory agency.

7.2.113 The advantages of attaching regulatory powers to an individual are as follows-

* The development of a quicker and less bureaucratic system of regulation;
* Personal responsibility for regulation would reassure the public who could identify regulation with an individual protector of their interests rather than some vague commission of faceless persons.[201]

7.2.114 The disadvantages of an individual regulator, on the other hand, included the following -

* The possibility that significant political pressures may be directed at one person;
* A lack of accountability to a board or equivalent;
* The potential for unpredictable decision making;
* One person would be responsible for advising organisations and adjudicating

200 ***ALRC Discussion Paper*** at 1162.

201 ***ALRC Discussion Paper*** at 1162 reference to Baldwin R & Cave M Understanding Regulation: Theory, Strategy and Practice (1999) .

disputes involving the same organisation (its enforcement actions could therefore be seen to be tainted by its policy-making concerns and vice versa);

7.2.115 The advantages of a commission-like structure are the following -

* Helps reduce the danger that regulators will feel vulnerable and behave defensively;
* Creates the sense that decisions follow internal debate;
* Increases legitimacy and accountability; and
* Spreads the workload involved in regulating complex industries.

7.2.116 The disadvantages of a commission-like structure are the following -

* May lead to inconsistent decisions as decisions are made by a commission whose composition may change;
* Slower decision making;
* Possible loss of clarity of responsibility.

7.2.117 The importance of this distinction for the current discussion is that a decision has to be taken regarding the structure of the regulating authority for information protection in South Africa. POPIA sets out a commission-like structure to be referred to as an Information Protection Regulator. However, the option supported by the Review Committee is that a Commissioner in the South African Human Rights Commission should be identified as an Information Commissioner. See the discussion in this regard below.

Costs to responsible parties to comply with legislation

7.2.118 It was argued[202] that compliance with the requirements and administrative procedures of the draft Bill will cause an increase in the cost of conducting business across most

[202] Vodacom (Pty)Ltd.

of the sectors of the South African economy. The result of such increase is that it will result in increased costs in terms of prices charged by business to consumers. The increase in costs is likely to result from inter alia:

- the requirements of chapter 6 read with section 16 of the Discussion Paper Bill ie the notification requirements; and
- the requirements for the appointment of IPO's by responsible parties.
- stringent requirements on "responsible parties" which may require extensive software changes, that are both costly and take time to implement .[203]

7.2.119 The Commission was referred[204] to the report "Counting the Cost of Red Tape for Business in SA"[205] (the SBP report") where it is cited that the regulatory compliance costs (excluding administrative and efficiency costs) in South Africa for 2004 was equal to 6.25% of GDP. This is excessively high especially considering that it is also generally accepted that the cost of regulation is ultimately borne by the consumer and that poorer consumers tend to bear a heavier burden. The concern relating to regulatory costs was re-affirmed by President Thabo Mbeki in his State of the Nation Address on 3 February 2006 when he stated that the government will "introduce a regulatory impact assessment system to enable the government regularly to assess the impact of its policies on economic activity in our country." The Commission was, therefore, requested to keep the administrative (and the attendant financial) burden imposed in terms of the draft Bill to the bare minimum so as not to hamper normal business.[206]

---

203 Board of Health Care Funders; Momentum Health.

204 Ibid.

205 Strategic Partnerships for Business Growth in Africa ***Counting the Cost of Red Tape in South Africa*** June 2005.

206 According to the SBP report every regulatory impact assessment must answer inter alia the following critical questions:

- Is the regulatory problem correctly identified?
- Is government action justified?
- Is regulation the best form of government action?
- Is there a legal basis for regulation?
- What is the appropriate level or levels of government for this action?
- Do the benefits of regulation justify the costs?
- Is the distribution of effects across society transparent?
- Is the regulation clear, consistent, comprehensible and accessible to users?
- Have all the interested parties had the opportunity to present their views?
- How will compliance be achieved?

7.2.120 With regard to the anticipated costs of implementation of the requirements of an information protection statute, together with the costs of setting up and maintaining a regulatory authority, it is suggested that (rather than compromising on the broad principles and more formal requirements which would ensure consistent compliance and provide satisfactory protection to data subjects) a phase-in period be allowed for local businesses to convert existing data and databases and to implement processes and procedures in order to comply with the legislative requirements.[207] The Law Reform Commission was urged to ensure, in its proposals for legislation, that the costs for the protection of privacy are not onerous on service providers and operators. While the creation of a privacy culture in South Africa as well as the development of legislation to facilitate the development of that culture is wholly supported, one would wish to avoid a "double taxation" for members who have to absorb the costs of enabling surveillance and at the same time protect privacy.[208]

7.2.121 The Commission was also referred to a report[209] commissioned by the European Commission's Internal Market Director-General to evaluate the transposition of the Directive into national law and especially measuring the economic impact of the Directive on responsible parties(data controllers). Based on the case studies of fives sectors[210] in five EU member states,[211] the conclusion was that the costs of compliance with the national legislation implementing the Directive are relatively low for the sectors examined. This is especially true for small companies and institutions. The costs for multi-national companies and large public administrations are also minor relative to the size and turnover of these organisations.

Costs to data subjects to enforce their rights

---

207 Nedbank.

208 The Internet Service Providers' Association; The Department of Communications noted that it is currently in the process of drafting directives for the implementation of the RIC Act, in consultation with industry. This Act has some severe cost implications for the communications industry and currently cost-sharing models with the government have been precluded which will certainly have an impact downstream on smaller providers and consumers.

209 European Commission Final Report on the Economic Evaluation of the Data Protection Directive 95/46/EU (prepared by RAMBOLL management) May 2005.

210 Pharmacies, NGO's, customs authorities, IT service providers and retail.

211 France, Germany, Denmark, Italy and UK.

7.2.122 It was argued that it is important that the legislation contemplates an easy means for data subjects to report on contraventions, which would not involve huge costs. Even if greater awareness is achieved, the over complicated enforcement processes involved in the PAIA (requiring litigation over the most simple dispute) dilute the value of the legislation.[212]

7.2.123 Furthermore, the reliance on outdated court processes to ensure compliance with these protections undermines their benefits.[213] The need was stressed for a cheap, accessible, quick, effective and authoritative dispute-resolution mechanism. In particular, what is required is access to a mechanism available after the rejection of an internal appeal against denial of access to information, but before the commencement of court action.[214]

7.2.124 In April 2003, South African History Archives spent a week in Canada to examine that country's model. What impressed them was the extent to which, at federal level, the Commissioner's interventions had led to resolution and avoided expensive litigation. In its own work SAHA has taken six refusals to the High Court and each time an out of court settlement occurred. The settlements were facilitated by the State Attorney, who played a powerful mediating role. This is precisely what an Information Commissioner could do at a fraction of the cost. [215]

7.2.125 In this regard, an adequately resourced oversight body or person is important to ensure that individuals and companies can have recourse to the law without the need for an expensive process.[216]

Resources needed by regulatory authority

---

212 ISPA.

213 Internet Service Providers Association.

214 SAHA.

215 SAHA.

216 ISPA.

7.2.126 It is also important to recognise the need for additional resources to be committed to ensure effectiveness of any new independent review mechanism, for items such as staffing and training.[217] It is imperative that an oversight authority should have adequate funding (now and in the future) as well as the resources to adequately conduct oversight and enforcement.[218] Whether the entity is a single person, or has regional officers or offices, government has to be lobbied to ensure that this 'regulator' is adequately resourced to carry out its mandate.[219]

7.2.127 Two issues were raised-

a) It may be decided that Parliament should decide on and allocate "such sums of money as may be necessary" for the Commission to carry out its powers, duties and functions. It is unclear if the Commission will, in these circumstances, be a schedule 2 entity under the PFMA. It is argued[220] that the Commission ought to be funded and account for its spending, in the same way as any other public entity.

b) Secondly, given the wide range of powers given to the Commission under clause 39, there is a concern that the Commission should be adequately funded to enable it to operate effectively.[221] [222]

7.2.128 It was noted[223] that the Discussion Paper Bill provides for the appointment of Commissioners, committees and information protection officers. These appointments will undoubtedly have considerable financial implications, which would render the provisions of this Bill useless if not properly enforced. The Commission is also given extensive powers that will also have considerable financial implications. It was suggested that a detailed cost analysis be done and that sufficient monies be budgeted for the effective implementation of this Bill once enacted. The PAIA

217 SAHA.

218 EPIC and Privacy International ***Privacy and Human Rights*** 2002 at 13 and 14; MFSA.

219 The Internet Service Providers' Association.

220 SNO (Second National Operator) Telecommunications (Pty) Ltd.

221 Reports directly to Parliament, national public entity in terms of section 1 of PFMA (Public Finance Management Act 1999) Circular 71 of 2000.

222 SNO (Second National Operator) Telecommunications (Pty) Ltd.

223 Provincial Administration Western Cape.

was referred to as an example of practical problems being experienced due to financial constraints in effectively administering the Act.

Independence

7.2.129 It was stressed that any regulating agency must be independent, that is, able to criticise any privacy invasive proposals.[224] This also requires sufficient insulation and protection from other arms of government. It was even suggested that such a person or office be afforded Chapter 9 protection as envisaged by the Constitution.

7.2.130 It was, furthermore, noted that the independence of the body tasked with the protection of the right to privacy must be beyond question. By omitting a selection and recommendation procedure prior to the appointment of the Commission (which is appointed directly by the President) the impression may be created that the State has direct control over the members of the Commission and therefore controls the enforcement and application of the Privacy Bill. The State itself may be criticised as creating a Big Brother culture of accessing personal information at will.[225] In terms of clause 41(1) of the Discussion Paper Bill the Commission must submit programmes to the Minister for approval. This contradicts clause 40(1) which stipulates that the Commission is independent in the performance of Its functions. It was proposed that clause 41(1) be deleted.[226]

Alignment of regulators

7.2.131 Finally, this office should be coordinated and streamlined with other sector

---

224 Nedbank; EPIC and Privacy International ***Privacy and Human Rights*** 2002 at 13 and 14; MFSA.

225 SNO (National Operator)Telecommunications.

226 Department of Communications.

regulators to ensure effective regulation of the sector.[227]

7.2.132 The proposal was supported regarding the establishment of one regulatory authority to administer and enforce both PAIA and data protection and privacy legislation.[228]

7.2.133 Clause 69, furthermore, anticipates that the Commission may consult with other regulatory bodies. Since the Commission will be the body tasked with the protection of privacy, it was stated that it is not clear why another body might be involved. Such a provision may encourage forum-shopping. The Commission should enter into a memorandum of understanding with other regulatory agencies to ensure that their respective functions are carried out in a co-ordinated way.[229]

7.2.134 The Regulator's role should be:[230]

(i) to not only focus on private bodies' interaction with PAIA and POPIA, but also on public bodies, particularly proposed new regulators in terms of the National Credit Bill, Electronic Communication Bill, Auditing Profession Act, Co-operatives Act etc for whom access is a secondary issue and who are fully indemnified for bona fide actions (thereby making a concern about unintentional intrusions of less concern);

(ii) extended to include education and oversight of the proper implementation of the Protected Disclosures Act, Interception Act and perhaps even the Electronic Communications and Transactions Act in so far as it relates to access to information.

One regulatory authority for PAIA and POPIA

227 The Internet Service Providers' Association; SAFPS also supports the harmonisation of the Bill with the NCA and the Consumer Protection Bill.

228 Vodacom; See discussion below.

229 SNO Telecommunications.

230 Contemporary Gazette (Pieter Stassen).

7.2.135 As stated above, there have been increasing appeals in South Africa for the appointment of an Information Commissioner tasked with the regulation of PAIA. It has been reported[231] that about 50 percent of the requests for information from government departments in terms of PAIA never receive a response.

7.2.136 In 2006 the Supreme Court of Appeal[232] expressed its displeasure with the fact that there seemed to be a disregard of the aims of the Act. Combrink AJA stated as follows:[233]

> It is unfortunate that the Promotion of Access to Information Act 2 of 2000 ("the Act") which (as appears from the preamble)was intended to:
>
> * foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information;
> * actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all their rights,'
>
> should result in pre-trial litigation involving huge costs before the merits of the matter are aired in court. One of the objects of the legislation is to avoid litigation rather than propagate it. This is the fourth case in which information has been sought in terms of the Act that has in the past eighteen months required the attention of this court. I refer to Clutchco (Pty)Ltd v Davis 2005 (3) SA 486 (SCA), Unitas Hospital v Van Wyk 2006 (4) SA 436(SCA) and MEC for Roads and Public Works v Intertrade Two (Pty) Ltd 2006 (5) SA 1 (SCA). The present appeal illustrates how a disregard of the aims of the Act and the absence of common sense and reasonableness has resulted in this court having to deal with a matter which should never have required litigation.

7.2.137 The complex and potentially expensive appeals mechanism provided for in PAIA places further put obstacles in the way of an ordinary individual wishing to access information. The Act contains a long list of grounds for refusing a request. Once a request has been refused, an elaborate internal process must be followed, which requires that an individual provide legal reasons for the appeal. This is not an easy task for most lay persons. [234]

7.2.138 Should the internal appeals process be unsuccessful, an aggrieved individual can

---

231 ***Chapter 9 and Associated Institutions Report*** at 173.

232 ***Claase v Information Officer of South African Airways (Pty) Ltd*** 2007 (5) SA 469 (SCA).

233 Para [1].

234 ***Chapter 9 and Associated Institutions Report*** at 173.

only challenge decisions denying access to information in an ordinary court of law. The cost and complexity of such processes often make it difficult, if not impossible, for individuals or groups without adequate resources to exercise their right to information through the Act. It is significant that only a handful of cases reach the courts.[235]

7.2.139 Members of the public whose requests for information are denied would have to show extraordinary resilience if they were to lodge a successful appeal in the courts.[236]

7.2.140 In its submission to the Committee tasked with the review of the so-called Chapter 9 Institutions, the SA Human Rights Commission has, therefore, set out proposals to deal with the abovementioned problems. The proposals centre around the establishment of an independent information commissioner mandated to receive appeals from persons lodging requests for information and make binding orders on access and disclosure. From its report it seems as though the Review Committee accepts the need for an Information Commissioner. The Committee indicated that it believes that a dedicated information commissioner would go a long way towards ensuring effective implementation of PAIA.[237]

7.2.141 The submission of the SAHRC is in accordance with discussions held between the SAHRC and the SALRC on POPIA.[238] The draft Bill on POPIA published for comment recommends, amongst other things, the establishment of an independent Information Commission (Regulator) responsible for both PAIA and POPIA. Since both pieces of legislation is in need of a champion, it was thought to be an expedient solution. It should be noted that this system is working well in the United Kingdom, as well as in Germany, the federal states of Canada and Mexico, where the Information Commissioner administers both the Data Protection Act,1998 and the Freedom of Information Act, 2000.

---

235 ***Supra*** at 174.

236 ***Chapter 9 and Associated Institutions Report*** at 174.

237 Views regarding the exact location of the Commissioner is discussed below.

238 Meeting held on 7 November 2006 at the Offices of the SAHRC in Johannesburg.

7.2.142 The recommendation in the SALRC' Discussion Paper to set up one agency to deal with both the rights to access to information and privacy has, however, drawn conflicting responses.

7.2.143 The opinion was stated that there is an apparent contradiction in legislating two competing Acts, one of which protects the right to privacy and the other which promotes access to information and have both regulated by one Commissioner.[239]

7.2.144 It was, furthermore, argued that the combination of these roles under one agency would dilute the Commission's ability to ensure the smooth implementation of both laws. It could also place too much power in one official who could easily favour consolidating a culture of secrecy in carrying out his or her duties under the POPIA ahead of promoting disclosure and transparency.[240]

7.2.145 On the other hand, some commentators expressed support for the establishment of one regulatory authority to administer and enforce both PAIA and POPIA.[241]

7.2.146 It was argued that if separate agencies dealt with each right, a third authority or independent process would be required to ensure they were appropriately balanced when they, or actions of authorities responsible for them, conflicted. This would be impractical. Consideration of appropriate features of an authority responsible for privacy, therefore, requires consideration of existing regulatory arrangements regarding the right of access to information.[242]

7.2.147 It was noted that, in Canada, there are two commissioners at federal level – one for Freedom of Information and one for Privacy. This has lead to clashes between the two officials. It was, therefore, argued that it may be better to have one officer combine both roles in South Africa.

---

239 Board of Health Care Funders; Momentum Health.

240 Commonwealth Human Rights Initiative.

241 Vodacom (Pty)Ltd.

242 SAHA.

It would also be necessary to clarify the role of this officer in relation to the role of the Human Rights Commission which has statutory functions in terms of PAIA.[243]

7.2.148 It was argued that there seems to be no reason why an oversight body should not be given authority to investigate complaints in terms of both PAIA and any proposed information privacy legislation. It was submitted that such legislation is so closely related that a single referee would seem to be the most practical and financially sound method[244] of ensuring compliance. Two separate Commissions is an unnecessary duplication of administrative effort for the responsible parties, increased costs to the state and two Commissions could result in duplication of work or matters potentially falling through the cracks.[245] It is worth noting that since the enactment of PAIA there appears to have been virtually no compliance policing and an oversight body would be ideally suited to perform this task on receipt of complaints from consumers and members of the public.[246]

7.2.149 It was stated that, in light of the submission by the Commission to Parliament on the Information Commissioner's (IC) Office, and also in view of international developments of rationalising these two offices, the Bill has to recognise these developments and they be included.[247]

7.2.150 In its report to the Human Rights Commission on its role with respect to PAIA, SAHA argued that section 8 of the Human Rights Commission Act[248] dealing with dispute resolution does not allow the HRC to undertake dispute-resolution under PAIA, because PAIA establishes a legislative scheme to enforce the Act conferring specific power to resolve disputes on the Public Protector and very general and vague powers of this type on the Human Rights Commission. Given this, neither PAIA nor the Human Rights Commission Act should be interpreted to allow the Commission to "cut across" the dispute-resolution functions conferred on the Public Protector or to

243 National Archives.

244 Nedbank.

245 Nedbank.

246 SAFPS; Vodacom(Pty)Ltd.

247 SAHRC.

248 Human Rights Commission Act 54 of 1994.

go beyond the specific role assigned to it by PAIA. The Commission itself, however, takes the view that its role regarding constitutional rights allows it to resolve disputes under PAIA in light of PAIA implementing a constitutional right. The Commission's Legal Department does informally attempt to resolve disputes and its Complaints Committee of three Commissioners considers disputes which cannot be resolved informally. However, given uncertainty over the Commission's powers under PAIA, the following recommendations were made:[249]

* Removal of the current role of the Public Protector in dispute-resolution under PAIA;
* Insertion into both PAIA and privacy legislation of specific provisions conferring powers of dispute-resolution on either the Human Rights Commission or an independent Information and Privacy Commissioner.[250]

7.2.151 It was, futhermore, suggested that consideration be given to assigning particular commissioners to issue binding orders if the responsible authority also undertakes activities such as advising parties as to their legislative rights and facilitating handling of their complaints or applications at an earlier stage of the dispute-resolution process.[251]

7.2.152 In Canada, an independent report was commissioned by the federal Government[252] to assess the merits of combining the functions of the Information Commissioner and the Privacy Commissioner, either through a full merger of the commissioner's offices or the cross-appointment of a single commissioner to both positions.[253] It recommended that both offices should remain

---

249 SAHA.

250 SAHA also argued that the Human Rights Commission is currently inadequately resourced to perform this role, even before considering it's role regarding dispute-resolution. The need for adequate resourcing should therefore also be considered with respect to promotional and related functions under privacy legislation.

251 SAHA.

252 La Forest G V ***The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*** Report of the Special Advisor to the Minister of Justice 15 November 2005 (hereafter referred to as the "***Canadian Merger Report"***).

253 Canada has two separate agencies regulating access to information and privacy of information at federal level. At provincial level a number of states have a single regulator dealing with both aspects. During 1983 and 2002 the two offices at federal level shared corporate management personnel (ie finance, human resources, information technology, and general administration).

separate. [254]

7.2.153 It stated that the rights protected by both Acts are of the highest importance in the functioning of a modern democratic state. [255] The Privacy Commissioner is, furthermore, expected to perform seven interrelated roles: ombudsman, auditor, consultant, educator, policy adviser, negotiator and enforcer. Many of these roles are performed by the Information Commissioner as well. Each of these roles, and the increasingly strenuous demands they place on the offices of the two commissioners, must be considered in assessing the wisdom of any form of merger.[256]

7.2.154 Two sets of arguments were considered in order to come to a decision. The first relates to the potential of the merger to generate financial and administrative efficiencies. The second set of arguments involve the question of whether a single commissioner model would better serve the policy aims of the access to information and privacy statutes.

7.2.155 It was argued that, to the extent that efficiency is relied on (streamlined government and cost savings) as a justification for a merger, it will be critically important for such an analysis to be performed before any merger is pursued. On the evidence available it seems as though the savings of a combined office, as compared to the total combined expenditures of the two offices, would be modest. Viewed in relation to overall government expenditures, the costs associated with the two offices are, futhermore, minimal.[257]

7.2.156 Four types of policy argument were identified and considered: The first contends that a single commissioner would provide more consistent and balanced advice to government institutions dealing with both access and privacy issues; the second is that a single commissioner will have more success in persuading government to comply with their obligations under the access

254 It should be noted that two offices already existed at federal level in Canada, that it was a tenable model and that users had become familiar with the system. The basis of the report was therefore that the burden of persuasion lies with those advocating the adoption of a single commissioner model. This burden was not met.

255 ***Canadian Merger Report*** at 8.

256 ***Supra*** at 18.

257 ***Supra*** at 26.

and privacy statutes; the third argument asserts that a single commissioner would be predisposed to favour one principle at the expense of the other in cases where access and privacy comes into conflict; the fourth argument maintains that a single commissioner would be overburdened and hence have diminished capacity to pursue the goals of protecting privacy and encouraging openness in government.[258]

7.2.157 In conclusion the Report states that each of the one and two commissioner models has advantages and disadvantages. In the abstract neither is demonstrably superior to the other. However, the following conclusions may be drawn:[259]

a) There is little conflict between the mandates of the two commissioners.

b) It may be that a single commissioner would be able to develop a more productive relationship with government since it will be seen as more objective.

c) There is a real danger that a single commissioner would be overburdened and thus unable to respond as effectively to the increasingly demanding challenges posed to both the access and privacy regimes.

d) In the single-commissioner model, healthy public debate may give way to internal, bureaucratic discussion and compromise.

Where should a regulator be located?

7.2.158 The question as to where a statutory authority should be situated produced different views:

* Some commentators were in favour of a separate independent authority. They indicated that they did not support the view that the authority should reside within or be related to the existing SAHRC. [260]

---

258 ***Canadian Merger Report*** at 29.

259 ***Supra*** at 44.

260 Eg The Banking Council.

* Others felt that, rather than to create another regulatory authority, the regulation of information protection had to be placed in the hands of an existing authority, such as the South African Human Rights Commission (SAHRC).[261] [262]

* Situating the regulatory authority within the Public Protector was also suggested as a possibility.

Each of these suggestions will be discussed in turn.

Independent institution

7.2.159 In the Discussion Paper the Commission proposed that an independent body be instituted. Such a step would be in line with international precedent and ensure the integrity and independence of the body. It would ,furthermore, provide the Commission with a high profile which would assist in the protection of the personal information of persons. See the futher discussion above.

7.2.160 Although the SAHRC, in its submission to the Chapter 9 Review Committee, set out two options concerning the location of an information commissioner, their preferred stated position was in favour of the creation of an independent institution. They argued that an independent body would ensure that the staff and commissioner of this body would be appointed as specialists, who would deal solely with PAIA and POPIA.[263]

7.2.161 It should further be noted that the Privacy Commissioner in Australia was originally a member of the Human Rights and Equal Opportunity Commission (HREOC) before the Office

---

261 Society of Advocates, KwaZulu Natal; the Financial Services Board stated that a mere supervisory authority with mere overseeing and advisory functions is acceptable, as otherwise those functions would have to be left to relevant State departments where specialist knowledge and experience will obviously not always be present It would suffice if the Human Rights Commission is utilised for that purpose, with the Access to Information Act as a precedent (see section 10 and Part V of that Act); ENF for Nedbank suggested that the regulator should be situated within the Department of Communications.

262 See also the discussion on sector-specific regulators below.

263 ***Chapter 9 and Associated Institutions Report*** at 174.

of the Privacy Commissioner was established as a separate office in July 2000. It was suggested that a separate office was consistent with the approach taken in other countries and that it would provide an opportunity to further increase the profile, and thus effectiveness of the work of the Privacy Commissioner and of the Office of the Privacy Commissioner.[264]

South African Human Rights Commission

7.2.162 The second option set out by the SAHRC in it submission to the Review Committee, and the option which the Committee favoured, was to appoint an information commissioner within the Human Rights Commission.[265] In its report the Committee stated that it is opposed to the proliferation of human rights bodies, and this approach would ensure that the information commissioner works within an existing structure. To ensure the success of this intervention, the Committee proposes that the information commissioner should be allocated a "ring-fenced" budget within the budget allocation of the Human Rights Commission and dedicated staff.[266]

7.2.163 The Committee regarded the second option as the best solution since it entails the efficient and effective sharing of infrastructure and other resources. At the request of the Committee, the Commission costed the two options. The estimated cost for option 1 is approximately R7,6 million, while that for option 2 is approximately R5,6 million. The Committee recognises that accepting the second option of vesting an information commissioner within the Human Rights Commission is much cheaper and, therefore, cost effective.[267]

7.2.164 Section 184 of the Constitution requires the SAHRC to promote respect for human rights and a culture of human rights; to promote the protection, development and attainment of human rights; and to monitor and access the observance of human rights in South Africa. It should,

---

264 ***SALRC Discussion Paper*** at 1160.

265 The Human Rights Commission Act 54 of 1994 forms the basis of the Commission's work. This Act together with section 184 of the 1996 Constitution, the Promotion of Access to Information Act 2 of 2000, and the Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 provide the legal mandate of the Commission.

266 ***Chapter 9 and Associated Institutions Report*** at 175.

267 It should be noted that the estimated costs for both options seems to be very low and may be unrealistic.

however, be noted that information privacy is not solely human rights based. Data protection can also be defined as part of consumer protection based on market forces. The regulation of information privacy by the SAHRC is therefore not a perfect fit. Another point to be noted is that the SAHRC cannot make binding decisions on complaints lodged with it. Rights are protected through investigation, mediation, litigation and redress only.

Public Protector

7.2.165 The Public Protector is appointed by the President, on the recommendation of the National Assembly, in terms of Chapter 9 of the Constitution. The Office of the Public Protector was instituted through the Public Protector Act.[268] Section 181 of the Constitution ensures that the Public Protector shall be subject only to the Constitution and the law. He must be impartial and must exercise his or her powers and perform his or her functions without fear, favour or prejudice. No person or organ of state may interfere with the functioning of the Public Protector's Office.

7.2.166 The mandate of the Public Protector is to investigate matters and to protect the public against matters such as maladministration in connection with the affairs of government, improper conduct by a person performing a public function, improper acts with respect to public money, improper or unlawful enrichment of a person performing a public function and an act or omission by a person performing a public function resulting in improper prejudice to another person.

7.2.167 In terms of section 91 of PAIA the Public Protector has powers to mediate, conciliate or negotiate or advise where necessary, any complaint regarding appropriate remedies; or any other means that may be expedient in the circumstances. There is no absolute enforcement mechanism for non-compliance with the Act.

7.2.168 In comments received the Public Protector was, however, not deemed to be the appropriate body to perform the function of dispute-resolution under PAIA and privacy legislation

---

[268] Public Protector Act 23 of 1994. Date of commencement 25 November 1994.

for the following reasons:[269]

- Its role is limited to disputes over mal-administration, whilst what is required is a more effective mechanism to deal with disputes over enforcement of substantive rights under PAIA and privacy legislation.
- It deals solely with the public sector, whilst PAIA covers both the public and private sector as will privacy legislation. This in turn reflects the application of the rights of privacy and access to information to both the public and private sectors.
- It has no power to make binding orders.

The discussion regarding the location of the Regulator should be read and considered with the sections on the structure, independence scope and resources of a possible regulatory body.

Powers and duties

7.2.169 It was submitted that the powers set out in the Bill are very broad. It is, furthermore, unclear whether one is dealing with powers or duties.[270]

7.2.170 Enforcement of the provisions of the Act is not specifically addressed. It is proposed that in clause 39(1) of the Discussion Paper, the heading "monitor compliance" be amended to read, "monitor and enforce compliance" and the subclause be amended accordingly when necessary.[271]

Technical drafting points

7.2.171 The following technical points were made:

---

269 SAHA.

270 SNO(Second National Operator) Telecommunications (Pty) Ltd.

271 Department of Communications; Society of Advocates, Kwazulu Natal.

a) Clause 35(4) of the Discussion Paper Bill provides only for the resignation of the Commissioner (full time member). Provision should be made for others to resign.[272]

b) Provision should be made for the duties of the Commission relating to PAIA.[273]

c) Privacy call centres and special courts should be established in order for ordinary people to be given the opportunity to lodge complaints as is the case with equality and gender courts.[274]

d) It was suggested that the meaning of "information matching programme" in Clause 39 (1) (k) of the Discussion Paper Bill be clarified. [275]

(ii) Self-regulatory system

7.2.172 One submission was received in which self-regulation[276] as a way of privacy protection in the private sector was promoted. It was received from the United States Department of Commerce and set out the position regarding privacy protection in the United States as follows:[277]

* The importance of protecting the privacy of individuals' personal information is a priority for the federal government and consumers. The United States Government is focused on creating the best environment for growth through a deliberate and balanced approach to privacy that is open to innovations.

* Despite the benefits of information sharing, concerns about privacy are real and legitimate. Consumers repeatedly cite fears that their personal information will be misused as a reason for not doing business online. Therefore, moves to bolster on and off-line privacy and to protect consumer interests will fuel trust and the broader growth of cross-border trade, on-line communications, innovation, and business.

---

272 Department of Communications.

273 Sovereign Health.

274 Dr MDC Motlata.

275 SAIA.

276 Self-regulation implies sectoral legislation or codes of conduct only, and then only when and if necessary, without an oversight agency .

277 United States Department of Commerce.

* At this time, the U.S. does not have federal comprehensive legislation of mandatory "baseline" privacy requirements. Instead, the U.S. has adopted a flexible approach to privacy protection. The U.S. believes that self-regulatory initiatives (including company codes of conduct, "seal programs" and alternative dispute resolution mechanisms), coupled with a governmental enforcement backstop, are effective tools for achieving meaningful privacy protections.

* On the other hand, in certain highly sensitive areas, legislative solutions are appropriate. Congress has adopted legislation to protect certain highly sensitive personal information, including children's information, medical records and financial information. In addition, the Administration has moved forward with an agenda to further prevent identity theft, spamming and the unauthorized use of social security numbers.

* In order to achieve these ends, the U.S. Federal Trade Commission (FTC) has announced a major privacy enforcement initiative that increases resources dedicated to protecting consumers from the negative consequences of the misuse of consumer information, whatever the source. The FTC is committed to vigorously enforcing current laws that impact consumer privacy, including unwanted and fraudulent telemarketing sales, spam, Internet fraud, identity theft and The Children's Online Privacy Protection Act, to name just a few areas, in addition to enforcing commercial privacy policy promises.

* The U.S. believes that it is important to continue its dialogue with the business community and consumer groups to encourage broader adoption of privacy protections and adherence to self-regulatory privacy policies. Multilateral and private-sector initiatives have an important role to play in encouraging the development and use of privacy-enhancing technologies and in promoting consumer education and awareness about online privacy issues. The U.S. has continued its commitment to work with other countries, private sector groups such as the Global Business Dialogue on Electronic Commerce (GBDe) and the Trans-Atlantic Business Dialogue (TABD), multilateral organizations such as the Organization for Economic Cooperation and Development (OECD), and other stakeholders, such as

consumer groups, to promote internationally compatible approaches to privacy. [278]

* Reference was also made to the role of privacy sector initiatives. The following privacy resources and organizations were referred to:

  a) Codes of Conduct/Privacy Frameworks;[279]

  b) Privacy Policy Generator Tools;[280]

---

278 USA; ***OECD.*** Current OECD work on privacy and the protection of personal data builds on the 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. The October 1998 Ottawa Declaration on the Privacy of Global Networks reaffirmed the commitment of the OECD member countries to protect privacy on global networks and specifically recognized self-regulatory approaches. The OECD's current work program includes further encouraging the use of privacy-enhancing technologies and promoting user education and awareness about online privacy issues.

GBDe. The GBDe has also been active on the privacy front. The GBDe is in a unique position to facilitate discussion between consumers, industry and government. It is helping to lead the international effort to address consumer confidence on and off-line with the aim of making recommendations to governments. The GBDe has prepared draft personal data privacy protection guidelines which calls for companies to set company policies that respect and use the guidelines whether or not they are required by applicable law. The U.S. believes that the GBDe draft guidelines, and similar initiatives, are useful alternatives to the "one-size fits-all" legislative approach to data privacy protection.

APEC. APEC is in the process of developing the APEC Privacy Framework that will include both privacy principles and implementation mechanisms. The Framework will build upon the 1980 OECD Privacy Guidelines (referenced above) to create a system of privacy protection that is appropriate for the particular conditions in the APEC economies. The framework will focus on a cooperative approach that will balance and promote both effective privacy protection and the free flow of information in the Asia Pacific region.

279 Online Privacy Alliance (http://www.privacyalliance.org/)
The alliance has developed guidelines for creating an effective privacy policy, establishing enforcement mechanisms, and protecting children's privacy online. The alliance is comprised of more than 40 global corporations and associations.

Privacy Leadership Initiative (PLI) (http://understandingprivacy.org)
PLI has developed model practices for the exchange of personal information between business and consumers. Comprised of more than 20 companies and associations.

Network Advertising Initiative (http://www.networkadvertising.org/)
Created by leading online advertisers engaged in "online profiling". Sets forth self-regulatory principles for online advertisers to protect consumers' privacy while engaging in online advertising.

Global Business Dialogue on Electronic Commerce (GBDe) (http://www.gbde.org/gbde2003.html)
A worldwide, CEO-led, business initiative, established in January 1999 to assist in the creation of a policy framework for the development of a global online economy. Has developed personal Data Protection Guidelines for online merchants, trustmark providers, and any other businesses.

AICPA/CICA Privacy Framework
(http://www.aicpa.org/innovation/baas/ewp/2003_06_ed_execsumm.asp)
The Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accountants (AICPA) and the Assurance Services Development Board (ASDB) of the Canadian Institute of Chartered Accountants (CICA) have issued an exposure draft of a proposed Privacy Framework. The proposed Framework provides criteria and related material for protecting the privacy of personal information and can be used by certified public accountants (CPAs) in the United States and chartered accountants (CAs) in Canada, both in industry and in public practice, to guide and assist the organizations they serve in implementing privacy programs.

280 USA; **Organization for Economic Cooperation and Development (OECD)** (http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm)
Electronic commerce is a central element in the OECD's vision of the potential that our networked world holds for sustainable economic growth, more and better jobs, expanding world trade, and improved social conditions. The OECD's analysis has permitted a broad-based policy reflection on the establishment of the various elements that can provide a favorable environment for electronic commerce.

Direct Marketing Association (DMA) (http://www.the-dma.org/privacy/creating.shtml)
This tool has been developed to help marketers create policies that are consistent with The DMA's Privacy Principles for

c) Privacy “Seal” Programs/Verification Services;[281]

d) Alternative Dispute Resolution Providers;[282] and

Online Marketing.

281 TRUSTe (http://www.truste.org/)
TRUSTe is an independent, non-profit privacy organization whose mission is to build users' trust and confidence on the Internet and, in doing so, accelerate growth of the Internet industry. Through extensive consumer and Web site research and the support and guidance from many established companies and industry experts, TRUSTe has earned a reputation as the leader in promoting privacy policy disclosure, informed user consent, and consumer education. TRUSTe was founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium, who act as independent, unbiased trust entities. The TRUSTe privacy program-based on a branded online seal, the TRUSTe "trustmark"-bridges the gap between users' concerns over privacy and Web sites' desire for self-regulated information disclosure standards. Also serves as a verification system and dispute resolution provider for its seal-holders.
BBBOnLine (http://www.bbbonline.org/)
BBBOnLine is a wholly owned subsidiary of the Council of Better Business Bureaus. BBB*OnLine*'s mission is to promote trust and confidence on the Internet through the BBB*OnLine* Reliability and Privacy Seal Programs. BBB*OnLine*'s web site seal programs allow companies with web sites to display the seals once they have been evaluated and confirmed to meet the program requirements. The BBB*OnLine* Privacy Seal confirms a company stands behind its online privacy policy and has met the program requirements regarding the handling of personal information that is provided through its web site. Also serves as a dispute resolution provider for its seal-holders.
BBBOnLine is also developing the Global Trustmark Alliance (GTA). GTA will help expand the access of businesses online to the international marketplace by increasing consumer confidence around the world in cross-border Internet transactions. The Alliance, a partnership between non-profit business and consumer associations and governments around the world, will be especially helpful to small and medium sized businesses (SMEs) that particularly suffer from name recognition problems outside their local marketplaces.
Direct Marketing Association (The DMA) (http://www.the-dma.org
The Direct Marketing Association (The DMA) is the largest trade association for businesses interested in interactive and database marketing. Companies displaying The DMA Member logo have committed to the association's Privacy Promise. The DMA’s Privacy Promise is an assurance to consumers that U.S. marketers who are DMA members will use personal information in a manner that respects consumers’ wishes. Also serves as a dispute resolution provider for its seal-holders.
AICPA WebTrust (http://www.cpawebstrust.org)
The WebTrust program is a set of e-commerce standards comprised of prevailing best practices and requirements from around the world; an independent verification that a site meets the standards; and an internationally recognized web trust seal, announcing that an e-Commerce site meets the stringent standards. Also serves as a dispute resolution provider for its seal-holders.
SquareTrade (http://www.squaretrade.com/cnt/jsp/index.jsp)
SquareTrade's mission is to build trust in transactions and to create a better online trading experience. SquareTrade's services aim to help buyers identify trustworthy sellers they can buy from safely, as well as help good sellers show buyers that they can be trusted.
Entertainment Software Rating Board (ESRB) (http://www.esrb.org/privacy.asp)
ESRB Privacy Online addresses consumers’ concerns regarding privacy by requiring Web publishers to develop and implement meaningful and informative privacy policies and practices for their websites. ESRB protects the rights of Web consumers, and the interests of Web publishers, and help make the Internet a secure, reliable, and private place to share information and conduct business. Also serves as a verification system and dispute resolution provider for its seal-holders.

282 In addition to the “seal” programs listed above, the following organizations provide dispute resolution services for their members/clients:
American Arbitration Association (http://www.adr.org/index2.1.jsp)
The American Arbitration Association is available to resolve a wide range of disputes through mediation, arbitration, elections and other out-of-court settlement procedures. The American Arbitration Association assists in the design of ADR systems for corporations, unions, government agencies, law firms and the courts. The American Arbitration Association has played an instrumental role in establishing systems, which may utilize a variety of dispute resolution techniques, to address a full range of disputes involving, but not limited to, employment, consumer, technology, health care, bankruptcy, financial services, accounting, international trade and mass claims.
JAMS (http://www.jamsadr.com/home.asp)
JAMS provides the highest quality dispute resolution services to our clients and to our local, national and global communities. JAMS’ neutrals include the ADR industry's most respected mediators, arbitrators, private judges, facilitators, special masters (or referees) and neutral advisors.
Privacy Council (http://www.privacycouncil.com/)
Privacy Council consultants have worked for years with organizations in the United States and around the world on privacy-related issues. Their expertise ranges from helping organizations to develop privacy programs to ensuring that

e) Privacy Protection Training/Awareness.[283]

7.2.173 With respect to the possibility of legislative measures in South Africa to address privacy protection issues, caution was expressed against the unintended consequences of broadly prescriptive legislative measures. In this regard the possible costs resulting from implementing privacy legislation, which may be highly resource intensive for government and private sector, had to be noted.

7.2.174 It was suggested that, as important trade partners, South Africa and the United States should work together on approaches for addressing legitimate concerns about privacy protection and relevant trans-border issues. The initiatives used in the USA as set out above could serve as useful alternatives to "one-size-fits-all" legislative approaches to privacy protection. South Africa was encouraged to actively consider these efforts and the role that self-regulatory programs can play in bolstering privacy protection.

7.2.175 In concluding their comments it was stated that the challenge for the U.S. and its partners is to achieve internationally compatible standards for privacy protection while preventing the interruption of trans-border information flows, the life-blood of electronic commerce and cross-border trade and services.

7.2.176 Another respondent, however, raised a cautionary note [284] in indicating that the

---

their Web sites comply with privacy laws. Privacy Council is also in the process of enhancing its existing services to provide dispute resolution for its clients.

283 GetNetWise (http://www.getnetwise.org
ISP organization that educates parents on tools and measures to protect their children's privacy and security online.
Center for Democracy and Technology (http://www.cdt.org/privacy/) and the Privacy Leadership Initiative Created "privacy toolboxes" for online users, which are posted on their websites. These "toolboxes" typically tell users how they can limit disclosure of their personal information, what choices they have about how such information is used and shared, and under what circumstances they can access it
Econsumer.gov (http://econsumer.gov/)
Website provides means of consumer reporting in Internet privacy complaints and those relating to cross-border e-commerce transactions.
U.S. Federal Trade Commission (http://www.ftc.gov
Provides public information on privacy compliance initiatives and safeguards.

284 Andrew Rens.

absence of a contractual remedy in the South African law for damages to personality interests[285] undermines theories of market based or self regulation. While the market might generate an incentive to incorporate privacy policies in agreements there is no corresponding legal incentive to adhere to the policy. It could be argued that customers will eventually refuse to contract with an entity if it notoriously does not keep its promises, however ease of incorporation and corporate access to channels of communication undermines this. The status of privacy as a constitutional right also raises problems for a purely market based approach since the law on contracting around constitutional rights is not clear.[286]

(iii) Co-regulatory system

7.2.177 Respondents in favour of the co-regulatory system made it is clear that they see information protection legislation as the appropriate legal instrument in terms of which to control the collection, processing and security of personal information. However, while regulation should provide benefits for society in general, it should not place unnecessary and excessive burdens on industries. In particular, it should be ensured that the compliance and enforcement costs of regulation should not exceed the benefits. [287]

7.2.178 A framework should, therefore, make provision for regulatory and self-regulatory mechanisms that complement each other. Ensuring high quality and effective information processing and information security systems should be an area of self-regulation. Cognizance

---

285 According to two Appellate Division cases only patrimonial damages can be recovered on the strength of a breach of contract. In ***Administrator, Natal v Edouard*** 1990 (3) SA 581 (A) at 595-596 the court held that only patrimonial damages may be recovered for breach of contract. While the ratio decidendi in that case concerned a sui generis claim for pain and suffering, the principle was applied to 'sentimental damages' in ***Jansen Van Vuuren ao NNO v Kruger*** 1993(4) SA 842 (A), in which it was held that "only patrimonial damages can be recovered on the strength of a breach of contract". Infringement of personality is a circumstance that affects both the lawfulness of conduct and amount of an award. This produces the same problem that arose under the Aquilian action, that these types of damages are not appropriate for damage to personality. Damages for harm to personality interests have a rather different conceptual basis and while this is in itself problematic it fits breaches of privacy better than contractual damages does.

286 Andrew Rens.

287 Credit Bureau Association.

should, furthermore, be taken of a voluntary ombud which exist outside legislation but could be an important part of any framework.[288]

7.2.179 One respondent[289] indicated that sectoral laws which complement more comprehensive legislation may be the best option. The view was raised that the legislature should enact information protection laws specific to state owned entities while at the same time ensuring that general or sectoral privacy protection laws are such that each state owned entity is able to apply its own privacy regulatory policies in whichever industry the state owned entity falls without any constraints or conflicts. An organisation is best placed to understand the needs, demands and restrictions of its particular business and could thus be solely responsible for determining the manner in which it regulates privacy and information protection under the guidance and authorisation of some kind of regulatory body. Alternatively, the organisation could work closely with the body responsible for structuring its specific policy and code in the development of such policies and codes. Other entities, particularly state owned entities, in other industries could also work closely with such a regulatory body to ensure that the laws developed and enacted are practical.[290]

7.2.180 Another view was that the idea of a flexible approach is supported wherein industries would develop their own codes of practice, but that the concept of a regulatory overseer is not supported. A statutory regulatory agency should be established but this should be in the form of an ombudsman's office, who would have legislative powers to react to complaints of non compliance with the proposed legislation. Within the proposed legislation the Ombudsperson should be provided with powers to adjudicate, suspend, caution and in the event of serious non-compliance, even close down any organisation or concern that does not comply with the industry standard which would form part of a specific industry. [291]

---

288 Credit Bureau Association.

289 SABC.

290 SABC.

291 SAFPS. In addition to the above, SAFPS, in conclusion again re-iterates the need for inclusion in the legislation of a provision similar to section 29 of the UK Data Protection Act. It argues that a failure by the legislature to include such a provision will result in wholesale fraudulent activity by unscrupulous and criminal elements in society.

7.2.181 The following framework to deal with privacy and information protection was proposed:

* A general Privacy Act should constitute a generic framework to apply across different industries. The overriding legislation should not be too specific, in order not to be too restrictive in its impact. For that reason, the definitions in that Act should be wide and generic in nature, and should only contain the general principles. The generic nature would be important to assist different industries in complying with the proposed Act.[292]
* Compliance should be monitored by the different regulatory bodies overseeing the various industries, with codes of conduct made applicable within the various industries. It would be up to each industry to ensure compliance with general guidelines, but with particular rules operating within their own industry.[293]
* This would provide a real incentive for Industry to "own' their legal obligations and be educated about them. By being informed and pro-active, tangible business benefits and competitive advantage can be gained.[294]
* By ensuring that there is an enforcement agency with oversight obligations and registration procedures for industry Codes of Conduct that is governed by a supporting legislative framework enshrining Privacy Principles, industry-specific practices and policies can be codified and measured (via standards).[295]

7.2.182 This flexible and pragmatic approach by way of enforceable sectoral and regulatory approved codes of conduct will therefore balance and accommodate varying interests. It will also be the most pragmatic route to follow. [296]

---

292 LOA; In order to assist the Minister to draft appropriate regulations, it is proposed that a formal Advisory Council be appointed, with representation from different industries. Such representation should include long-term insurers as well as intermediary bodies. This process follows the general trend, which has emerged in recent years with legislation such as the Financial Intelligence Centre Act and the Financial Advisory and Intermediary Services Act. Representation should also include contact with bodies such as the International Security Forum, and other international bodies, who have conducted much research into data protection and privacy issues.

293 LOA.

294 Michalsons for IMS.

295 Michalsons for IMS.

296 Sanlam Life: Law Service.

7.2.183 An example supplied of an industry already subject to various codes was said to be that of the long-term insurance industry. All members of the Life Offices Association (LOA) are contractually bound to comply with the various codes of conduct of the LOA. A breach of any one of the codes of conduct can lead, in terms of the disciplinary provisions of the LOA, to the imposition of fines, suspension and termination of membership of the LOA. Peer pressure and market forces also compel insurers to comply with the codes.[297] Many of the principles espoused in the Issue Paper are already present in the LOA Code. [298]

(iv) Information Protection Officer

In favour of

7.2.184 It was submitted that the appointment (or designation) of current employees as IPO's by all responsible parties is supported. It would also facilitate the implementation of the suggestion regarding the registration process.[299]

---

297 Details of each of the LOA codes of conduct are available at www.loa.co.za . It is not intended to go into each of the codes in detail, but merely to provide two examples of the role the LOA plays with regard to privacy and data protection. The LOA Code on the Life Register provides in clause 1 as follows:

"The insurance risks which insurers are asked to cover, and the claims they are asked to pay, must be properly assessed. To do this insurers must be able to obtain information relevant to those risks and claims.

The Life Register is a data base through which insurers can share information about persons who propose for, or who are the lives assured under, policies and who have "notifiable impairments" that are relevant to the risk or claim assessment."

298 LOA; Annexure B to the Code on the Life Registry provides for access by the public to any data contained on the LOA Life Register relating to whether any data relating to that person exists on the Register and/or the nature of entries relating to that person. In terms of section 7.6 of the Code, "Should the accuracy of the information on the Registry be questioned by the person to whom the information relates, this issue is to be dealt with between that person and the life office concerned." The Code on the Life Register deals also with how a data subject may obtain information via his/her appointed medical doctor. Generally, the purpose of the information being stored is disclosed by the LOA and is freely available to the public. Regarding the accuracy of information, it is in the interests of long-term insurers to ensure that information maintained on a centralised LOA database is maintained and kept up to date. Some of these codes, such as the HIV Protocol are even more stringent with regard to the application of security regarding the data retained by life offices relating to the HIV status of individuals; LOA; "The purpose of the HIV Testing Protocol is to ensure that the life industry follows the highest standards in all aspects of HIV screening of applicants for life assurance…. It addresses issues such as identification, confidentiality, informed consent, pre- and post-test counselling, transmission of test results, accreditation of test kits and laboratories and the use of exclusion clauses."

299 Vodacom (Pty) Ltd.

7.2.185 The distinction between information officers in terms of POPIA and officers in terms of PAIA appears artificial. The protection of information should also form part of the duties of an information officer.[300]

Against

7.2.186 The mandatory appointment and registration of information protection officers are too burdensome or onerous, especially for private bodies. It was argued that the means of ensuring compliance must be left to the responsible party.[301]

Technical

7.2.187 It was stated that it was not clear what power the Commission has over parties that does not comply with the notification requirements of the Bill.[302]

7.2.188 Support was expressed for the notification procedures adopted in the Dutch Data Protection Act which stipulates that, where an organisation appoints its own privacy officer, notifications of processing can be given to the privacy officer and not to centralised data protection authority, especially where a data subject would prefer for data processing notification not to be given to a data protection authority. [303]

7.2.189 It was argued that it will be impractical for smaller responsible parties to comply with this requirement, without introducing a conflict of interest. It was recommended that some form of minimum threshold exemption be considered for inclusion in the Act. [304]

---

300 SAPS.

301 MTN(Pty) Ltd.

302 Department of Public Works.

303 Foschini's Group.

304 Banking Council.

7.2.190 The EU Directive and the Bill diverge on the question whether the Data Protection Official shall (or shall not) be independent from the data controller who has appointed him or her. [305] See discussion on in-house officials in para (v) at 330.

c) Recommendation

7.2.191 In evaluating the different systems discussed and the comments received , the following recommendations were made:

a) The Commission does not regard the self-regulatory system to be a suitable system for South Africa.[306] In evaluating the responses it was clear that this option received very little support. The Commission furthermore agrees with the argument that large areas of information processing go unregulated in such a system, causing a confusing patchwork of provisions that reveals large gaps resulting in information protection that becomes "fragmented, incomplete, and discontinuous".[307] Under these circumstances, individuals' rights are difficult and costly to pursue.[308]

b) Over time it has also become clear that the existence of a vigorous regulatory authority is a sine qua non of good privacy protection in as much as laws are not self-implementing and the culture of privacy cannot securely establish

---

305 Romain Perry; In that context, the French example of "Correspondant pour la protection des données personnelles" ("Data Protection Officer") might be relevant for the Committee, notably in relation to practical aspects.

In compliance with Article 18-2 of the EU Directive, article 22-III of the French Data Protection Act provides that "processing, for which the data controller has appointed a personal data protection officer charged with ensuring, in an independent manner, compliance with the obligations provided for under this Act, shall be exempted from the formalities provided for in Articles 23 (i.e. notification) and 24 (i.e. simplified notification), except where a transfer of personal data to a State that is not a Member State of the European Community is envisaged".

306 ***ALRC Discussion Paper*** at 1164 states that the regulatory authority should be structured and constituted in a manner that best helps it achieve its legislative purpose to promote and protect privacy in a country.

307 Reference by Bennett and Raab ***The Governance of Privacy*** to Gellman R "Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions" **Software Law Journal** 1993 Vol 6 199-231 at 238.

308 Bennett and Raab ***The Governance of Privacy*** at 105.

itself without an authoritative champion.[309]

c) A principles-based regime such as POPIA[310] should be administered through a compliance-orientated regulation framework.[311] The elements of compliance-orientated regulation are: (a) securing voluntary compliance with the regulatory objectives; (b) undertaking informed monitoring for non-compliance; and (c) engaging in enforcement actions where voluntary compliance fails.

d) The Information Protection Regulator should, furthermore, be enabled to act pro-actively to identify and resolve systemic issues before a breach occurs and enforce the Act in a manner which will not only provide specific deterrence to the responsible party involved, but general deterrence to other responsible parties.[312]

e) A statutory regulatory authority should, therefore:[313]

- **Administer both the access to information as well as privacy and information protection legislation;**
- **Be responsible for both promotion, publicity, education, advice, assistance, monitoring, and reporting to Parliament and for enforcement of rights and dispute-resolution;**
- **Be specifically empowered to resolve disputes under provisions of both PAIA and privacy legislation - this would involve amendments to PAIA;**
- **Be accessible as a dispute-resolution mechanism intermediate**

309 Bennett and Raab ***The Governance of Privacy*** at 107.

310 See discussion on the nature of principles-based legislation in Chapter 4 above.

311 ***ALRC Discussion Paper*** at 1145 and 1152 with reference to Parker C "Reinventing regulation within the Corporation: Compliance Oriented Regulatory Innovation (2002) 32 ***Administration and Society*** 529, 547. Compliance-orientated regulation takes an outcomes-based approach to regulatory design, in which strategies to foster, monitor and enforce compliance with the Act are chosen by reference to whether they will contribute to the outcome of compliance with regulatory goals.

312 ***ALRC Discussion Paper*** at 1149.

313 See SAHA submission. See consequential amendments in Annexure to the Bill.

between internal appeal against decisions of public or private bodies and recourse to the courts; and

- **Be empowered to make binding orders to resolve disputes.**

f) The interaction between the regulatory authority, industry specific regulators and self-regulating adjudicators should be established clearly. It should, however, be noted that many sectors (especially small to medium industries) do not necessarily have adjudicators or regulators. Provision will, therefore, still have to be made for those industries without sector-specific adjudicators through a general supervisory authority.[314] A sector-specific regulator, on the other hand, would also not be able to address problems in other sectors, once again leaving a gap that can only be filled by a supervisory authority.

g) The following steps in the dispute-resolution process under privacy legislation and PAIA should be voluntary, at the discretion of the applicant or complainant:

- **Internal appeals against decisions of public or private bodies (currently a compulsory step under PAIA); and**
- **dispute-resolution by the independent regulatory authority, intermediate between internal appeals against decisions of public or private bodies and recourse to litigation in the courts.**

h) In so far as the practical implementation of the abovementioned recommendations are concerned, it should be noted that the following options are available:

(i) Option 1: The Information Protection Regulator could be structured as an independent, separate entity; or

(ii) Option 2: The Information Protection Regulator could, as a matter of

314 Very few industries did in fact make use of the co-regulatory system in countries where it was available, reason being that the institution of an adjudicator was not found to be cost-effective and the fall-back system overseen by the regulatory authority seemed to be working well.

financial and administrative expediency, be placed within an existing entity such as :

*** the SAHRC; or**

*** the Public Protector.**

See the discussion in this regard above. Provision has been made in the draft Bill for an independent structure. However, should it be decided to follow option 2, it would be possible to use this same structure as a ring-fenced entity within either the SAHRC or the Public Protector.

i) A final question identified is whether information privacy should be regulated by an individual regulator or a commission-style regulatory agency. See the discussion above on the possible advantages and disadvantages of both structures.[315] Two options have been identified:

Option 1: A commission-like structure may be appointed, consisting of four part-time Regulators, chaired by one full-time Regulator.

Option 2: Two full-time Regulators (one for each Act to be administered) may be appointed, without any part time Regulators.

In both instances the Regulators will be supported by a Secretariat appointed in terms of the Public Service Act consisting of an administrative and a professional component. The Bill currently makes provision for option 1.

7.2.192 The Commission recommends that the information protection enforcement system provides for an independent, commission-like structure, chaired by one full-time Regulator to be referred to as the Information Protection Regulator. However, the provisions of the Act may be adjusted, if necessary, to accommodate any of the other options set out above.

---

315 See para 7.2.112.

CHAPTER 5

SUPERVISION

Part A
Information Protection Regulator

Establishment of Information Protection Regulator

35. There is hereby established a juristic person to be known as the Information Protection Regulator which -

(a) has jurisdiction throughout the Republic;

(b) is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice; and

(c) must perform its functions and exercise its powers in accordance with this Act and the Promotion of Access to Information Act 2 of 2000.

Constitution of Regulator and period of office of members

36.(1)(a) The Regulator consists of the following members -

(i) a Chairperson; and

(ii) four other persons as ordinary members of the Regulator;

(b) Members of the Regulator must be appropriately qualified, fit and proper persons for appointment on account of experience as a practising advocate or attorney or as a professor of law at any university, or on account of any other qualification relating to the objects of the Regulator;

(c) The Chairperson of the Regulator must perform his or her functions under this Act and the Promotion of Access to Information Act 2 of 2000 in a full-time capacity and must not be employed in any other capacity during the period in which he or she holds office as Chairperson;

(d) The other members of the Regulator must be appointed in a part-time capacity;

(e) The Chairperson must direct the work of the Regulator and the Secretariat; and

(f) No person will be qualified for appointment as a member of the Regulator if that person –

(i) is a member of a legislature;

(ii) is a councillor of a local authority;

(iii) is an unrehabilitated insolvent; or

(iv) has at any time been convicted of any offence involving dishonesty.

(2) Members of the Regulator referred to in section 36(1)(a) must be appointed by the President and must be persons -

(a) nominated by a committee after considering proposals made by interested parties in terms of subsection (4); and

(b) approved by the National Assembly by a resolution adopted by a majority of the total number of members of the House: Provided that if any nomination is not approved as required in paragraph (b), the joint committee must nominate another person.

(3) The President may appoint one or more additional members if he or she considers it necessary for the investigation of any particular matter or the performance of any duty by the Regulator.

(4) Before the members of the Regulator are appointed the Minister must invite interested parties through the media and by notice in the Gazette to propose candidates within 30 days of the publication of such notice, for consideration by the committee referred to in subsection (2)(a).

(5) The members of the Regulator will be appointed for a period of not more than five years and will, at the expiration of such period, be eligible for reappointment.

(6) A person appointed as a member of the Regulator may resign from office by writing under his or her hand addressed to the President and will in any case vacate office on attaining the age of seventy years.

(7) A member may be removed from office by the President on the request of Parliament only for inability to discharge the functions of the office (whether arising from infirmity of body or mind or any other cause) or for misbehaviour.

Remuneration, allowances, benefits and privileges of members

37.(1) A member of the Regulator who is not subject to the provisions of the Public Service Act, 1994 (Proclamation103 of 1994), will be entitled to such remuneration, allowances (including allowances for reimbursement of traveling and subsistence expenses incurred by him or her in the performance of his or her functions under this Act and the Promotion of Access to Information Act 2 of 2000), benefits and privileges as the Minister in consultation with the Minister of Finance may determine.

(2) The remuneration, allowances, benefits or privileges of different members of the Regulator may differ according to -

(a) the different offices held by them in the Regulator; or

(b) the different functions performed, whether in a part-time or full-time capacity, by them from time to time.

(3) In the application of subsections (1) and (2), the President or the Minister, as the case may be, may determine that any remuneration, allowance, benefit or privilege contemplated in those subsections, will be the remuneration, allowance, benefit or privilege determined from time to time by or under any law in respect of any person or category of persons.

Secretary and staff

38.(1) The Secretary of the Regulator and such other officers and employees as are required for the proper performance of the Regulator's functions, will be appointed in terms of the Public Service Act, 1994 (Proclamation 103 of 1994).

(2) The Regulator may, with the approval of the Minister in consultation with the Minister of Finance, on a temporary basis or for a particular matter which is being investigated by it, employ any person with special knowledge of any matter relating to the work of the Regulator, or obtain the co-operation of any body, to advise or assist the Regulator in the performance of its functions under this Act and the Promotion of Access to Information Act 2 of 2000 , and fix the remuneration, including reimbursement for travelling, subsistence and other expenses, of such person or body.

Committees of Regulator

39.(1) The Regulator may, if it considers it necessary for the proper performance of its functions -

(a) establish a working committee, which must consist of such members of the Regulator as the Regulator may designate;

(b) establish such other committees as it may deem necessary, and which must consist of -

(i) such members of the Regulator as the Regulator may designate; or

(ii) such members of the Regulator as the Regulator may designate and other persons appointed by the Minister for the period determined by the Minister.

(2) The Minister may at any time extend the period of an appointment referred to in subsection (1) (b) (ii) or, if in his or her opinion good reasons exist therefor, revoke any such appointment.

(3) The Regulator must designate the chairman and, if the Regulator deems it necessary, the vice-chairman of a committee established under subsection (1).

(4) (a) A committee referred to in subsection (1) must, subject to the directions of the Regulator, perform those functions of the Regulator assigned to it by the Regulator.

(b) Any function so performed by the working committee referred to in subsection (1) (a) will be deemed to have been performed by the Regulator.

(5) The Regulator may at any time dissolve any committee established by the Regulator.

(6) The provisions of sections 40 and 45(4) will with the necessary changes apply to a committee of the Regulator.

Meetings of Regulator

40.(1) Meetings of the Regulator must be held at the times and places determined by the chairperson of the Regulator.

(2) The majority of the members of the Regulator will constitute a quorum for a meeting.

(3) The Regulator may regulate the proceedings at meetings as it may think fit and must keep minutes of the proceedings.

Funds

41. Parliament will appropriate annually, for the use of the Regulator, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Regulator, of its powers, duties and functions under this Act and the Promotion of Access to Information Act 2 of 2000 .

(2) The financial year of the Regulator is the period from 1 April in any year to 31 March in the following year, except that the first financial year of the Regulator begins on the date that this Act comes into operation, and ends on 31 March next following that date.

(3) The Chairperson of the Regulator is the accounting authority of the Regulator for purposes of the Public Finance Management Act, 1999 (Act 1 of 1999) and will execute his or her dutiesin accordance with the Exchequer Act, 1975 (Act 66 of 1975).

(4) Within six months after the end of each financial year, the Regulator must prepare financial statements in accordance with established accounting practice, principles and procedures, comprising-

(a) a statement reflecting, with suitable and sufficient particulars, the income and expenditure of the Regulator during the preceding financial year; and

(b) a balance sheet showing the state of its assets, liabilities and financial position as at the end of that financial year.

(5) The Auditor General must audit the Regulator's financial records each year.

Protection of Regulator

42. The Regulator, and any person acting on behalf or under the direction of the Regulator is not civilly or criminally liable, for anything done, reported or said in good faith in the exercise or performance or purported exercise or performance of any power, duty or function of the Regulator in terms of this Act or the Promotion of Access to Information Act 2 of 2000.

Powers and duties of Regulator

43.(1) The powers and duties of the Regulator in terms of this Act are- --

education

(a) to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles;

(b) for the purpose of promoting the protection of personal information, to undertake educational programmes on the Regulator's own behalf or in co-operation with other persons or authorities acting on behalf of the Regulator;

(c) to make public statements in relation to any matter affecting the protection of the personal information of a data subject or of any class of data subjects;

monitor and enforce compliance

(d) to monitor and enforce compliance by public and private bodies of the provisions of this Act;

(e) to undertake research into, and to monitor developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of data subjects are minimised, and to report to the responsible Minister the results of such research and monitoring;

(f) to examine any proposed legislation (including subordinate legislation) or proposed policy of the Government that the Regulator considers may affect the protection of the personal information of data subjects, and to report to the responsible Minister the results of that examination;

(g) to report (with or without request) to Parliament from time to time on any matter affecting the protection of the personal information of a data subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the personal information of a data subject;

(h) on its own initiative or when requested to do so by a public or private body, to conduct an audit of personal information maintained by that body for the purpose of ascertaining whether or not the information is maintained according to the information protection principles;

(i) to monitor the use of unique identifiers of data subjects, and to report to Parliament from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the personal information of a data subject;

(j) to maintain, and to publish, make available and provide copies of such registers as

are prescribed in this Act;

(k) to examine any proposed legislation that makes provision for -

(i) the collection of personal information by any public or private body; or

(ii) the disclosure of personal information by one public or private body to any other public or private body, or both, to have particular regard, in the course of that examination, to the matters set out in section 44(3) of this Act, in any case where the Regulator considers that the information might be used for the purposes of an information matching programme, and to report to the responsible Minister and Parliament the results of that examination;

consultation

(l) to receive and invite representations from members of the public on any matter affecting the personal information of a data subject;

(m) to consult and co-operate with other persons and bodies concerned with the protection of personal information principles;

(n) to act as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the personal information of a data subject;

(o) to provide advice (with or without a request) to a Minister or a public or private body on their obligations under the provisions, and generally, on any matter relevant to the operation, of this Act;

complaints

(p) to receive and investigate complaints about alleged violations of the protection of personal information of data subjects and in respect thereof make reports to complainants;

(q) to gather such information as in the Regulator's opinion will assist the Regulator in discharging the duties and carrying out the Regulator's functions under this Act;

(r) to attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation;

(s) to serve any notices in terms of this Act and further promote the resolution of disputes in accordance with the prescripts of this Act;

research and reporting

(t) to report to Parliament from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a data subject;

(u) to report to Parliament on any other matter relating to protection of personal information that, in the Regulator's opinion, should be drawn to Parliament's attention;

codes of conduct

(v) to issue, from time to time, codes of conduct, amendment of codes and revocation of codes of conduct;

(w) to make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct;

(x) to review an adjudicator's decision under approved codes of conduct;

general

(y) to do anything incidental or conducive to the performance of any of the preceding functions;

(z) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Regulator by or under this Act or any other enactment;

(aa) to require the responsible party to disclose to any person affected by a compromise to the confidentiality or integrity of personal information, this fact in accordance with section 21 of this Act; and

(bb) to exercise the powers conferred upon the Commission by this Act in matters relating to the access of information as provided by the Promotion of Access to Information Act.

(2) The Regulator may, from time to time, in the public interest or in the legitimate interests of any person or body of persons, publish reports relating generally to the exercise of the Regulator's functions under this Act or to any case or cases investigated by the Regulator, whether or not the matters to be dealt with in any such report have been the subject of a report to the responsible Minister.

(3) The powers and duties of the Regulator in terms of the Promotion of Access to Information Act 2 of 2000 are set out in Part 5 of that Act.

Regulator to have regard to certain matters

44.(1) The Regulator is independent in the performance of its functions as set out in subsection 35 (b).

(2) In the performance of its functions, and the exercise of its powers, under this Act, the Regulator must -

(a) have due regard to the protection of personal information as set out in the information protection principles;

(b) have due regard for the protection of all human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the legitimate interest of government and business in achieving their objectives in an efficient way;

(c) take account of international obligations accepted by South Africa, including those concerning the international technology of communications; and

(d) consider any developing general international guidelines relevant to the better protection of individual privacy.

(3) In performing its functions in terms of section 43(1)(k) of this Act with regard to information matching programmes, the Regulator must have particular regard to the following matters -

(a) whether or not the objective of the programme relates to a matter of significant public importance;

(b) whether or not the use of the programme to achieve that objective will result in monetary savings that are both significant and quantifiable, or in other comparable benefits to society;

(c) whether or not the use of an alternative means of achieving that objective would give either of the results referred to in paragraph (b) of this section;

(d) whether or not the public interest in allowing the programme to proceed outweighs the public interest in adhering to the information protection principles that the programme would otherwise contravene; and

(e) whether or not the programme involves information matching on a scale that is excessive, having regard to -

(i) the number of responsible parties or operators that will be involved in the programme; and

(ii) the amount of detail about a data subject that will be matched under the programme.

Programmes of Regulator

45.(1) In order to achieve its objects in terms of this Act the Regulator must from time to time draw up programmes in which the various matters which in its opinion require consideration are included in order of preference, and must table such programmes in Parliament for information.

(2) The Regulator may include in any programme any suggestion relating to its objects received from any person or body.

(3) The Regulator may consult any person or body, whether by the submission of study documents prepared by the Regulator or in any other manner.

(4) The provisions of sections 2, 3, 4, 5 and 6 of the Commissions Act, 1947 (Act 8 of 1947), will apply with the necessary changes to the Regulator.

Reports of Regulator

46.(1) The Regulator must prepare a full report in regard to any matter investigated by it in terms of this Act and must submit such report to Parliament for information.

(2) The Regulator must within five (5) months of the end of a financial year of the Department for Justice and Constitutional Development submit to the Minister a report on all its activities in terms of this Act during that financial year.

(3) The report referred to in subsection (2) must be tabled in Parliament within fourteen days after it was submitted to the Minister, if Parliament is then in session, or, if Parliament is not then in session, within fourteen (14) days after the commencement of its next ensuing session.

Duty of confidentiality

47. A person acting on behalf or under the direction of the Regulator is required to treat as confidential the personal information which comes to his or her knowledge, except if the communication of such information is required by law or in the proper performance of his or her duties.

Part B

Information Protection Officer

Duties and responsibilities of Information protection officer

48.(1) An information protection officer's responsibilities include -

- *(a) the encouragement of compliance, by the body, with the information protection principles;*
- *(b) dealing with requests made to the body pursuant to this Act;*
- *(c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of this Act in relation to the body; and*
- *(d) otherwise ensuring compliance by the body with the provisions of this Act.*

(2) Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.

Designation and delegation of deputy information protection officers

49. Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act 2 of 2000, with the necessary changes, for -

(a) the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities set out in section 48(1) of this Act; and

(b) the delegation of any power or duty conferred or imposed on an information protection officer by this Act to a deputy information protection officer of that public or private body.

7.3 Notification, registration and licensing schemes

a) Proposals in the Discussion Paper[316]

316

CHAPTER 6
NOTIFICATION AND PRIOR INVESTIGATION

Part A
Notification

Processing to be notified to Commission

47. (1) The fully or partly automated processing of personal information intended to serve a single purpose or different related purposes, must be notified to the Commission before the processing is started.
(2) The non-automated processing of personal information intended to serve a single purpose or different related purposes, must be notified where this is subject to a prior investigation.

Notification to contain specific particulars

48. (1) The notification must contain the following particulars -

(a) the name and address of the responsible party;
(b) the purpose or purposes of the processing;
(c) a description of the categories of data subjects and of the information or categories of information relating thereto;
(d) the recipients or categories of recipients to whom the information may be supplied;
(e) planned cross-border transfers of information;
(f) a general description allowing a preliminary assessment of the suitability of the planned information security measures to be implemented by the responsible party, intended to safeguard the confidentiality, integrity and availability of the information which is to be processed.

(2) Changes in the name or address of the responsible party must be notified within one week and changes to the notification which concern (1)(b) to (f) must be notified in each case within one year of the previous notification, where they appear to be of more than incidental importance.

(3) Any processing which departs from that which has been notified in accordance with the provisions of (1)(b) to (f) must be recorded and kept for at least three years.

(4) More detailed rules can be issued by or under regulation concerning the procedure for submitting notifications.

Exemptions to notification requirements

49.(1) It may be laid down by regulation that certain categories of information processing which are unlikely to infringe the fundamental rights and freedoms of the data subject, are exempted from the notification requirement referred to in section 47.

(2). Where it is necessary in order to detect criminal offences in a particular case, it may be laid down by regulation that certain categories of processing by responsible parties who are vested with investigating powers by law, are exempt from notification.

(3) The notification requirement does not apply to public registers set up by law or to information supplied to an administrative body pursuant to a legal obligation.

Register of information processing

50.(1) The Information Protection Commission must maintain an up-to-date register of the information processing notified to it, which register must contain, as a minimum, the information provided in accordance with section 48(1)(a) to (f).

(2) The register may be consulted by any person free of charge.

(3) The responsible party must provide any person who so requests with the information referred to in section 48(l)(a) to (f) concerning information processing exempted from the notification requirement.

(4) The provisions of subsection (3) do not apply to -
(a) information processing which is covered by an exemption under Chapter 4.
(b) public registers set up by law.

Failure to notify

51. (1) If section 47(1) is contravened, the responsible party is guilty of an offence.
(2) Any person who fails to comply with the duty imposed by notification regulations made by virtue of section 96 is guilty of an offence.

Part B
Prior investigation

Processing subject to prior investigation

52. (1) The Commission must initiate an investigation prior to any processing for which responsible parties plan to-
(a) process a number identifying persons for a purpose other than the one for which the number is specifically intended with the aim of linking the information together with information processed by other responsible parties, unless the number is used for the cases defined in Chapter 4;
(b) process information on criminal behaviour or on unlawful or objectionable conduct for third parties;
(c) process information for the purposes of credit reporting; and
(d) transfer special personal information, as referred to in section 24, to third countries without adequate information protection laws.

(i) Choice of monitoring system

7.3.1 A primary condition for effective information protection is that of transparency.[317] Worldwide, responsible parties are enjoined to be open about their processing activities. [318] This obligation may include the requirement to inform (and to receive authorisation from) the supervisory authority of their processing activities.[319]

7.3.2 We have seen above that there are three main categories to the rules monitoring the activities of responsible parties.[320] In some countries mere notification is necessary before processing may start. Others require registration, and a third group insists on licensing as a pre-condition. A further requirement may be for the oversight authority to keep a register of the processing activities of which it has been informed.

---

(2) The provisions of subsection (1) may be rendered applicable to other types of information processing by law or regulation where such processing carries a particular risk for the individual rights and freedoms of the data subject.

Responsible party to notify Commission where processing is subject to prior investigation

53. (1) Information processing to which section 52 (1) is applicable must be notified as such by the responsible party to the Commission.

(2) The notification of such information processing requires responsible parties to suspend the processing they are planning to carry out until the Commission has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

(3) In the case of the notification of information processing to which section 52 (1) is applicable, the Commission must communicate its decision in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.

(4) In the event that the Commission decides to conduct a more detailed investigation, it must indicate the period of time within which it plans to conduct this investigation, which period must not exceed thirteen weeks.

(5) The more detailed investigation referred to under (4) leads to a statement concerning the lawfulness of the information processing.

(6) The statement by the Commission is deemed to be equivalent to an enforcement notice served in terms of section 83 of this Act.

317 See Principle 5: Openness as discussed in Chapter 4 above as well as the proposed clause 17(1) of the Discussion Paper Bill.

318 See in this regard Principle 6 of the OECD Guidelines set out in ftnt 315 in Chapter 4 above; See also Principle 3 of the UN Guidelines.

319 Bennett and Raab ***The Governance of Privacy*** at 99.

320 Para 7.2.22.

7.3.3 In terms of the notification requirement responsible parties simply notify information protection authorities of certain planned processing of personal information. Upon notification, processing is usually allowed to begin. Most information protection laws, including the EU Directive operate with this sort of requirement, though the ambit of their respective notification schemes varies.[321]

7.3.4 Occasionally, the notification requirement is, or has been, formalised as a system for registration. Under this system, responsible parties must, as a general rule, apply to be registered with the information protection authority as a necessary precondition for their processing of personal information. When applying for registration, a responsible party is to supply the authority with basic details of its intended processing operations.[322]

7.3.5 The final category requires that responsible parties must apply for, and receive, specific authorisation (in the form of a licence) from the relevant information protection authority prior to establishing a personal information register or engaging in a particular information-processing activity. Only a minority of countries operate, or have operated, with registered or comprehensive licensing schemes.[323]

7.3.6 The maintenance of national registers of responsible bodies is, furthermore, not a universal feature of information privacy laws, and there are many exemptions from such notification requirements where registers do exist. Over the years there has been an attempt to reduce the onerous burden placed on responsible parties by the obligation to notify or register their activities, whether through simplification or automation of the process, or through broadening the range of exemptions (eg in the UK and Germany).[324] In countries with new legislation, lighter notification responsibilities have been established from the start. Registration has never been seriously

---

321 Bygrave ***Data Protection*** at 75.

322 Bygrave ***Data Protection*** at 75.

323 Sections 4-9 of the UK Act of 1984 (repealed); Sweden's Data Act of 1973 (repealed); French Act (in relation to the public sector).

324 In the UK , a House of Commons select committee guessed in 1994 that about one third of controllers had failed to register. In Germany too, a system of central registration was considered "mere wishful thinking". In 1998 the system of registration in the UK under the 1984 Act was replaced by a scheme of notification; See also the problems experienced by the HRC in South Africa with the implementation of the disclosure provisions in terms of PAIA.

considered in information protection regimes in North America or Australasia.[325]

7.3.7 Compliance with notification everywhere also remains very low indeed.[326] One reason why notification is not more strongly pursued is that the information protection authorities in fact largely agree that the notified particulars are a very poor indication of what goes on in practice and that it adds little, if anything, to compliance with the more onerous requirements of the laws.

7.3.8 Many of the authorities would prefer to spend their resources on other measures which could contribute more effectively to compliance by responsible parties.[327] It was argued[328] that what matters for information protection is that the responsible parties respect the information protection rules when they process personal information and not that they send in papers to the oversight authority. The general perception worldwide is that bureaucracy should be contained[329] and that the supervisory authority should concentrate its activities both on giving advice and spreading awareness about information protection and supervising compliance. [330]

7.3.9 The Commission's preliminary proposal has been, therefore, that a light notification system which provides the oversight authority with enough statistical and other information to be able to comply with its educational and monitoring functions will be sufficient.

7.3.10 Notification appears to serve three main purposes:[331]

* It is helpful for data subjects because it is a major token of transparency in respect of the processing of personal information and can be the starting point for lodging a complaint with the competent authorities via the controls carried out in the Register

---

325 Bennett and Raab ***The Governance of Privacy*** at 99.

326 In the Netherlands there was found to be a discrepancy between the number of companies listed in the Companies Register and the number of responsible parties who notified their operations.

327 Korff ***Comparative Study*** at 170.

328 European Union Article 29 Working Party ***Report on the Obligation to Notify the National Supervisory Authorities on the Best Use of Exceptions and Simplification and the Role of the Data Protection Officers in the European Union*** WP 106 Adopted on 18 January 2005 (hereafter referred to as "***WP 106 on Notification***") at 18 referring to the position in Sweden.

329 Roos thesis at 354 referring to Jay and Hamilton Data Protection 135 states as follows:"By the 1990's the registration system came to be considered as 'burdensome, bureaucratic and unnecessarily detailed'".

330 See discussion below.

331 ***WP 106 on Notification*** at 6.

of processing operations (or of notifications);

* It is helpful for responsible parties as it assists in raising their awareness of notification duties and keeps them "tuned" to the need for complying with information protection requirements;
* It is helpful for information protection authorities because it allows them to keep abreast of the information processing situation in their countries (they can "feel the pulse") and, at the same time, enables several analyses to be carried out (statistical or otherwise) with a view to refining the approach to recommendation, audits and inspections.[332]

7.3.11 As to the latter point, it should be clarified that a distinction should be drawn between notification for prior checking purposes (as per Article 20 of the Directive) and notification submitted for processing that is not subjected to prior checking (as per Article 18 of the Directive).[333]

(ii) Processing operations which must be notified

7.3.12 The system of notification as set out in Articles 18-21 of Directive 95/46/EC reflects the different traditions in the EU member states at the time the Directive was negotiated in the early nineties.[334] [335]

7.3.13 The Directive requires, subject to several derogations, that responsible parties or their representatives notify the authority concerned of basic information about any wholly or partly automatic processing operations they intend to undertake (Article 18(1)).[336] Some countries extend

---

332 Register provides information for educational purposes.

333 See discussion below.

334 Whereas some relied heavily on notification and the keeping of registers, others sought to minimise these obligations or did have alternative systems in place.

335 ***WP 106 on Notification*** at 4.

336 Article 18 (1) of the EU Directive provides as follows:

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

the duty to notify processing operations also to all processing of information held in manual filing systems, some extend it to some manual systems, while others provide for wide exemptions.[337]

7.3.14 It should be noted that even where processing is not required to be notified to the authorities, such as most descriptions of manual processing, the responsible party is still under a duty to provide certain information to anyone making a written request. The purpose of this duty is to ensure transparency of processing even where formal notification is not required.

7.3.15 The general rule under the Data Protection Directive is that the duty of notification to the competent information protection authority is an obligation for all responsible parties. However, immediately after this general obligation, the Directive sets out extensive exemptions whose application is left to the discretion of the Member States. The idea is that some benign forms of automatic processing may be performed without the responsible party having an entry in the register.[338]

7.3.16 The legal framework for the exemptions to the duty of notification is mainly provided for in paragraphs 2 to 5 of Article 18 of the Directive.[339] There is no Member State where at least some

---

337 Korff ***Comparative Study*** at 168.

338 Bainbridge ***Data Protection*** at 69.

339 Art icle 18(2) -(5) of the EU Directive provides as follows:

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
* where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
* where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
    * for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
    * for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of 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 demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

partial exemptions from notification obligations have not been implemented.[340]

7.3.17 Besides these general exemptions, Article 9 of the Directive allows Member States to provide exceptions or derogations for the processing of personal information carried out solely for journalistic purposes or the purpose of artistic or literary expression. This might lead to an exemption to the duty of notification in these cases.[341]

7.3.18 The supervisory authorities, therefore, usually make an effort to exempt from the duty of notification, routine business activities and similar activities (unsuitable administrative formalities) to the extent permitted, with the proviso that the processing would not have any significant impact upon privacy. This has led to a broad catalogue of exemptions and considerable simplification.[342]

7.3.19 The Article 29 Working Party of the EU was requested to investigate possible means of providing further simplification to the duty of notification in the Member States. In its report[343] it confirmed the importance of having notification as a general requirement but identified best practices as regards the duty of notification to be followed.[344]

---

340 The exemption mechanism is useful in itself to allow data protection authorities to focus on really "dangerous" processing operations, i.e. those possibly jeopardising fundamental rights and freedoms.

341 ***WP 106 on Notification*** at 8; See, however, the discussion on exemptions in Chapter 4 above.

342 The Netherlands is a good example of the extensive reliance on certain categories of processing exemptions. As stipulated in article 43 of the Exemption Decree, some combinations of exempted processing operations are also exempted. In addition to that, the Data Protection Authority and the Ministry of Justice are currently reviewing the possibility to further extend the list of exemptions.

343 ***WP 106 on Notification***.

344 ***WP 106 on Notification*** at 4. In its recommendations at 22 the Art 29 Working Committee stated that:

* If amendments to the existing legal framework were envisaged, notification as a general requirement should not be eliminated.

* However, the Article 29 Working Party invites the Member States to make good use of the possibilities for exceptions and simplification available under the Directive and, where this is not yet the case, recommends Member States to empower the data protection authorities with appropriate regulatory powers to implement these exceptions accordingly.

* Notification should be regarded as a means to draw the responsible parties' attention to the need for abiding by data protection legislation. However, notification should not be just another bureaucratic step.

* States should enhance and pursue the userfriendly approach that is de facto adopted by Member States in dealing with notification requirements. This means enhancing the implementation of electronic and online notification mechanisms. Furthermore, the use of ready-made lists of purposes/data categories as already available in several Member States should be enhanced as this can reduce errors and harmonise notifications.

* Data Protection authorities within the Article 29 Working Party agree on the need to streamlining the exemption system.

7.3.20 As a general rule failure to notify is regarded as a criminal offence of strict liability.[345]

(iii) Notifiable particulars and publication of particulars

7.3.21 With some exceptions the types of information subject to the duty of notification must include at least the name and address of the responsible party and of his representative, if any; the purpose of the processing; a description of the category of data subject and of the information relating to them; the recipients to whom the information might be disclosed; proposed transfers of information to third countries; and a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing (Article 19).[346]

7.3.22 To the extent that they require notification, the States list (at least) all the matters mentioned in Article 19(1)(a) – (f) of the Directive, quoted above; and they all also stipulate that if such aspects of a processing operation change, the change too must be reported. However, they differ

---

345 Bainbridge ***Data Protection*** at 67 for UK example.

346 Article 19 of the EU Directive
Contents of notification
1. Member States shall specify the information to be given in the notification. It shall include at least:
(a) the name and address of the controller and of his representative, if any;
(b) the purpose or purposes of the processing;
(c) a description of the category or categories of data subject and of the data or categories of data relating to them;
(d) the recipients or categories of recipient to whom the data might be disclosed;
(e) proposed transfers of data to third countries;
(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph I must be notified to the supervisory authority.

Article 21of the EU Directive
Publicizing of processing operations
1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority. The register shall contain at least the information listed in Article 19 (1) (a) to (e). The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request. Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of 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 provide of a legitimate interest.

considerably in their specification of additional notifiable particulars. [347]

7.3.23 All the EU member states provide for the establishment of a publicly accessible register of processing operations, containing all the notified particulars, except for details of the security measures taken by responsible parties in accordance with the Directive. The content of these registers will vary because of the differences in the notifiable particulars.[348]

7.3.24 The register must be open for inspection to any person. Where the processing is not subject to notification, the responsible party or authority must make the relevant information available on request.[349] Whereas these registers used to be available at the Offices of the oversight authority, they are lately made available for inspection on the Internet at the oversight authority's web site.[350]

(iv) Prior checking

7.3.25 "Prior checks" or a requirement that responsible parties obtain the "prior authorisation" of their national information protection authority, is the strictest form of control over processing operations.

7.3.26 The EU Directive allows for a system of "prior checking" by national information protection authorities with respect to processing operations that are likely to present specific risks to the rights and freedoms of data subjects (Article 20(1)).[351]

---

347 Korff ***Comparative Study*** at 173.

348 Ibid.

349 Roos thesis at 725.

350 Bainbridge ***Data Protection*** at 74 for UK example.

351 Article 20(1) of the EU Directive provides as follows:

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

7.3.27 Elaborating on what might constitute such processing operations, recital 53 refers to operations that are likely to pose specific risks "by virtue of their nature, their scope or their purposes, such as excluding individuals from a right, benefit or contract, or by virtue of the specific use of new technologies".[352]

7.3.28 The system is most widely developed in France, where (under the current, pre-implementation law) all processing operations in the public sector must be based on a regulation, adopted after the information protection authority has first given its "advice" - which in practice comes close to a "prior check".

7.3.29 In the UK the term "assessable processing" is used. The Commissioner will consider the processing and give written notice to the responsible party stating whether and to what extent the processing is likely or unlikely to comply with the provisions of the Act.[353] However, no processing has, to date, been made subject to a "prior check" in the UK (even though the 1998 law does provide for the possibility).[354]

7.3.30 There are substantial differences between the EU member states regarding the kinds of operations for which they stipulate such prior formalities. Examples are the processing of sensitive information; processing for the purpose of credit referencing; and processing involving interconnections between different databases. It is also required for the processing by private-sector entities, staff recruitment agencies, processing for the keeping of legal information systems, or for the transfer of sensitive information to third countries without adequate protection.[355]

7.3.31 In the Netherlands, a "prior check" must be carried out for the use of an identification number for a different purpose than the one for which the number is intended, in order to match information with information processed by a different responsible party; for the recording of information obtained through a responsible party's own observations (which include both secret video surveillance and the capturing of Internet or intranet activities) if the data subject is not

---

352 ***WP 106 on Notification*** at 3.

353 Bainbridge ***Data Protection*** at 78.

354 Korff ***Comparative Study*** at 173.

355 Korff ***Comparative Study*** at 174.

informed of this; and for the processing of information on criminal-legal matters, other than by licenced detective agencies. [356]

7.3.32 It would appear from Article 28(3) of the Directive, together with recitals 9, 10 and 54 that information protection authorities may stop planned information-processing operations pursuant to this system of "prior checking".[357]

7.3.33 Recital 54 makes it clear, though, that such a system is to apply only to a minor proportion of information processing operations: with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited. In other words, information protection regimes in which prior checking is the rule rather than the exception do not conform with the Directive.[358]

7.3.34 In some sectors, the obtaining of prior opinions or prior checks, or prior authorisations or permits does become the norm, especially if (a) failure to obtain such a permit can lead to the loss of a licence and (b) the information protection authority puts in a concerted effort to convince those in the sector of the serious repercussions that failure to comply with the required formality may entail. It also helps if the sector in question is not too large. Purely because of resource implications, such a system must, however, by its nature, be limited to selected areas or kinds of responsible parties.[359]

(v) In-house officials

---

356 Ibid.

357 ***WP 106 on Notification*** at 3.

358 ***WP 106 on Notification*** at 4.

359 Korff ***Comparative Study*** at 175.

7.3.35 Article 18 (2) of the EU Directive[360] allows Members States to exempt responsible parties from notification duties where "the responsible party, in compliance with the national law which governs him or her, appoints a personal information protection official, responsible in particular for:

* Ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive;
* Keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2) (…)".[361]

7.3.36 The main task of the in-house official is to ensure compliance with the legislation and any other information protection-relevant legal provisions in all the personal information processing operations of his employer or principal. To this end, the responsible party must provide the official with an overview of its processing operations, which must include the information which (if it was not for the fact that the responsible party has appointed an in-house official) would have had to be notified to the authorities (as discussed below, under the heading notification) as well as a list of persons who are granted access to the various processing facilities. In practice, it is often the first task of the official to compile this information, and suggest appropriate amendments (eg, clearer definitions of the purpose(s) of specific operations, or stricter rules on who has access to which information). Once an official has been appointed, new planned automated processing operations must be reported to him or her before they are put into effect. The official's tasks also include verifying the computer programmes used in this respect and training the staff working with personal information. More generally, the official is to advise the responsible party on relevant operations, and to suggest changes where necessary. This is a delicate matter, especially if the legal requirements are open to different interpretations. The official may, "in cases of doubt" contact the relevant supervisory authority. However (except in the special context of a "prior check"), this is not

---

360 Article 18(2) of the EU Directive provides as follows:

2.Member States may exempt controllers from notification where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

* For ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive.
* For keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21(2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

361 This alternative to notification provided by the Directive is currently implemented in Germany, the Netherlands, Sweden, Luxembourg and France.

obligatory.[362]

7.3.37 The Dutch Data Protection Act stipulates that if there is a privacy officer, notifications can be done to the privacy officer (thus not to the data protection authority). The Dutch Data Protection Authority has developed a special notification programme for privacy officers. This adapted version of the notification programme offers the privacy officer the possibility to further process the notifications within a database or intranet within the organisation.[363]

b) Evaluation

Notification to be given once only

7.3.38 There was overwhelming agreement that the requirement of notice contained in clause 16(1) of the Discussion Paper Bill should make it clear that notice would only have to be given once, and not each time personal information is received or processed.[364] The administrative burden of complying with the Act every time information is collected would be unduly cumbersome.[365]

7.3.39 The Information Regulator should, therefore, have a list or data base of every single responsible party that processes information as contemplated for purposes of performing its enforcement functions in terms of chapter 8. The details set out in clause 48(1)(b)(f) of the Discussion Paper Bill should be provided as part of the general registration by the responsible party of its activities and not to register individual processing.[366]

7.3.40 It was recommended that processors be given a reasonable window period after the Act comes into effect, to notify the Information Protection Regulator without clause 51(1) of the

362 Korff ***Comparative Study*** at 176.

363 About 165 privacy officers are currently installed. The Dutch authority expects this number to increase further. They are active in all sectors of society. Examples are banks, insurance companies, trade unions, financial regulatory bodies, schools, hospitals, municipalities, ministries, and a variety of big and medium-size business.

364 Office of the Director-General, Department: Land Affairs; SAIA; Vodacom (Pty)Ltd; Cell C; SNO Telecommunications; Banking Association; Nedbank; MTN (Pty) Ltd.

365 ESKOM; Vodacom(Pty) Ltd.

366 Vodacom (Pty)Ltd.

Discussion Paper Bill being in force. The relevant authorities were also urged to carry out an education campaign, in an effort to avoid similar confusion to what was caused by the Promotion of Access to Information requirements to lodge manuals.[367]

Thresholds

7.3.41 It was requested that thresholds should be used to exclude smaller enterprises from the operation of the draft Bill. Only entities with more than 50 employees and a turnover of R25 million or more should be required to comply. It was also suggested that entities which employ less than 50 employees and have a turnover of less than R25 million should be exempt from complying with the administrative provisions in the draft Bill but that the other provisions in particular the information protection principles, be complied with and that the penalties would still apply to such entities.[368]

7.3.42 Commentators were pleased that clause 16 (5)(d) of the Discussion Paper Bill exempted them from notification of collection if this would prejudice the purpose of such collection. This would be particularly relevant in cases where insurers collect information in respect of fraudulent claims.[369]

7.3.43 It was proposed that, in instances where personal information is collected in terms of a legal or regulatory requirement,[370] it should not be necessary to notify the Regulator, as the processing of the information has already been sufficiently regulated. [371]

Costs

7.3.44 Agreement was indicated, in principle, with the proposals set out in the Discussion Paper

---

367 Nedbank.

368 Sovereign Health.

369 SAIA.

370 Clause 16(2)(d) of the Discussion Paper Bill.

371 Cell C.

Bill, but it was noted that their implementation could be both time consuming and costly.[372]

Registration done in terms of PAIA

7.3.45 Commentators referred to the fact that the Commission had, during workshops, mentioned that the notification provided for in the Bill would not be necessary if a responsible party was already registered under PAIA. Since the Discussion Paper Bill is silent on this issue, clarification was sought. It was contended that if this is indeed the intent of the legislature, it should be clearly stated in the Bill.[373]

7.3.46 The Discussion Paper Bill, furthermore, states that information may only be collected once the Commission has been notified and such notification has been noted in a register. The latter requirement may prove problematic in that there may be a delay between the actual notification by the responsible party and the noting in the register. [374]

Failure to notify

7.3.47 It was noted that clause 51 of the Discussion Paper Bill (failure to notify) makes it an offence to contravene clause 47 and any regulations on notification under clause 96. The implications of clause 47 are far-reaching and it was argued that it will be important, therefore, to curb and clarify the language and scope of the provision because of the consequences of a failure to comply.[375]

Prior investigation

7.3.48 It was contended that there should not be a general requirement in this regard but that the clause should only be triggered where the regulatory authority has reasonable grounds to suspect

---

372 SAFPS.

373 Board of Health Care Funders; Momentum Health; Sovereign Health.

374 Sovereign Health.

375 SNO Telecommunications.

or believe that the processing is being, or will be, conducted in contravention of the information principles set out in the draft Bill. This will be consistent with the exercising of the regulatory authority's general enforcement powers in terms of Chapter 8 as well as its powers and procedures for issuing information notices as stipulated in terms of clause 81(1) of the draft Bill.[376]

7.3.49 Clarification was sought as to whether a prior investigation would be necessary if the responsible party was already subject to a sector code. If not, such an exemption should specifically be provided for in the Bill.[377]

7.3.50 A proposal was received that the provisions of clause 53(6) of the Discussion Paper Bill should be amended to read as follows:[378]

> The statement by the Commission is deemed to be an enforcement notice served In terms of section 83 of this Act'-

7.3.51 The question was posed who will make the determination as to whether processing falls under clause 52(2) of the Discussion Paper Bill and hence clause 52(1) would accordingly apply.[379]

7.3.52 Section 53 of the Discussion Paper Bill requires responsible parties to "suspend the processing they are planning to carry out until the Commission has completed its investigation…". Certain time thresholds (e.g. 4 weeks, 13 weeks) are also specified within which the Commission must complete its duties. It was argued that it is unclear what the status in law will be where, for whatever reason, the Commission is unable to complete its statutory tasks in the specified times. It was, therefore, recommended that a presumption clause be included, to read as follows:[380]

> (7) any responsible party that has suspended its processing as required by subsection 2, and which has not received the Commission's decision within the specified time limits in subsections (3) and (4), may presume a decision in its favour and continue with its processing.

c) Recommendation

---

376 Vodacom (Pty)Ltd.

377 Sovereign Health.

378 Department of Communications.

379 SNO Telecommunications.

380 Banking Association.

7.3.53 After evaluating the comments, the Commission's recommendation is that a system of light notification (subject to exemptions) and prior investigation be implemented.

7.3.54 However, since the Information officer contemplated in Part B of Chapter 5 of the Bill is appointed by the responsible party and not by the Commission and is not subject to independence requirements, an exemption from notification requirements, as provided for in some jurisdictions, has been excluded.

7.3.55 It will be an offence to process personal information without notification unless the processing is exempt from notification, and liability will be strict.

7.3.56 As suggested by commentators, specific provision has been made in the Bill for the fact that notice will only have to be given once and not each time personal information is processed.

7.3.57 It is also recommended that prior investigations will not be necessary where a code of conduct has been issued and has come into effect in a specific sector.

7.3.58 No blanket exemption is provided in this Bill for smaller enterprises. However, any exemption granted to responsible parties from the provisions set out in sections 14 and 51 of PAIA will also apply as an exemption of the notification requirements set out in terms of POPIA. The Regulator, may, furthermore, by notice, exempt certain categories of information processing.

7.3.59 The proposed legislative enactment will read as follows:

CHAPTER 6

NOTIFICATION AND PRIOR INVESTIGATION

Part A

Notification

Notification of processing

50. (1) A responsible party must notify the Regulator before commencing the -

(a) fully or partly automated processing of personal information or categories of personal information intended to serve a single purpose or different related purposes; or

(b) non-automated processing of personal information intended to serve a single purpose or different related purposes, must be notified if this is subject to a prior investigation.

(2) The notification referred to in subsection (1) must be noted in a register kept by the Regulator for this purpose.

Notification to contain specific particulars

51.(1) The notification must contain the following particulars -

(a) the name and address of the responsible party;

(b) the purpose or purposes of the processing;

(c) a description of the categories of data subjects and of the information or categories of information relating thereto;

(d) the recipients or categories of recipients to whom the personal information may be supplied;

(e) planned transborder flows of personal information; and

(f) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

(2) Subject to subsection (3) a responsible party will only have to give notice once, and not each time personal information is received or processed.

(3) Changes in the name or address of the responsible party must be notified within one week and changes to the notification which concern subparagraphs (1)(b) to (f) must be notified in each case within one (1) year of the previous notification, if they appear to be of more than incidental importance.

(4) Any processing which departs from that which has been notified in accordance with the provisions of (1)(b) to (f) must be recorded and kept for at least three years.

(5) More detailed rules can be issued by or under regulation concerning the procedure for submitting notifications.

Exemptions to notification requirements

52.(1) The Regulator may by notice exempt certain categories of information processing which are unlikely to infringe the legitimate interests of the data subject from the notification requirement referred to in section 50.

(2) If processing of personal information is necessary in order to detect criminal offences in a particular case, it may be laid down by regulation that certain categories of processing by responsible parties who are vested with investigating powers by law, are exempt from notification.

(3) The notification requirement does not apply to public registers set up by law or to information supplied to a public body pursuant to a legal obligation.

(4) Any exemption granted to a responsible party from the provisions set out in sections 14 and 51 of the Promotion of Access to Information Act 2 of 2000 will also apply as an exemption of the notification requirements set out in terms of this Act.

Register of information processing

53.(1) The Information Protection Regulator must maintain an up-to-date register of the information processing notified to it, which register must contain, as a minimum, the information provided in accordance with section 51(1)(a) to (f).

(2) The register may be consulted by any person free of charge.

(3) The responsible party must provide any person who requests information referred to in section 50(l)(a) to (f) with the information so requested.

(4) The provisions of subsection (3) do not apply to -

(a) information processing which is covered by an exemption under Chapter 4; and

(b) public registers set up by law.

Failure to notify

54.(1) If section 50(1) is contravened, the responsible party is guilty of an offence and liable to a penalty as set out in section 99.

(2) Any responsible party who fails to comply with the duty imposed by notification regulations made by virtue of section 102 is guilty of an offence and liable to a penalty as set out in section 99.

Part B

Prior investigation

Processing subject to prior investigation

55.(1) The Regulator must initiate an investigation prior to any processing if a responsible party plans to -

(a) process a number identifying data subjects for a purpose other than the one for which the number is specifically intended with the aim of linking the information together with information processed by other responsible parties, unless the number is used for the cases defined in Chapter 4;[381]

(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(c) process information for the purposes of credit reporting; and

(d) transfer special personal information, as referred to in section 26, to foreign countries without adequate information protection laws.

(2) The provisions of subsection (1) may be applied by the Regulator to other types of information

381 Exemptions.

processing by law or regulation if such processing carries a particular risk for the legitimate interests of the data subject.

(3) Part B of Chapter 6 will not be applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 of this Act in a specific sector or sectors of society.

Responsible party to notify Regulator if processing is subject to prior investigation

56.(1) Information processing under a code of conduct as contemplated in section 55(3) must be notified as such by the responsible party to the Regulator.

(2) Responsible parties may not carry out information processing that has been notified to the Regulator in terms of subsection (1) until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

(3) In the case of the notification of information processing to which section 55(1) is applicable, the Regulator must inform the responsible party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.

(4) In the event that the Regulator decides to conduct a more detailed investigation, it must indicate the period of time within which it plans to conduct this investigation, which period must not exceed thirteen weeks.

(5) On conclusion of the more detailed investigation referred to in subsection (4) the Regulator must issue a statement concerning the lawfulness of the information processing.

(6) A statement by the Regulator in terms of subsection (5) is deemed to be an enforcement notice served in terms of section 90 of this Act.

(7) A responsible party that has suspended its processing as required by subsection 2, and which has not received the Regulator's decision within the specified time limits in subsections (3) and (4), may presume a decision in its favour and continue with its processing.

7.4 Codes of conduct

a) Proposals in the Discussion Paper[382]

382

CHAPTER 7
CODES OF CONDUCT

Issuing of codes of conduct

54. (1) The Commission may from time to time issue a code of conduct.
(2) A code of conduct must---
(a) incorporate all the information protection principles or set out obligations that, overall, are the equivalent of all the obligations set out in those principles; and
(b) prescribe how the information protection principles are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which these bodies are operating.

(3) A code of conduct may apply in relation to any one or more of the following -
(a) any specified information or class or classes of information;
(b) any specified body or class or classes of bodies;
(c) any specified activity or class or classes of activities;
(d) any specified industry, profession, or calling or class or classes of industries, professions, or callings.

(4) A code of conduct must also---
(a) impose, in relation to any body that is not a public body, controls in relation to the comparison (whether manually or by means of any electronic or other device) of personal information with other personal information for the purpose of producing or verifying information about an identifiable person;
(b) provide for the review of the code by the Commission;
(c) provide for the expiry of the code.

Proposal for issuing of code of conduct

55. (1) The Commission may issue a code of conduct under section 54 of this Act on the Commission's own initiative or on the application of any person.

(2) Without limiting subsection (1) of this section, but subject to subsection (3) of this section, any person may apply to t he Commission for the issuing of a code of conduct in the form submitted by the applicant.

(3) An application may be made pursuant to subsection (2) of this section only -
(a) by a body which is, in the opinion of the Commission, sufficiently representative of any class or classes of bodies, or of any industry, profession, or calling as defined in the code; and
(b) where the code of conduct sought by the applicant is intended to apply in respect of the class or classes of body, or the industry, profession, or calling, that the applicant represents, or any activity of any such class or classes of body or of any such industry, profession, or calling.

(4) Where an application is made to the Commission pursuant to subsection (2) of this section, or where the Commission intends to issue a code on its own initiative, the Commission must give public notice in the Gazette that the issuing of a code of conduct is being considered, which notice must contain a statement that -
(a) the details of the code of conduct being considered, including a draft of the proposed code, may be obtained from the Commission; and
(b) submissions on the proposed code may be made in writing to the Commission within such period as is specified in the notice.

(5) The Commission must not issue a code of conduct unless it has considered the submissions made to the Commission in terms of subsection (4) and is satisfied that all persons affected by the proposed code has had a reasonable opportunity to be heard.

(6) The decision as to whether an application for the issuing of a code has been successful must be made within a reasonable period of time which must not exceed fourteen weeks.

Notification, availability and commencement of code

56. (1) Where a code of conduct is issued under section 54 of this Act,---

(a) the Commission must ensure that there is published in the Gazette, as soon as reasonably practicable after the code is issued, a notice---

(i) indicating that the code has been issued; and

(ii) indicating where copies of the code are available for inspection free of charge and for purchase; and

(b) The Commission must ensure that so long as the code remains in force, copies of the code are available -

(i) for inspection by members of the public free of charge; and

(ii) for purchase by members of the public at a reasonable price.

(2) Every code of conduct issued under section 54 of this Act comes into force on the 28th day after the date of its notification in the Gazette or on such later day as may be specified in the code and is binding on every class or classes of body, industry, profession or calling referred to therein.

Amendment and revocation of codes

57. (1) The Commission may from time to time issue an amendment or revocation of a code of conduct issued under section 54 of this Act.

(2) The provisions of sections 54 to 58 of this Act must apply in respect of any amendment or revocation of a code of conduct.

Procedure for dealing with complaints

58. (1) The code may prescribe procedures for making and dealing with complaints alleging a breach of the code, but no such provision may limit or restrict any provision of Chapter 8 (Complaints and proceedings by the Commission) of this Act;

(2) If the code sets out procedures for making and dealing with complaints, the Commission must be satisfied that:

(a) the procedures meet the:

(i) prescribed standards; and

(ii) Commission's guidelines (if any) in relation to making and dealing with complaints; and

(b) the code provides for the appointment of an independent adjudicator to whom complaints may be made; and

(c) the code provides that, in performing his or her functions, and exercising his or her powers, under the code, an adjudicator for the code must have due regard to the matters that section 40(2) requires the Commission to have due regard to; and

(d) the code requires a report (in a form satisfactory to the Commission) to be prepared and submitted to the Commission within five months of the end of a financial year of the Department for Justice and Constitutional Development on the operation of the code during that financial year; and

(e) the code requires the report prepared for each year to include the number and nature of complaints made to an adjudicator under the code during the relevant financial year.

(3) A person who is aggrieved by a determination, including any finding, declaration, order or direction that is included in the determination, made by an adjudicator (other than the Commission) under an approved code of conduct after investigating a complaint may apply to the Commission for review of the determination.

(4) The adjudicator's determination continues to have effect unless and until the Commission makes a determination under Chapter 8 relating to the complaint.

Guidelines about codes of conduct

59. (1) The Commission may provide written guidelines -

(a) to assist bodies to develop codes of conduct or to apply approved codes of conduct; and

(b) relating to making and dealing with complaints under approved codes of conduct; and

(c) about matters the Commission may consider in deciding whether to approve a code of conduct or a variation of an approved code of conduct.

(2) Before providing guidelines for the purposes of paragraph (1)(b), the Commission must give everyone the Commission considers has a real and substantial interest in the matters covered by the proposed guidelines an opportunity to comment on them.

7.4.1 As noted above, codes of conduct are found in all the privacy systems discussed above.[383] Since the Commission has already indicated its preference for a regulatory system, the discussion in this section will, therefore, be restricted to codes of conduct as found within this system. Five kinds of privacy code can be identified[384] according to the scope of application: organisational code,[385] the

(3) The Commission may publish guidelines provided under subsection (1) in any way the Commission considers appropriate.

Register of approved codes of conduct

60. (1) The Commission must keep a register of approved codes of conduct.

(2) The Commission may decide the form of the register and how it is to be kept.

(3) The Commission must make the register available to the public in the way that the Commission determines.

(4) The Commission may charge reasonable fees for:
(a) making the register available to the public; or
(b) providing copies of, or extracts from, the register.

Review of operation of approved code of conduct

61. (1) The Commission may review the operation of an approved code of conduct.
(2) The Commission may do one or more of the following for the purposes of the review:
(a) consider the process under the code for making and dealing with complaints;
(b) inspect the records of an adjudicator for the code;
(c) consider the outcome of complaints dealt with under the code;
(d) interview an adjudicator for the code;
(e) appoint experts to review those provisions of the code that the Commission believes require expert evaluation.

(3) The review may inform a decision by the Commission under section 57 to revoke the approved code of conduct with immediate effect or at a future date to be determined by the Commission.

Effect of code

62. Where a code of conduct issued under section 54 of this Act is in force, failure to comply with the code, must, for the purposes of Chapter 8 of this Act, be deemed to be a breach of an information protection principle.

383 See para 7.2.1 - 7.2.34 (regulatory system), paras 7.2.35 - 7.2.65 (self-regulatory system) and para 7.2.66 -7.2.73 (co-regulatory system) as well as the evaluation of these systems in paras 7.2.78 and further. See also section 13 of the Irish Act; Parts VI-VII of the New Zealand Privacy Act, 1993; section 51(3) and (4) of the UK Data Protection Act, 1998; Part IIIAA of the Australian Privacy Act, 1988 and Article 25 of the Dutch Personal Data Protection Act.

384 Raab presentation 2002 at 9-11. See also Bennett and Raab ***The Governance of Privacy*** at 123-126.

385 This applies to one agency that is bound by a clear organisational structure.

sectoral code,[386] the functional code,[387] the professional code,[388] and the technological code.[389]

7.4.2 The EU Directive clearly provides for the use of codes of conduct. [390]To contribute to the proper implementation of the Directive at the national level, Article 27 of the Directive[391] directs the EU member states and the EU Commission to encourage the development of codes of conduct. EU member states are required to facilitate the approval procedure of draft codes and amendments or extensions to existing codes prepared by trade associations and other bodies. Organisations representing certain industry sectors, and established in multiple Member States, may futhermore submit draft Community codes, and amendments or extensions to existing Community codes, to the Article 29 Working Party to determine whether the drafts comply with the Directive. [392]

7.4.3 The OECD Guidelines, furthermore, provide that member countries should encourage and support self-regulation, whether in the form of codes of conduct, or otherwise.[393]

7.4.4 Codes of conduct are, therefore, seen as a useful means to clarify the application of

386 The defining feature of a sectoral code is that there is a broad consonance of economic interest and function and a similarity in the kinds of personal information collected. Examples are the banking industry, life insurance etc.

387 This code is defined less by the economic sector and more by the practice in which the organisation is engaged, for example direct mail and marketing. The Direct Marketing Association in South Africa, for instance, represents businesses in a wide number of sectors.

388 Codes developed for those directly involved in information processing activities eg market researchers, and health professionals.

389 As new potentially intrusive technologies have entered society, codes have developed to deal with their specific application.

390 The Directive does not, however, provide any indication of the exact legal status to be provided to such codes.

391 Article 27 of the EU Directive:

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.
3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

392 Wugmeister et al ***Codes of Conduct***".

393 Paragraph 19(b) OECD Guidelines. Paragraph 19(b) is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action.

information protection law in a particular sector, and can also be used as an alternative to sectoral regulation.[394] In theory, the drafting of codes should be a simpler, more flexible means to achieve the same end, the laying down of sector-specific rules applying the more general information protection rules.[395] It, furthermore, has the advantage that, once negotiated, the codes can be adapted to changing economic and technological developments.[396]

7.4.5 A substantial portion of a code of conduct should therefore deal explicitly with the information privacy principles, covering how compliance with each principle is to be secured. Some of the principles will bear more heavily on some sectors than others and will require more detailed consideration.[397]

7.4.6 Codes will typically be promoted or initiated by trade associations, representative or professional bodies or Government departments, and will cover the application of the information privacy principles to particular groups of "agencies" (eg health sector, law enforcement agencies, direct marketing companies etc) or for particular types of information (eg. employment information and credit information). The Information Regulator may also initiate codes of practice.[398]

7.4.7 While it is preferable for codes to emanate from the representative associations themselves, the Regulator will be free to initiate codes of conduct wherever it is considered that the best interests of data subjects so require. Naturally, any actions in this area will have to be on the basis of full consultation with all interests affected, including both representative bodies and the public, more generally.[399]

7.4.8 The Regulator may, however, prefer to rely on the issuing of its own sectoral rules (rather than on leaving the initiative, at least initially, to the sectors concerned). In several countries some specific

---

394 See sections 15 and 16 of the Financial Advisory and Intermediary Services Act 37 of 2002 for an example of the successful use of codes of conduct to regulate different sectors of the financial services industry.

395 Korff ***Comparative Study*** at 196.

396 Bennett and Raab ***The Governance of Privacy*** at 113.

397 Office of the Privacy Commissioner of New Zealand ***Draft Guidance Note on Codes of Practice under Part VI of the Privacy Act*** Issue No. 5 dated 5 December 1994 (hereafter referred to as "NZ ***Codes of Practice Guidance note***") at 3.

398 NZ ***Codes of Practice Guidance note*** at 2.

399 Korff ***Comparative Study*** at 197 with reference to the Irish Commissioner in his 2001 Annual Report.

sectors are already regulated in some detail in the law or in regulations issued under the law (e.g., the direct marketing- and credit reference sectors) - but elsewhere (eg in the UK) the possibility of issuing State-imposed sectoral rules is regarded more as a "stick behind the door", to be used only if a sector does not itself put forward adequate rules.[400]

7.4.9 In practice, self-regulation and State-imposed sectoral regulation are not as different as one might expect: self-regulation increasingly takes place in a legal framework which allows for, or indeed requires, the assessment or approval of "voluntary" codes, while State regulation may involve the drawing up of rules in consultation with (or even by) sectoral organisations.[401]

7.4.10 The development and adoption of a code by an organisation could be used to send a powerful message to consumers that the organisation is conscious of the privacy concerns of individuals and is active in protecting their privacy rights.[402] They also allow organisations to remove suspicions about the improper collection, processing and dissemination of personal information that may exist and thereby facilitate an "enhanced measure of understanding on both sides".[403]

7.4.11 As discussed above, there are three different models that have evolved in those countries that use privacy codes:

a) The first, and in many ways most stringent, is represented by the system under the New Zealand Privacy Act. The crucial aspect of the New Zealand approach is that codes of practice negotiated under the Privacy Act have the force of law. A breach of a ratified code of practice is as serious as a breach of the information privacy principles expressed in the law, which would then trigger the complaints and enforcement

---

400 Ibid.

401 Korff ***Comparative Study*** at 196.

402 Malcolm Crompton, Federal Privacy Commissioner of Australia in his forward to the ***Guidelines on Privacy Code Development*** published by the Office of the Federal Privacy Commissioner September 2001. See also the reference to other reasons for developing a code set out at 18 of the same document:. A code may -

* be a good way of changing the culture of an organisation or industry by raising awareness of privacy and by introducing a compliance regime;
* serve as a guide to regulation by providing industry standards written in industry specific language. It is often quicker and easier to amend codes than it is to amend the law, allowing organisations to keep up with developments and respond to concerns.

403 Bennett and Raab ***The Governance of Privacy*** at 113 referring to Hustinx P "The Use and Impact of Codes of Conduct in the Netherlands" Paper presented to the 16th Conference of Data Protection Commissioners, The Hague, 1994.

procedures in the legislation.

b) The second, slightly more flexible regime, exists in the Netherlands. Although the Dutch system is similar in most respects to that in New Zealand, the codes are not formally binding on the courts. If an organisation can prove that it has met the requirements of its code, it will have a strong case. Conversely, a complainant's demonstration that the provisions of the code have been breached constitutes prima facie evidence of liability under the law. Codes therefore, have indirect, rather than direct legal effect.[404]

c) In other countries, such as the UK and Canada, the law simply empowers the Commissioner concerned to encourage the development of codes as a further instrument of compliance with the law. Indeed, this is all that is expected by the EU Directive.[405]

7.4.12 In Europe the stipulations in the Directive confirm a trend towards what one may call quasi-self-regulation (whereby it may be noted that the paragraph concerning Community Codes clearly envisages the "approval" of such codes, while the paragraphs concerning national codes refer more vaguely to the obtaining of an "opinion"). The laws in all the EU Member States now include provisions on the drafting of self-regulatory codes of conduct. In most, the laws refer to the "checking" or "assessing" of the compatability of the code with the law; to the issuing of an "opinion" on that conformity; or to the drawing up of codes "in cooperation" with the information protection authority.[406]

7.4.13 A certain tension has been noted in the EU between the views taken of codes by industry and regulators. The former sometimes feel that the latter are too rigorous in their initial assessments of draft codes submitted for an "opinion", while the latter sometimes feel that the former are trying to use codes as a means to evade certain strict rules in the law. The process for obtaining an "opinion" or assessment is consequently often long (as is also the case, it may be noted, with regard to the

404 To date, the Dutch Data Protection Authority ("DPA") has approved fifteen codes of conduct, mainly in the financial services, pharmaceutical and direct marketing services sector that can be used to satisfy national requirements for the processing of personal data. These codes are used to promote compliance with sector specific data protection requirements.

405 Bennett and Raab ***The Governance of Privacy*** at 113.

406 Ibid.

approval of Community Codes).[407]

7.4.14 It has been argued that where a formal ratification process is laid out, as in New Zealand and the Netherlands, this can bureacratise a process that, in theory, is supposed to allow the flexibility of self-regulation. Another problem encountered is that the submission of the codes in some sectors may be hindered by competition within the sector, and by unclear boundaries and overlaps that weaken the claim that the association submitting the code is sufficiently "representative".[408]

7.4.15 The following guidance have been given on the matters that should be addressed in particular in acceptable codes of conduct:[409]

* What type of personal information is covered;
* For what purpose is this information processed;
* How is the personal information obtained;
* How can the personal information be processed;
* To whom will the personal information be disclosed; and
* For how long will the personal information be retained.

7.4.16 A code of conduct will furthermore include provisions for:[410]

* Commencement, review and expiry of the code;
* A precise definition of the scope or application of the code;
* A complaints procedure and how individuals can exercise any rights flowing from the code. Depending on the nature of the particular sector, this may range from an independent complaints mechanism to an obligation for the privacy officer of a body to reconsider any complaint received or a senior person independent of the person whose decision is complained about.

---

407 Ibid. Note that some codes modify the application of the Information Privacy Principles (prescribing more stringent or less stringent standards or by exempting actions). This is the position in New Zealand. In Australia the law stipulates that the codes should be at least the equivalent of the privacy principles as stated in the Act. The current proposal for South Africa is that the codes should be the exact equivalent of the privacy principles.

408 Bennett and Raab ***The Governance of Privacy*** at 113.

409 Korff ***Comparative Study*** at 198.

410 NZ ***Codes of Practice Guidance Note*** at 4.

7.4.17 Particular procedures for the adoption of codes of conduct may differ in various countries, as do the status for such codes. However, it might be advisable to stress that the process for adopting draft codes should not be too cumbersome (whereby it could be added that the operation of a code in practice can be, and should be, kept under review).[411]

7.4.18 Organisations need to be aware, however, that to develop and implement a privacy code requires a commitment of resources. Costs will vary from scheme to scheme, with the establishment of a complaints handling body adding substantially to the resource requirements.[412]

7.4.19 An exciting new development to be noted[413] is that a code of conduct approach is developing to cross-border information transfers.[414] More and more companies are pushing for the development of global codes that would govern their global information processing practices and at the same time facilitate all their international information transfers. Given the growing number of cross-border information transfers, the idea of relying on global rules for all cross-border information transfers is attractive. [415]

7.4.20 The EU has published a Working Document[416] which provides Guidelines for determining whether a self-regulatory instrument can be considered as a valid ingredient of "adequate protection":

a) It should include the basic content of information protection principles;

b) It should contain certain mechanisms for effectively ensuring -

   (i) a good level of general compliance;

   (ii) support and help to individual data subjects; and

   (iii) appropriate redress.

b) Evaluation

411 Korff ***Comparative Study*** at 198.

412 Office of the Federal Privacy Commissioner Australia ***Guidelines on Privacy Code Development*** September 2001 (hereafter referred to as " Australian ***Privacy Code Guidelines***") at 20.

413 Especially in so far as South Africa's trade with the rest of Africa is concerned.

414 Wugmeister ***Codes of Conduct*** et al at 1; See discussion in Chapter 6 in this regard.

415 See further discussion on cross-border data transfers in Chapter 6 above.

416 ***WP 12*** at 11.

General

7.4.21 Most commentators were in favour of the implementation of codes of conduct.[417] It was argued that the approach should be flexible in that industries should develop their own codes of good practice as guidelines to develop industry standards which will form part of that specific industry (sector) codes.[418]

7.4.22 It was held that the proposed development of codes of conduct would help substantially in making all segments of our society aware of the principles of data privacy and enable them to implement them as necessary.[419]

7.4.23 Some pre-requisites were, however, put forward for consideration. Such codes must -

a) not be used to impose obligations on stakeholders, but merely constitute best practice guidelines; and

b) be based on wholehearted buy-in from all affected stakeholders. [420]

7.4.24 It was contended that a code of conduct for banks is vital in order to clarify the requirements of all banks in as far as their compliance with this legislation is concerned. This will assist consumers and assist the banks with implementing uniform data protection requirements and policies in line with the legislation. To this end, it was suggested[421] that a mandatory obligation be imposed on the Information Protection Regulator to put in place, within a specified period of time, a code of conduct for the banking industry as well as for other industries who deal extensively with personal information, including the insurance industry, marketing industry and the health sector.[422]

7.4.25 It was submitted that codes of conduct must be industry specific and flexible to take into

---

417 Land and Agricultural Development Bank; Law Society of South Africa; Vodacom; Society of Advocates, KwaZulu Natal; Nedbank.

418 Land and Agricultural Development Bank.

419 Law Society of South Africa.

420 Vodacom.

421 Nedbank.

422 Nedbank.

account such matters as fraudulent behaviour on the part of data subjects.[423]

Issuing of codes (sections 54 and 55 of the Discussion Paper Bill)

7.4.26 It was argued that a specific industry should be charged with the drafting of the Codes (as done in terms of the ECT Act) and not the Regulator.[424]

7.4.27 It was noted that in clause 55(4) of the Discussion Paper Bill reference is made to 'public notice in the gazette..." It was proposed that the word "public" be deleted. Furthermore, in clause 55(5) it was proposed that after '. . .subsection (4)", the words "if any" be added.[425]

7.4.28 It was pointed out that clause 54, subclause (2)(a) provides that the code of conduct "must incorporate all the information protection principles or set out obligations that, overall, are the equivalent of all the obligations set out in those principles….". The fact that it is necessary and appropriate to repeat provisions of a law in a code of conduct, was queried.[426]

Adjudicators (clause 58 of the Discussion Paper Bill)

7.4.29 In general, the appointment of self-regulating adjudicators was supported, as such individuals will be well-versed with the applicable industry. It was proposed that more than one adjudicator be registered with the Commission for efficiency reasons. It would afford the industry the opportunity to apply their minds to any problems and reach agreement prior to the proposal being sent to the regulatory authority. [427]

7.4.30 Subclause 58(3) of the Discussion Paper Bill provides that any person aggrieved by the decision of an adjudicator (other than the Regulator) may apply to the Regulator for a review of that decision. Given the nature and costs associated with these adjudications (mostly acrimonious and

---

423 SAFPS.

424 MTN(Pty)Ltd.

425 Department of Communications.

426 SNO Telecommunications.

427 MTN(Pty)Ltd.

bitter; free to the complainant) it would be highly likely, that most, if not all, aggrieved persons would revert to the Regulator (at no charge). This could over-burden the Regulator. It was recommended that this section be amended to provide that aggrieved persons should turn to the courts for redress (at their cost).[428]

Commencement

7.4.31 It was proposed that clause 56(1)(b) of the Discussion Paper Bill be amended to read as follows:

> (b) the Regulator must ensure that as long as the code remains in force, copies of it are available -
> (i) on the Commission's web site;
> (ii) for inspection by members of the public free of charge at the Commission's offices; and
> (iii) for purchase or copying by members of the public at a reasonable price at the Commission's offices.

Stakeholder involvement (self-regulation or regulatory system)

7.4.32 It was argued that clause 55(1) of the Discussion Paper Bill only guarantees genuine stakeholder involvement in instances where the code is issued on application of a person. Where it is issued by the Regulator on its own initiative, there is no provision allowing for genuine stakeholder participation. The requirement to publish the code of conduct in the Gazette for comments is not sufficient to satisfy the fundamental principles underpinning a code of conduct ie self-regulation. Stakeholders who are to be subject to the code must be involved in the formulation, implementation and enforcement of such code. It must be a set of rules, norms and standards voluntarily formulated and adopted by the relevant industry players. It must, therefore, be initiated by the Regulator in consultation with stakeholders. The following amendment to clause 55(1) of the Discussion Paper Bill was suggested:[429]

> 55(1) The Commission may issue a code of conduct under section 54 of this Act :[on the Commission's own initiative or on the application of any person]
> (a) on the Commission's own initiative but in consultation with affected stakeholders or an industry body representing such stakeholders; or
> (b) on application of any person.

---

428 Banking Association.

429 Vodacom; SNO Telecommunications.

Status and effect

7.4.33 It was noted that codes of conduct should have legal binding powers on the organisations or persons governed by them. This is the only way to ensure compliance. Having said that, certain industries, such as the banking industry are mature in their understanding and awareness of consumer rights and data protection and accordingly, the banking sector has had a successful self-regulatory model in the Code of Banking Practice, which all banks take very seriously.[430]

Guidelines (section 59 of the Discussion Paper Bill)

7.4.34 It was proposed that subclause 59(3) should be amended to provide that guidelines are to be published in the Government Gazette.[431]

c) Recommendation

7.4.35 The Commission confirms its proposals set out in the Discussion Paper and recommends that provision should be made in the proposed legislation for the development of codes of conduct in appropriate circumstances. This would contribute to the proper implementation of the information protection principles in each sector.

7.4.36 In order to facilitate the enforcement of the provisions set out in the codes, it is further recommended that the codes should have legal binding powers on the bodies to which it will apply.

7.4.37 In order to avoid over-burdening the Regulator, a fee is prescribed where a person aggrieved by the decision of an adjudicator applies to the Regulator for a review of that decision.

---

430 Nedbank.

431 Banking Council.

7.4.38 Enhanced provision has been made in clause 58(1) for stakeholder involvement and consultation in the issuing of a code of conduct.

7.4.39 The legislative enactment of this provision will read as follows:

CHAPTER 7
CODES OF CONDUCT

Issuing of codes of conduct

57.(1) The Regulator may issue codes of conduct.

(2) A code of conduct must -

(a) incorporate all the information protection principles or set out obligations that provide a functional equivalent of all the obligations set out in those principles; and

(b) prescribe how the information protection principles are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which the responsible parties are operating.

(3) A code of conduct may apply in relation to any one or more of the following -

(a) any specified information or class or classes of information;

(b) any specified body or class or classes of bodies;

(c) any specified activity or class or classes of activities; or

(d) any specified industry, profession, or calling or class or classes of industries, professions, or callings.

(4) A code of conduct must also -

(a) in relation to any body that is not a public body, provide for controls in relation to the comparison (whether manually or by means of any electronic or other device) of personal information with other personal information for the purpose of producing or verifying information about an identifiable data subject;

(b) provide for the review of the code by the Regulator;

(c) provide for the expiry of the code.

Proposal for issuing of code of conduct

58.(1) The Regulator may issue a code of conduct under section 57 of this Act -

(a) on the Regulator's own initiative but in consultation with affected stakeholders or a body representing such stakeholders; or

(b) on the application of any person as provided in subsection (3) of this section.

(2) Without limiting subsection (1) of this section, but subject to subsection (3) of this section, any person may apply to the Regulator for the issuing of a code of conduct in the prescribed form submitted by the applicant.

(3) An application may be made pursuant to subsection (2) of this section only -

(a) by a body which is, in the opinion of the Regulator, sufficiently representative of any class or classes of bodies, or of any industry, profession, or calling as defined in the code; and

(b) if the code of conduct sought by the applicant is intended to apply in respect of the class or classes of bodies, or the industry, profession, or calling, that the applicant represents, in respect of such class or classes of bodies or such industry, profession, or calling.

(4) If an application is made to the Regulator pursuant to subsection (2) of this section, or if the Regulator intends to issue a code on its own initiative, the Regulator must give notice in the Gazette that the issuing of a code of conduct is being considered, which notice must contain a statement that -

(a) the details of the code of conduct being considered, including a draft of the proposed code, may be obtained from the Regulator; and

(b) submissions on the proposed code may be made in writing to the Regulator within such period as is specified in the notice.

(5) The Regulator must not issue a code of conduct unless it has considered the submissions made to the Regulator in terms of subsection (4) if any and is satisfied that all persons affected by the proposed code have had a reasonable opportunity to be heard.

(6) The decision as to whether an application for the issuing of a code has been successful must be made within a reasonable period of time which must not exceed thirteen(13) weeks.

Notification, availability and commencement of code

59.(1) If a code of conduct is issued under section 57 of this Act -

(a) the Regulator must ensure that there is published in the Gazette, as soon as reasonably practicable after the code is issued, a notice -

(i) indicating that the code has been issued; and

(ii) indicating where copies of the code are available for inspection free of charge and for purchase; and

(b) the Regulator must ensure that as long as the code remains in force, copies of it are available -

(i) on the Regulator's web site;

(ii) for inspection by members of the public free of charge at the Regulator's offices; and

(iii) for purchase or copying by members of the public at a reasonable price at the Regulator's offices.

(2) A code of conduct issued under section 57 of this Act comes into force on the 28th day after the date of its notification in the Gazette or on such later date as may be specified in the code and is binding on every class or classes of body, industry, profession or calling referred to therein.

Amendment and revocation of codes

60.(1) The Regulator may from time to time amend or revoke a code of conduct issued under section 57 of this Act.

(2) The provisions of sections 57 to 61 of this Act must apply in respect of any amendment or revocation of a code of conduct.

Procedure for dealing with complaints

61.(1) A code of conduct may prescribe procedures for making and dealing with complaints alleging a breach of the code, but no such provision may limit or restrict any provision of Chapter 8 of this Act.

(2) If the code sets out procedures for making and dealing with complaints, the Regulator must be satisfied that -

(a) the procedures meet the -

(i) prescribed standards; and

(ii) any guidelines issued by the Regulator in terms of section 62 relating to making of and dealing with complaints;

(b) the code provides for the appointment of an independent adjudicator to whom complaints may be made;

(c) the code provides that, in performing his or her functions, and exercising his or her powers, under the code, an adjudicator for the code must have due regard to the matters listed in section 44(2);

(d) the code requires the adjudicator to prepare and submit a report (in a form satisfactory to the Regulator) to the Regulator within five (5) months of the end of a financial year of the Department for Justice and Constitutional Development on the operation of the code during that financial year; and

(e) the code requires the report prepared for each year to specify the number and nature of complaints made to an adjudicator under the code during the relevant financial year.

(3) A data subject who is aggrieved by a determination, including any declaration, order or direction that is included in the determination, made by an adjudicator (other than the Regulator) after investigating a complaint relating to the protection of personal information under an approved code of conduct, may lodge a complaint with the Regulator against the determination on payment of a prescribed fee.

(4) The adjudicator's determination continues to have effect unless and until the Regulator makes a determination under Chapter 10 relating to the complaint.

Guidelines about codes of conduct

62.(1) The Regulator may provide written guidelines -

(a) to assist bodies to develop codes of conduct or to apply approved codes of conduct;

(b) relating to making and dealing with complaints under approved codes of conduct; and

(c) about matters the Regulator may consider in deciding whether to approve a code of conduct or a variation of an approved code of conduct.

(2) Before providing guidelines for the purposes of paragraph (1)(b), the Regulator must give everyone the Regulator considers has a real and substantial legitimate interest in the matters covered by the proposed guidelines an opportunity to comment on them.

(3) The Regulator must publish guidelines provided under subsection (1) in the Government Gazette.

Register of approved codes of conduct

63.(1) The Regulator must keep a register of approved codes of conduct.

(2) The Regulator may decide the form of the register and how it is to be kept.

(3) The Regulator must make the register available to the public in the way that the Regulator determines.

(4) The Regulator may charge reasonable fees for -

(a) making the register available to the public; or

(b) providing copies of, or extracts from, the register.

Review of operation of approved code of conduct

64.(1) The Regulator may, at its own instance, review the operation of an approved code of conduct.

(2) The Regulator may do one or more of the following for the purposes of the review -

(a) consider the process under the code for making and dealing with complaints;

(b) inspect the records of an adjudicator for the code;

(c) consider the outcome of complaints dealt with under the code;

(d) interview an adjudicator for the code; and

(e) appoint experts to review those provisions of the code that the Regulator believes require expert evaluation.

(3) The review may inform a decision by the Regulator under section 60 to revoke the approved code of conduct with immediate effect or at a future date to be determined by the Regulator.

Effect of failure to comply with code

65. If a code of conduct issued under section 57 of this Act is in force, failure to comply with the code is deemed to be a breach of an information protection principle.

CHAPTER 8: ENFORCEMENT

8.1 Introduction

8.1.1 In a broad sense, enforcement can be understood as any action leading to better compliance with national privacy legislation, including awareness raising activities and the development of guidance. In a narrower sense, enforcement means the undertaking of investigative actions, or even solely, the imposition of sanctions.[1] In this chapter the narrower interpretation will be investigated.[2]

8.1.2 Enforcement, in this sense, therefore, refers to the third element of the compliance-orientated regulation framework discussed in Chapter 7 above.[3]

8.1.3 The grounds for starting an enforcement action in the narrow sense can vary; on the one hand, enforcement action can be based on concrete information that there is a breach of the information protection legislation. Such information can come from the complainant, from the press etc. On the other hand, oversight authorities can develop their own investigation or audit programmes. Such programs could be aimed at providing a more accurate picture of the implementation of particular information protection rules or information protection legislation within particular sectors, with a view to developing the policies of the oversight authorities, providing guidance etc. The purpose of such programs could also be to check whether or not responsible parties comply with the rules, and to aim at underlining to responsible parties what is expected of them. In investigation or audit programs, the use of formal powers, and the imposition of sanctions at a national level, could turn out to be necessary.[4]

8.1.4 It is, therefore, clear that the existence and ready availability of effective remedies

---

1 European Union Article 29 Data Protection Working Party ***Declaration of the Article 29 Working Party on Enforcement*** WP101 (12067/04/EN) Adopted on 25th November 2004 (hereafter referred to as "***WP101 on Enforcement***") at 3.

2 See, however, the discussion in Chapter 7 entitled "Supervision".

3 Par 7.2.189.

4 ***W101 on enforcement*** at 3.

against unlawful or improper processing is essential to ensure both compliance with the law, generally, and enjoyment of the rights and remedies of data subjects in particular.[5]

8.1.5 We have already established[6] that the most notable difference between the self-regulatory system, on the one hand, and the regulatory or co-regulatory systems, on the other, is the manner in which the information protection principles are enforced.[7] In the self-regulatory system there is no general information protection authority to oversee the implementation of the privacy legislation. The chosen method of implementation has, on occasion, been described as "voluntary compliance and self-help" or a "dispersed responsibility method". In other words, it is up to the responsible parties themselves to comply with the Act and an individual has to enforce his or her rights under the Act through the courts.[8] The regulatory and co-regulatory system, on the other hand, makes provision for an authority to oversee enforcement (external supervision). This is the system preferred by the Commission.

8.1.6 The topic of sanctions and remedies is dealt with only in very general terms by the CoE Convention, OECD Guidelines and UN Guidelines. The EU Directive is more specific. In particular, Article 28(3) states that supervisory authorities shall have investigative powers and powers to collect all the information necessary, effective powers of intervention and the power to engage in legal proceedings.[9] Article 28(4) provides that the authority shall consider

---

5 Korff ***Comparative Study*** at 179.

6 See Chapter 7 above.

7 See also Roos thesis at 533.

8 Roos thesis at 534.

9 Article 28(3) of the EU Directive provides as follows:
Each authority shall in particular be endowed with:
* investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties.
* effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;
* the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive has been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

complaints.[10] Article 22 furthermore requires that data subjects be given the right to a "judicial remedy" for "any breach" of their rights pursuant to the applicable national information protection law.[11] Article 28(3) also stipulates that decisions by an information protection authority which give rise to complaints "may be appealed against through the courts".[12] Finally, Article 28(6) stipulates that the supervisory authorities must cooperate with one another.[13]

8.1.7 The purpose of external supervision of information protection is therefore threefold:

* To deliver a satisfactory level of compliance with the rules contained in the information protection legislation;
* To provide support and help to data subjects in the exercise of their rights;
* To provide appropriate redress to prejudiced data subjects where rules are not complied with.

8.1.8 All information protection Acts stipulate a variety of sanctions and remedies for breach of their provisions.[14] Provision is usually made for a combination of penalties (fines and imprisonment), compensatory damages and where applicable, revocation of licences and deregistration.

8.1.9 In the final analysis, the central question concerns the extent of the powers of a Commission to order compliance with the information protection principles. There is a clear difference between those authorities whose powers are limited to those of investigation and

---

10 Article 28(4) of the EU Directive provides as follows:
Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

11 Article 22 of the EU Directive provides as follows:
Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question.

12 See Article 28(3) of the EU Directive in fn 9 above.

13 Article 28 (6) of the EU Directive provides as follows:
Each supervisory authority..... The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

14 The Article 29 Working Party stated that the promotion of harmonised compliance in order to promote better compliance with data protection laws on a national level is a strategic and permanent goal of the Working Party. It has decided to exchange best practices, discuss enforcement strategies and to investigate possibilities for the preparation of EU wide, synchronised, national enforcement actions for Member States.

recommendation, and those that can mandate changes in behaviour.[15]

8.1.10 In the Discussion Paper the Commission indicated that it is clear that the best way of providing external supervision is through an independent regulatory authority,[16] as well as by providing data subjects with legal remedies which they can enforce in a court of law.[17] The regulatory authority should have investigative powers and powers to engage in legal proceedings where the information protection legislation has been violated. The individual should also have rights of enforcement independent of the information protection authority, 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 itself. An individual who has suffered damage by reason of a contravention of the information protection legislation should furthermore be entitled to compensation by either the responsible parties or the data processors.[18] Finally, in accordance with most other jurisdictions, the legislation should also provide for a number of criminal offences under the Bill.

8.1.11 In general, commentators[19] were in agreement with the enforcement provisions set out in Chapter 8 and in Chapter 9 of the Discussion Paper Bill. Enforcement of rights and the protection of personal information must be possible and it was argued that the Discussion Paper Bill does seem to provide a suitable and workable arrangement in clauses 63 to 84.[20] It was stated that the structures proposed will encourage and protect the emergence of a culture of respect for personal data privacy and resultant new principles. The provisions, furthermore, also do not exclude our existing courts, but allow the courts to encourage acceptance of the principles by imposing damages awards in appropriate circumstances.[21]

8.1.12 In the rest of this Chapter the detailed provisions of the proposed system will be discussed under the following headings:

---

15 Bennett and Raab ***The Governance of Privacy*** at 117.

16 See Chapter 7 above.

17 See discussion in Chapter 7 above; Roos thesis at 723 referring to Data Protection Working Party Transfers of personal data to third countries 4-5.

18 Summary in Roos thesis at 538.

19 Society of Advocates of Kwa-Zulu Natal; Law Society of South Africa.

20 Law Society of South Africa.

21 Law Society of South Africa.

* Complaints procedure (para 8.2);
* Assessment/Audit (para 8.3);
* Advisory approach (para 8.4);
* Enforcement powers (para 8.5);
* Courts/judicial remedies (para 8.6);
* Compensation (para 8.7).

8.2 Complaints procedure

a) Proposals in the Discussion Paper[22]

22 **CHAPTER 8**
ENFORCEMENT

Interference with the protection of the personal information of a person -
63. For the purposes of this Chapter, an action is an interference with the protection of the personal information of a person if, in relation to that person -
(i) the action breaches an information privacy principle; or
(ii) the provisions of section 20 of this Act have not been complied with; or
(iii) the provisions of section 93 of this Act have not been complied with; or
(iv) the provisions of section 94 of this Act have not been complied with.
.
Complaints
64. Any person may submit a complaint to the Commission in the prescribed manner and form alleging that any action is or appears to be an interference with the protection of the personal information of a person.

Mode of complaint to Commission
65. (1) A complaint to the Commission may be made either orally or in writing.
(2) A complaint made orally must be put in writing as soon as reasonably practicable.
(3) The Commission must give such reasonable assistance as is necessary in the circumstances to enable an individual, who wishes to make a complaint to the Commission, to put the complaint in writing.

Investigation by Commission
66. (1) The functions of the Commission under this Chapter of this Act are to --
(a) investigate any action that is or appears to be an interference with the protection of the personal information of a person;
(b) act as conciliator in relation to any such action;
(c) take such further action as is contemplated by this Chapter of this Act.

(2) The Commission may commence an investigation under subsection (1)(a) of this section either on complaint made to the Commission or on the Commission's own initiative.

Action on receipt of complaint
67. (1) On receiving a complaint under this Chapter of this Act, the Commission may -
(a) investigate the complaint; or
(b) decide, in accordance with section 68 of this Act, to take no action on the complaint.
(2) The Commission must, as soon as practicable, advise the complainant and the person to whom the complaint relates of the procedure that the Commission proposes to adopt under subsection (1) of this section.

Commission may decide to take no action on complaint
68. (1) The Commission may in its discretion decide to take no action or, as the case may require, no further action, on any complaint if, in the Commission's opinion -
(a) the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable; or
(b) the subject-matter of the complaint is trivial; or

(c) the complaint is frivolous or vexatious or is not made in good faith; or
(d) the person alleged to be aggrieved does not desire that action be taken or, as the case may be, continued; or
(e) the complainant does not have a sufficient personal interest in the subject-matter of the complaint; or
(f) where -
(i) the complaint relates to a matter in respect of which a code of conduct issued under section 54 of this Act is in force; and
(ii) the code of conduct makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.

(2) Notwithstanding anything in subsection (1) of this section, the Commission may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Commission that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

(3) In any case where the Commission decides to take no action, or no further action, on a complaint, the Commission must inform the complainant of that decision and the reasons for it.

Referral of complaint to regulatory body
69.(1) Where, on receiving a complaint under this part of the Act, the Commission considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body, the Commission must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned.

(2) If the Commission determines that the complaint should be dealt with by another body as described above, the Commission must forthwith refer the complaint to this body to be dealt with accordingly and must notify the complainant of the action that has been taken.

Pre-investigation Proceedings of Commission
70. Before proceeding to investigate any matter under this Chapter of this Act, the Commission must inform -
(a) the complainant, the person to whom the investigation relates, and any individual alleged to be aggrieved (if not the complainant), of the Commission's intention to make the investigation; and
(b) the person to whom the investigation relates of the ---
(i) details of the complaint or, as the case may be, the subject-matter of the investigation; and
(ii) right of that person to submit to the Commission, within a reasonable time, a written response in relation to the complaint or, as the case may be, the subject-matter of the investigation.

Settlement of complaints
71. Where it appears from a complaint, or any written response made in relation to a complaint under section 70(b)(ii) of this Act, that it may be possible to secure a settlement between any of the parties concerned and, if appropriate, a satisfactory assurance against the repetition of any action that is the subject-matter of the complaint or the doing of further actions of a similar kind by the person concerned, the Commission may, without investigating the complaint or, as the case may be, investigating the complaint further, use his or her best endeavours to secure such a settlement and assurance.

Investigation proceedings of the Commission
72. For the purposes of the investigation of a complaint the Commission may -
(a) summon and enforce the appearance of persons before the Commission and compel them to give oral or written evidence on oath and to produce any records and things that the Commission considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;
(b) administer oaths;
(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commission sees fit, whether or not it is or would be admissible in a court of law;
(d) at any reasonable time, subject to section 73, enter and search any premises occupied by a responsible party;
(e) converse in private with any person in any premises entered under section 75 subject to section 73; and
(f) otherwise carry out in those premises any inquiries that the Commission sees fit in terms of section 73.

Issue of warrants
73. (1) If a judge of the High Court, a regional magistrate or a magistrate is satisfied by information on oath supplied by the Commission that there are reasonable grounds for suspecting that -

(a) a responsible party is interfering with the protection of the personal information of a person, or
(b) an offence under this Act has been or is being committed,
and that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, it may, subject to subsection 2, provided the premises are within the jurisdiction of that judge or magistrate, grant a warrant to enter and search such premises to the Commission.

(2) A warrant issued under subsection (1) authorises the Commission or any of its officers or staff, subject to section 75, at any time within seven days of the date of the warrant to enter the premises as identified in the warrant, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal information and to inspect and seize any documents or other material found there which may be such

evidence as is mentioned in that sub-section.

Requirements for issuing of warrant

74.(1) A magistrate or judge must not issue a warrant under section 73 unless he or she is satisfied-
(a) that the Commission has given seven days' notice in writing to the occupier of the premises in question demanding access to the premises, and
(b) that either-
(i) access was demanded at a reasonable hour and was unreasonably refused, or
(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by any of the Commission's members or officers or staff to permit the members or the officer or member of staff to do any of the things referred to in section 73(2), and
(c) that the occupier, has, after the refusal, been notified by the Commission of the application for the warrant and has had an opportunity of being heard by the judge on the question whether or not it should be issued.
(2) Subsection (1) must not apply if the judge or magistrate is satisfied that the case is one of urgency or that compliance with those provisions would defeat the object of the entry.
(3) A judge or magistrate who issues a warrant under section 73 must also issue two copies of it and certify them clearly as copies.

Execution of warrants
75.(1) A person executing a warrant issued under section 73 may use such reasonable force as may be necessary.

(2) A warrant issued under this section must be executed at a reasonable hour unless it appears to the person executing it that there are grounds for suspecting that the evidence in question would not be found if it were so executed.

(3) If the person who occupies the premises in respect of which a warrant is issued under section 73 is present when the warrant is executed, he or she must be shown the warrant and supplied with a copy of it; and if that person is not present a copy of the warrant must be left in a prominent place on the premises.

(4) A person seizing anything in pursuance of a warrant under section 73 must give a receipt for it if asked to do so.

(5) Anything so seized may be retained for so long as is necessary in all the circumstances but the person in occupation of the premises in question must be given a copy of anything that is seized if he or she so requests and the person executing the warrant considers that it can be done without undue delay.

(6) A person authorised to conduct an entry and search in terms of section 73 may be accompanied and assisted by a police officer.

(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard for each person's right to dignity, freedom, security and privacy.

(8) A person who enters and searches premises under this section, before questioning any person -

(a) must advise that person of the right to be assisted at the time by an advocate or attorney; and
(b) allow that person to exercise that right.

Matters exempt from search and seizure
76. The powers of search and seizure conferred by a warrant issued under section 73 must not be exercisable in respect of personal information which by virtue of section 32 (exemptions) are exempt from any of the provisions of this Act.

Communication between legal adviser and client exempt

77.(1) Subject to the provisions of this section, the powers of search and seizure conferred by a warrant issued under section 73 must not be exercisable in respect of -

(a) any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act, or

(b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the court) and for the purposes of such proceedings.

(2) Subsection (1) applies also to-

(a) any copy or other record of any such communication as is there mentioned, and

(b) any document or article enclosed with or referred to in any such communication if made in connection with the giving of any advice or, as the case may be, in connection with or in contemplation of and for the purposes of such proceedings as are there mentioned.

Objection to search and seizure

8.2.1 Worldwide, oversight authorities are charged with investigating possible breaches of the law within their jurisdiction. As stated above, such investigations can arise out of operational activities or out of specific complaints from individual data subjects.[23]

8.2.2 The oversight function of information protection authorities typically encompasses the handling and resolution of complaints by citizens pertaining to the processing of personal information.[24] Since few cases under information privacy laws ever reach the courts, the overwhelming majority of complaints of breach of privacy laws are resolved by Commissioners, whether by mediation or by the exercise of binding powers where they have them.[25]

8.2.3 In most countries the national authorities are vested with extensive powers of access to files and filing systems used to process personal information, and the authorities can therefore usually demand full access to all relevant sites and materials.[26]

8.2.4 Commissioners are sometimes given astonishingly wide and strong powers of search and

---

78. If the person in occupation of any premises in respect of which a warrant is issued under this Schedule objects to the inspection or seizure under the warrant of any material on the ground -

a) that it contains privileged information and refuses the inspection or removal of such article or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the registrar of the High Court which has jurisdiction or his or her delegate, to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not;

b) that it consists partly of matters in respect of which those powers are not exercisable, he or she must, if the person executing the warrant so requests, furnish that person with a copy of so much of the material as is not exempt from those powers.

Return of warrants

79. A warrant issued under this section must be returned to the court from which it was issued-

(a) after being executed, or

(b) if not executed within the time authorised for its execution;

and the person by whom any such warrant is executed shall make an endorsement on it stating what powers have been exercised by him or her under the warrant.

23 Korff ***Comparative Study*** at 206.

24 Bygrave ***Data Protection*** at 70.

25 Greenleaf G "Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners" Paper originally prepared for a workshop at the International Conference of Privacy and Data Protection Commissioners, Cardiff, UK September 2002. (hereafter referred to as "Greenleaf presentation 2002") at 1. Prof Greenleaf argues the case for the publication by Commissioners of complaint resolutions.

26 Korff ***Comparative Study*** at 206.

entry, often exercisable without a judicial warrant.[27]

8.2.5 After a complaint has been received the authority usually gets in touch with the responsible party concerned, "advises" and acts as a conciliator, and tries to reach an amicable solution to the dispute. In many cases, the issues are straight-forward and easily resolved on the basis of clear legal principles. For instance, a responsible party refusing to grant a data subject access to his or her information may need to be "reminded " by the authority of its duty to allow such access. Other cases, however, are more complex, and in those the authority tries to reach a compromise acceptable to both the responsible party and the data subject. Again, this approach is almost always "successful" in the sense that the authority does not need to use formal enforcement measures: the authorities in the EU Member States have reported that they only resort to "hard" enforcement measures in a minute proportion (a few percent) of complaints.[28]

8.2.6 Examples of the work done by Privacy Commissioners in other countries are set out in Chapter 7 above. [29]

8.2.7 In the UK the Commissioner's 2002 Report indicated that her office received about 10,000 complaints annually, and about 5% of these (ie 500) result in "verified assessments suggesting compliance unlikely".[30]

b) Evaluation

8.2.8 The following written comments were received regarding specific aspects of enforcement:

(i) Mode of complaint

---

27 Korff ***Comparative Study*** at 200; See eg section 34(1)(d) of the Canadian Privacy Act; section 12(1)(d) of the Canadian PIPEDA.

28 Korff ***Comparative Study*** at 208.

29 See specifically para 7.2.26 and further.

30 Greenleaf presentation 2002 at 24.

8.2.9 The Commission was reminded[31] that complaints concerning the Intelligence Services can already be lodged with the civil courts, the Inspector-General, JSCI and the Public Protector. It was also argued[32] that the party about whom the complaint is lodged must have the opportunity to respond to its own regulatory body.

(ii) Investigation proceedings

8.2.10 Clause 72(c) of the Discussion Paper Bill states that the Commission may receive any evidence "whether or not it is or would be admissible in a court of law". The Regulator may, therefore, accept evidence as hearsay. It was suggested[33] that this clause be aligned with constitutional dictates so that evidence that is not admissible in a court of law is also inadmissible in the Commission's inquiry.

8.2.11 On the other hand, clarity was sought as to whether surveillance information, which may have been improperly or unconstitutionally obtained,[34] may be considered or whether it will, per se, be a violation of the complainant's right to privacy. [35] In the Ombudsman's Annual Report[36] it is explained that an approach has been formulated where the overarching principle is fairness to both parties. It was argued that this does not mean that there is necessarily a duty to disregard evidence improperly or unconstitutionally obtained.

8.2.12 Fairness may sometimes require one to have regard to relevant and reliable evidence. Like a court, there is a discretion to accept and consider such evidence, taking into account how it was obtained, whether it could have been obtained lawfully, the reasons why proper means were not used, the reliability of the evidence, whether the acceptance of such evidence would be improper as to transgress constitutionality, the materiality of the evidence, whether such evidence was necessary to have a balanced view of the dispute, and the nature and degree of

---

31 National Intelligence Agency.

32 SAIA.

33 Department of Home Affairs. The Department of Home Affairs processes personal information on a daily basis as its core function is the providing of enabling documents.

34 Confronted with concealed video camera footage showing that a person who had claimed to be in a wheelchair could in fact walk.

35 Ombudsman for Long Term Insurance.

36 Ombudsman for Long Term Insurance ***Annual Report*** 2005 at 44.

impropriety of obtaining the evidence. [37]

(iii) Warrants to enter and search

8.2.13 A concern was expressed that in clause 73 of the Discussion Paper Bill (Issue of warrants), there is no obligation on the Regulator to carry out an investigation, first, before approaching the magistrate to grant a warrant in relation to an alleged infringement of the right to privacy. The section also does not provide for notice to be given to the alleged infringer to remedy the breach, although clause 81 does provide for an information notice, in other circumstances, to be given to the alleged infringer.

8.2.14 It was, furthermore, argued that clause 74(1)(c) of the Discussion Paper Bill[38] which provides for seven days notice in writing demanding access to the premises, is not sufficient, particularly given the provisions of clause 75 (Execution of warrants) which permits the use of "reasonable force", and as subclause (c) anticipates that an appearance before a judge will be limited to whether or not the warrant should be issued, not whether or not the alleged infringer has any justification for its actions or omissions.[39]

8.2.15 It was indicated[40] that the proposal that the Regulator be authorised to perform search and seizure operations where interference with personal information or an offence in terms of the draft Bill is suspected, is not supported. If offences are committed, the SAPS is constitutionally mandated, equipped and trained to deal with the same.

8.2.16 In this regard it was, furthermore, stated that the word "may" in sub-clause (6) should be

---

37 Ombudsman for Long Term Insurance.

38 Clause 74(1) states as follows:

"A magistrate or judge must not issue a warrant under section 73 unless he or she is satisfied-
(a) that the Commission has given seven days' notice in writing to the occupier of the premises in question demanding access to the premises; and
(b) that either -
(i) access was demanded at a reasonable hour and was unreasonably refused, or
(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by any of the Commission's members or officers or staff to permit the members or the officer or member of staff to do any of the things referred to in section 73(2); and
(c) that the occupier, has, after the refusal, been notified by the Commission of the application for the warrant and has had an opportunity of being heard by the judge on the question whether or not it should be issued."

39 SNO Communications (Pty) Ltd.

40 SAPS; Banking Council.

substituted for the word “must”, as the sub-clause grants the person authorised to conduct an entry and search wide powers and section 25 of the Criminal Procedure Act of 1977[41] provides that only police officials may enter premises and conduct searches and seizures in terms of a warrant.[42] It was argued that although it may be necessary to use reasonable force, those circumstances should be spelt out in the Bill. A person who executes a warrant must at all times be accompanied by a police officer (section 75(6) of the Discussion Paper Bill).[43]

8.2.17 It was submitted that subclause (4) places the onus on the person whose goods are being seized to request a receipt. However, the onus should be reversed – the person seizing goods must issue a receipt.[44]

(iv) Communication with legal adviser

8.2.18 Subclauses 77(1)(a) and (b) of the Discussion Paper Bill restrict attorney-client privilege to matters under or out of "this Act" only. This could result in a serious breach of privilege where the Act is used for search and seizure in relation to other Acts.[45]

c) Recommendation

8.2.19 The Commission confirms its proposals regarding the complaints procedure as set out in the Discussion Paper Bill subject only to clarifications on points of detail. Provision is made for data subjects to lodge a complaint with the Regulator regarding any interference with the protection of their personal information. In terms of the procedures set out in the Bill the Regulator may investigate, conciliate and settle complaints where possible. Special provision is made for the Regulator to approach the Magistrates’ Court to grant a warrant to enter and search the premises of a responsible party in specified

---

41 Act 51 of 1977.

42 Provincial Administration, Western Cape.

43 Department of Communications.

44 Banking Council.

45 Banking Council.

circumstances. It is, however, explicitly stated that a police officer must accompany and assist any person conducting an entry and search in terms of the Bill. See clauses 70 to 86 as set out on page 598 below.

8.3 Assessment/Audit

a) Proposals in the Discussion Paper[46]

8.3.1 If a person believes processing is being carried on which directly affects him or her, he or she, or a person on his or her behalf, may apply for an assessment as to whether the processing is likely to, or unlikely to, comply with the provisions of the Bill. Such an assessment may also be conducted on the initiative of the Regulator itself (especially where new technology is being used for the first time).[47]

8.3.2 Section 13(1)(b) of the New Zealand Act provides that when requested to do so by a responsible party (agency), the Commissioner must conduct an audit of personal information maintained by that agency for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles.

---

46 **Assessment**

80. (1) The Commission, acting in its official capacity, or at a request made to the Commission by or on behalf of any person who is, or reasonably believes himself to be, affected by an action in terms of section 63, must make an assessment, subject to subparagraph (2), as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act.

(2) The Commission must make the assessment in such manner as appears to be appropriate, unless, where the assessment is made on request, it has not been supplied with such information as it may reasonably require in order to-

(a) satisfy itself as to the identity of the person making the request, and
(b) enable it to identify the action in question.

(3) The matters to which the Commission may have regard in determining in what manner it is appropriate to make an assessment include the extent to which the request appears to it to raise a matter of substance, and where the assessment is made on request, -

(a) any undue delay in making the request, and

(b) whether or not the person making the request is entitled to make an application under Principle 7 (access) in respect of the personal information in question.

(4) Where the Commission has received a request under this section it must notify the person who made the request-

(a) whether it has made an assessment as a result of the request, and

(b) to the extent that it considers appropriate, having regard in particular to any exemption from Principle 7 applying in relation to the personal information concerned, of any view formed or action taken as a result of the request.

47 See eg section 42 of the UK Data Protection Act, 1998; section 13(1) (b) of the New Zealand Act; Section 60 of the WBPin the Netherlands; section 18 of the Canadian PIPEDA (private bodies); section 37 of the Canadian Privacy Act (public bodies).

8.3.3 Section 42 of the UK Data Protection Act also makes provision for this position. The Commission must, upon receipt of such a request make such an assessment, provided the Commissioner has been provided with sufficient information to identify the person making the request and the processing in question.[48] It, furthermore, stipulates the matters the Commissioner may take into account to determine the manner of the assessment. They are the extent to which the request appears to raise a matter of substance, any undue delay in making the request, and finally whether the person making the request is entitled to make a subject access request.

8.3.4 In terms of the UK legislation an information notice may be served requiring the responsible party (data controller) to furnish the Commissioner with information relating to the processing of the information. Finally, special information notices may be served where requests in terms of section 42 have been received with regard to processing for special purposes (journalism, literary and artistic purposes).

8.3.5 As is the case with enforcement notices discussed above, the latter notices are also subject to an appeal procedure set out in terms of section 48 of the Act. Under section 47(1) a person who fails to comply with an enforcement notice, information notice or special information notice commits an offence. A person who makes false or reckless statements in purported compliance with the notices also commits an offence.

8.3.6 In Canada, when an alleged breach of privacy occurs at a public body, the Office of the Information and Privacy Commission will normally assist the responsible party (agency) involved in conducting its own investigation. Since the goal in such circumstances is to seek a systemic solution, the Office depends on the investigative and auditing capacity of the public body in the first instance and then reviews the resulting report.[49]

8.3.7 The case has, therefore, been argued for the use of this privacy impact assessment as an additional tool in the arsenal of the Information Commissioner.[50] In recent years privacy specialists have developed an assessment model for the application of new technology or the

---

48 Bainbridge ***Data Protection*** at 146.

49 Flaherty DH "How to do a Privacy and Freedom of Information Act Site Visit" A revised version of a presentation to the Privacy Laws and Business Annual Conference, Cambridge, UK, July 1998 .

50 Flaherty DH "Privacy Impact Assessments: An Essential Tool for Data Protection" 2000 accessed at http://aspe.hhs.gov/datacncl/flaherty.htm on 15/7/2005.

introduction of a new service, which has a high potential for raising privacy alarms at an early stage in an organisation's planning process in either the public or the private sectors.

8.3.8 The essential goal is for an organisation itself to describe personal information flows as fully as possible so that the privacy implications can be analysed and addressed in a coherent manner and compliance with fair information practices may be established. Conducting a privacy impact assessment is also an effective method of engaging a team of persons at an organisation, including technology, policy, legal and privacy specialists, to work together to identify and resolve information protection.

b) Evaluation

8.3.9 It has been noted that the central tension in regulating compliance with the legislation is how to strike a balance between resolving individual complaints and remedying systemic issues.[51] It has been suggested that tools such as prior investigations,[52] assessments, audits[53] and Privacy Impact Assessments (PIA) are all pro-active compliance measures that may assist in ensuring a proper system of protection.

8.3.10 It is, however, important to distinguish between the different concepts. The prior investigation is conducted by the Regulator in instances where such processing carries a particular risk for the individual rights and freedoms of the data subject.[54]

8.3.11 A PIA, on the other hand, is a (mostly) voluntary tool,[55] used by the responsible party, itself, to consider future consequences for the privacy of data subjects as a result of any proposed processing of personal information. The questions that a responsible party needs to answer are, firstly, how the proposed project will affect the privacy of data subjects and secondly, whether it is possible to achieve the objectives of the project while also protecting the privacy

---

51 ***ALRC Discussion Paper*** at 1242. Systemic issues refer to issues that are about an organisation's or industry's practice rather than about an isolated incident.

52 Clause 55 of the Bill.

53 Clause 87 of the Bill.

54 See discussion in Chapter 7 above.

55 See, however, discussion on USA and Canada in fn 56 below.

of data subjects. The most significant benefits of a PIA are achieved when it is integrated into the decision-making process for the project.[56]

8.3.12 The third category is the assessment as set out in clause 80 of the Discussion Paper Bill. The assessment is an audit, conducted by the Regulator, of processing practices already in place.

8.3.13 All these tools can play a role in ensuring good business practice in general. A suggestion was made that there should be an independent body, rather than the Regulator, to make such an assessment.[57]

c) Recommendation

8.3.14 The Commission regards the remedies that address systemic issues and are able to effect systemic changes in organisations as of utmost importance. The Commission, therefore, confirms its proposal in the Discussion Paper that provision should be made, where appropriate, for an assessment or audit of the processing of personal information practices already in place to determine whether it complies with the provisions of the Bill. The assessment may be conducted at the Regulator's own initiative or at the request of another person.

8.3.15 In order to acquire the information necessary to conduct the assessment the Regulator may serve the responsible party with an information notice requiring the responsible party, either to furnish the Regulator with an independent auditor's report indicating that the processing is taking place in accordance with provisions of the Act, or with such other information as specified.

8.3.16 After completing the assessment the Regulator reports the results of the assessment to the responsible party and makes an appropriate recommendation. The recommendation is deemed to be the equivalent of an enforcement notice.

---

56 ***ALRC Discussion paper*** at 1200; In the USA section 208 of the E-Government Act 2002 2458 Stat 803 (US) requires that a PIA be undertaken, reviewed and if practicable published before a government agency develops or procures a new information system or initiates a new collection of personally identifiable information. In Canada, PIA's are also mandatory. Under the Canadian Government's Privacy Impact Assessment Policy all federal governments must conduct a PIA for proposals for all new programmes that raise privacy issues.

57 SAIA.

8.3.17 The legislative enactment to make provision for assessments, as well as the furnishing of information to the Regulator, is set out in clauses 87 to 88 on page 606 below.

8.3.18 Responsible parties should, furthermore, be encouraged to conduct PIA's for new products and education should be provided by the Regulator regarding the value of such an action. Privacy protection should be seen, not as an obstacle to be overcome, but rather as a design objective in the development of new information processing systems.

8.4 Advisory approach

a) Proposals in the Discussion Paper

8.4.1 In most cases, the authorities are empowered to issue legally binding (though appealable) orders. In some jurisdictions, however, the authorities either do not have such competence at all,[58] or they have not had it in relation to certain sectors.[59]

8.4.2 The more advisory approach is often preferred because it avoids the adversarial relationships that arise when enforcement powers are used or threatened. It may be argued that adverse publicity for poor privacy protection can be an effective sanction.[60] The implementation of the Directive does not appear to have changed the generally advisory and concilliatory approach of the national information protection authorities.[61]

8.4.3 Even if blatant violations of the law are found (such as non-registration or processing operations) the authority will usually first only issue a "reminder", "warning" or "advice" and it will not resort to more formal measures unless these "softer" measures are ignored or disputed. [62]

---

58 Eg Germany's Federal Data Protection Commissioner see the Federal Data Protection Act ss 24-26.

59 Bygrave ***Data Protection*** at 71.

60 Bennett and Raab ***The Governance of Privacy*** at 117.

61 Korff ***Comparative Study*** at 200.

62 Korff ***Comparative Study*** at 207.

In many jurisdictions, the enforcement of information protection laws seems rarely to involve meting out penalties in the form of fines or imprisonment.

8.4.4 The authorities pride themselves on the effectiveness of their conciliatory approach, pointing out that they have to resort to hard enforcement measures in only a very limited number of cases. A variety of other means of remedying recalcitrance - most notably dialogue and, if necessary, public disclosure via the mass media - seem to be preferred instead. In other words, information protection laws often function to a relatively large extent as soft law, ie law which works by persuasion, is enforced by shame and punished by blame.[63] However, the outcomes may be more in line with compromises than a solution imposed on the basis of a purely legal ruling.[64] It would appear that if the authority has a "stick behind the door" it can be more forceful in such attempts at "conciliation".[65]

8.4.5 The benefit of giving advice is that it gives organisations the heads-up, often early in the design phase, and before major commitment of funds, of privacy risks or roadblocks. It is furthermore pro-active and often more systemic in nature than a complaints-handling focus. There is, however, the risk that advice-giving raises the litigation risk of a claim of pre-judgment, or bias, where a complaint is later made about the matter.[66]

(b) Evaluation

8.4.6 Commentators were, in general, in favour of an advisory approach combined with a pro-active systemic handling of problematic issues. The Bill makes provision for conciliation and mediation as part of the Regulator's duties.[67]

8.4.7 It was, however, emphasised that advisory powers, on its own, would not be sufficient to

---

63 Bygrave ***Data Protection*** at 79 and references therein.

64 Korff ***Comparative Study*** at 207.

65 Ibid; Thus the CNIL in France has, on occasion, imposed strict conditions on processing operations which could not lawfully commence until an "opinion" has not been issued by the authority. The threat of formal action (eg the issuing of a "preliminary" enforcement notice in the UK) have been used effectively to "persuade" a data user to accept the solution "proposed" by the authority.

66 Loukidelis D "Privacy Law Enforcement: The Experience in British Columbia Canada "Paper delivered at the APEC Symposium on Data Privacy Implementation: Developing the APEC Privacy Framework, Santiago, Chile, February 2004.

67 See also discussion in Chapter 7 above.

ensure the proper protection of personal information.[68]

(c) Recommendation

8.4.8 The Commission recommends that the proposed Bill should be pro-active in nature, focussing on ensuring that proper systems are put in place in stead of only policing encroachments. Mediation and conciliation should be used as a first step to resolve disputes between responsible parties and data subjects. However, should mediation and conciliation prove to be ineffective, a system of notices with binding effect is proposed.[69]

8.5 Enforcement powers

a) Proposals in the Discussion paper[70]

---

68 Nedbank.

69 See par 8.5.

70 **Information notice**

81. (1) If the Commissioner-
(a) has received a request under section 80 in respect of any processing of personal information, or
(b) reasonably requires any information for the purpose of determining whether the responsible party has interfered or is interfering with the protection of the personal information of a person, it may serve the responsible party with a notice (in this Act referred to as "an information notice") requiring the responsible party, within such time as is specified in the notice, to furnish the Commission, in such form as may be so specified, with such information relating to the request or to compliance with the principles as is so specified.

(2) An information notice must contain -
(a) in a case falling within subsection (1)(a), a statement that the Commission has received a request under section 80 in relation to the specified processing, or

(b) in a case falling within subsection (1)(b), a statement that the Commission regards the specified information as relevant for the purpose of determining whether the responsible party has complied, or is complying, with the information protection principles and his reasons for regarding it as relevant for that purpose.

(3) An information notice must also contain particulars of the rights of appeal conferred by section 85.

(4) Subject to subsection (5), the time specified in an information notice must not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(5) If by reason of special circumstances the Commission considers that the information is required as a matter of urgency, it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion; and in that event subsection (4) must not apply, but the notice must not require the information to be furnished before the end of the period of seven days beginning with the day on which the notice is served.

(6) A person must not be required by virtue of this section to furnish the Commissioner with any information in respect of -

(a) any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act, or

(b) any communication between a professional legal adviser and his client, or between such an adviser or his client and

any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the court) and for the purposes of such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser include references to any person representing such a client.

(8) A person shall not be required by virtue of this section to furnish the Commissioner with any information if the furnishing of that information would, by revealing evidence of the commission of any offence other than an offence under this Act, expose him to proceedings for that offence.

(9) The Commissioner may cancel an information notice by written notice to the person on whom it was served.

(10) After completing the assessment the Commission has to report to the responsible party the results of the assessment and any recommendations that the Commission considers appropriate and where appropriate a request, that within a time specified therein, notice be given to the Commission of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(11) The Commission may make public any information relating to the personal information management practices of an organisation if the Commission considers it in the public interest to do so.

Parties to be informed of result of investigation

82. Where any investigation is made following a complaint, and the Commission in its discretion does not believe that an action in terms of section 63 has taken place and hence do not serve an enforcement notice, the complainant must be informed accordingly as soon as reasonably practicable after the conclusion of the investigation and in such manner as the Commission thinks proper, of the result of the investigation.

Enforcement notice

83.(1) If the Commission is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a person, the Commission may serve the responsible party with a notice (in this Act referred to as "an enforcement notice") requiring the responsible party to do either or both of the following -
(a) to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified, or
(b) to refrain from processing any personal information, or any personal information of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified.

(2) An enforcement notice must contain -
(a) a statement indicating the nature of the interference with the protection of the personal information of the person and the reasons for reaching that conclusion, and
(b) particulars of the rights of appeal conferred by section 85.

(3) Subject to subsection (4), an enforcement notice must not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(4) If by reason of special circumstances the Commission considers that an enforcement notice should be complied with as a matter of urgency it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion; and in that event subsection (3) must not apply but the notice must not require the provisions of the notice to be complied with before the end of the period of seven days beginning with the day on which the notice is served.

Cancellation of enforcement notice

84.(1) A person on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal can be brought against that notice, apply in writing to the Commission for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the information protection principle or principles to which that notice relates.

(2) If the Commission considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the information protection principle or principles to which it relates, it may cancel or vary the notice by written notice to the person on whom it was served.

Right of appeal

85. A person on whom an information or enforcement notice has been served may appeal to the any court of competent jurisdiction for cancellation or variation of the notice within thirty days.

8.5.1 It is often contended that the ability to negotiate with data users is facilitated by the existence of enforcement powers, even if those powers are rarely used. Moreover, government and business organisations need certainty and consistency in the application of information protection rules. The provision of a formal order-making process assures a greater level of consistency, transparency and accountability over time in the implementation of the law.[71]

8.5.2 The Directive is silent on whether or not oversight authorities shall be able to impose fines and order compensation for damages, though such competence would clearly be compatible with the Directive. The Directive, furthermore, also does not specifically address whether or not these authorities must be given competence to issue legally binding orders. [72]

8.5.3 Authorities may usually order remedial action - usually subject to an appeal to a court or a special tribunal, although often information can be blocked by the authority, or processing stopped pending such an appeal in urgent cases in which there is a serious threat to the rights and interests of individuals. In addition, in many countries, the authorities can impose administrative fines. Again, such formal actions are, in practice, used only as a very last resort.[73]

8.5.4 The law in most countries provide for the imposition, by the national information protection authorities, of a range of formal sanctions seeking to force data users to comply with the law.[74]

8.5.5 Examples of different enforcement procedures are as follows:

Consideration of appeal

86.(1) If on an appeal under section 85 the court considers-
(a) that the notice against which the appeal is brought is not in accordance with the law, or
(b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,
the court must allow the appeal or substitute such other notice or decision as could have been served or made by the Commissioner; and in any other case the court must dismiss the appeal.

(2) On such an appeal, the court may review any determination of fact on which the notice in question was based.

71 In the UK fines may be levied on controllers (responsible parties) convicted of an offence.

72 Bygrave ***Data Protection*** at 72. Article 28 (3) of the Directive, read in conjunction with recitals 9-11 tends to suggest that such competence is required but the wording is not entirely conclusive. Authorities are to be given "effective powers of intervention".

73 Korff ***Comparative Study*** at 208.

74 Ibid.

a) In France, the French Information Commission (CNIL) can refuse to issue a "receipt" of a registered operation, or order changes to a processing operation on the basis of the findings of an investigation.[75]

b) The New Zealand Privacy Commissioner reaches opinions concerning breaches of the Act after investigating complaints (and also conciliates) but only the Human Rights Review Tribunal can make binding decisions.[76]

c) The Australian federal Privacy Commissioner is unusual in having powers under the Privacy Act 1988 (Cth) that allow him or her both to mediate complaints, and to make "determinations" under section 52[77] that respondents should provide various remedies, including that they should pay monetary compensation. A de novo hearing before a Court is necessary in order to enforce a determination (section 55A) but the determination is prima facie evidence of the facts on which it is based. (section 55B).[78]

d) In the UK the Data Protection Act 1998 gives the Commissioner powers of enforcement whilst also providing for a number of criminal offences under the Act. The Commissioner therefore has powers and functions pertaining to notification, enforcement, prosecution of offenders and powers of entry and inspection all set out in the relevant sections of the Act.

A system of enforcement notices provide for three forms of notice, being:

(i) the enforcement notice;
(ii) the information notice; and
(iii) the special information notice.

Under section 40, if the Commissioner is satisfied that the responsible party (data controller) has contravened or is contravening any of the information protection principles, he or she may serve a notice requiring the responsible party (data controller)

---

75 Ibid.

76 Greenleaf presentation 2002 at 9.

77 See section 52 (4) of the federal Privacy Act.

78 Greenleaf presentation 2002 at 11.

to take or refrain from taking specified steps within a specified time and to refrain from processing any personal information, personal information of a specified description; or for a specified purpose or purposes or in a specified manner, after a specified time.

In deciding whether to serve a notice, any personal damage or distress caused or likely to be caused has to be taken into account. The provisions as to the service of enforcement notices are subject to restrictions as regards processing for special purposes (journalism, literary and artistic purposes as set out in the Act).[79]

The Act also makes provision for the Data Protection Tribunal. The purpose of the Tribunal is primarily to hear appeals from data controllers in respect of notices served by the Commissioner or determinations made by the Commissioner as to whether processing is for special purposes. A data subject, however, does not have a right to appeal to the Tribunal against a decision of the Commissioner.

8.5.6 It is important to note that the enforcement functions of the authority should always be subject to judicial overview and indeed in appropriate cases, to prior judicial authorisation (such as the issuing of a warrant). There should furthermore be safeguards in place to ensure that the law is applied both equally (with all responsible parties being treated alike) and in such a way as to fully uphold data subject rights. This means that full information on all enforcement actions of the authorities should be publicly available and that data subjects are always fully informed of the outcome of any complaints, and involved in the process. In cases of disagreement, effective and effectively available judicial remedies should be at the disposal of all interested parties.[80]

b) Evaluation

8.5.7 Most commentators were in agreement that it should be an offence to process personal information without prior notification in terms of the proposed Bill, unless exempted from notification. There was agreement that liability should be strict and in agreement with the enforcement provisions in Chapter 6,8 and 9 of the Discussion

---

79 For a discussion of information notices, see para 7.3 above.

80 Korff ***Comparative Study*** at 201.

Paper Bill.[81]

Clause 63: *Interference with the protection of the personal information of a person*

8.5.8 One commentator[82] supported the inclusion of subpara (b) as suggested in fn 14 of the Bill.[83] It was noted that, in terms of the Discussion Paper Bill, if a private or public data controller (responsible party) acts wrongfully in terms of the information protection principles (as listed above), ordinary delictual remedies apply and fault should not be required in actions for satisfaction or damages, both of which are available to the prejudiced person[84]. Section 63 has been phrased to impose strict liability if a person's action breaches an information privacy principle, or fails to comply with a specific section mentioned. Given the consequences of section 63 (Interference with the protection of the personal information of a person), namely an investigation by the Commission, or the issuing of a warrant including a search and seizure warrant, and the issuing of an enforcement notice, and particularly given the provisions relating to payment of damages under section 87 (which are phrased such that damages could flow from a civil action against "any responsible party who has contravened or not complied with any provision of this Act"), the view was expressed that it would be fair and equitable to incorporate those elements of the New Zealand Act in order to balance the right to privacy against other factors (including potential defences). The claim for delictual damages would then have to be substantiated by evidence of the actual infringement of the right.

---

81 Kwa Zulu Natal Society of Advocates.

82 SNO Communications (Pty) Ltd.

83 Footnote 14 to clause 63(c) of the Discussion Paper Bill states as follows:

"The New Zealand definition includes subparagraph (b) set out below. Comment is invited.

1(1)For the purpose of this Part of the Act, an action is an interference with the privacy of a person if-
(a) in relation to that person,-
(i) the action breaches an information privacy principles; or
(ii) the provisions of Part X of this Act (which relates to information matching) have not been complied with; and
(b) the action has-
(i) caused, or may cause, loss, detriment, damage, or injury to that person; or
(ii) adversely affected, or may adversely affect, the rights, benefits, privileges, obligations or interests of that person; or
(iii) resulted in, or may result in, significant humiliation, significant loss of dignity, or significant injury to the feelings of that person."

84 Page 34 of the Discussion Paper at paragraph 2.3.54.

8.5.9 Another commentator[85] stated that the draft statute generally does not seem to cover the issues of breach of data privacy as fully as it could. It was suggested that the US Gramm-Leach-Bliley Act is an example of more specific and tighter control of personal financial information that could perhaps be included. The Privacy Act should include something akin to the financial privacy rule and the safeguards rule contained in the Gramm-Leach-Bliley Act to correct this lacuna.

Appeals procedure

8.5.10 In so far as the appeals procedure is concerned the following submissions were made:

* Clarification was sought as to which court is referred to in the phrase "any court of competent jurisdiction" and when the 30 days within which the appeal must be lodged will commence.[86]
* It was argued that the right of appeal in this clause should lie in relation to all matters under the Bill where the Commission takes action.[87]
* The question was posed whether the wording in clause 86 was wide enough to enable a Court to use its inherent jurisdiction to set aside an enforcement notice.[88]

c) Recommendation

8.5.11 The Commission confirms its proposals as set out in the Discussion Paper Bill. The Regulator should be authorised to enforce the legislation, using as a first step, a system of notices. The Regulator will, therefore, be empowered to make a determination that a responsible party must take specified action, or cease acting in a specific manner, within a specified period for the purpose of complying with the legislation. Failure to comply with the notices will be a criminal offence. The Bill will, therefore, make provision

---

85 Law Society of South Africa.

86 Department of Communications.

87 SNO Communications (Pty) Ltd.

88 SAIA.

for binding orders, subject to appeal to the courts. See also the discussion on compliance-orientated regulation in Chapter 7 above. See the proposed legislative enactment in clauses 90 to 93 on page 609 below.

8.6 Courts/judicial remedies

a) Proposals in the Discussion paper[89]

8.6.1 Ultimate redress in most countries is vested in the courts, and each law outlines the circumstances under which disputes might be reviewed at the judicial level.[90] Recital 55 of the

---

89 **CHAPTER 9**
OFFENCES AND PENALTIES

Obstruction of Commission

88. Any person who hinders, obstructs or unduly influences the Commission or any person acting on behalf or under the direction of the Commission in the performance of the Commission's duties and functions under this Act, is guilty of an offence.

Obstruction of execution of warrant

89. Any person who-

(a) intentionally obstructs a person in the execution of a warrant issued under section 73,or

(b) fails without reasonable excuse to give any person executing such a warrant such assistance as he may reasonably require for the execution of the warrant,

is guilty of an offence.

Failure to comply with enforcement or information notices

90.(1) A person who fails to comply with an enforcement notice served in terms of section 83, is guilty of an offence.

(2) A person who, in purported compliance with an information notice -
(a) makes a statement which he knows to be false in a material respect, or
(b) recklessly makes a statement which is false in a material respect,
is guilty of an offence.

Penal sanctions

91. Any person convicted of an offence in terms of this Act, is liable -
(a) in the case of a contravention of section 88, to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment; or
(b) in any other case, to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and imprisonment.

Magistrate's Court jurisdiction to impose penalties

92. Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in section 91.

90 Bennett and Raab ***The Governance of Privacy*** at 117.

EU Directive makes provision for judicial remedies.[91] Article 22 of the EU Directive[92] provides for judicial remedies for data subjects.

8.6.2 In the EU Directive, Article 24[93] permits sanctions to be imposed in case of infringement of the provisions adopted pursuant to the Directive.

8.6.3 All the EU members' laws contain extensive penal provisions, making most actions contrary to the information protection law a criminal offence, punishable by fines (or in serious aggravated case, eg where the offence was committed for gain, by **imprisonment)**. They also allow for the possibility of criminal prosecution of company directors. They adopt somewhat different formal procedures. For instance, in the UK and Ireland criminal sanctions are largely linked to "enforcement notices" which can be issued by the information protection authorities, and which are subject to appeal,[94] while other countries rely on denunciations of wrongdoers by the national authority to the prosecuting authorities, or allow the information protection authorities themselves to bring the prosecutions. These differences reflect the different legal cultures in the Member States; they do not detract from the in-principle availability of penal sanctions in all of them.[95]

8.6.4 Criminal prosecutions are, however, extremely rare. In the UK the annual level of prosecutions is about 55, of which 30 have in the past been for the offence of non-registration (now not prescribed anymore). Criminal prosecutions are reserved for the most obstinate or crass law breakers such as companies which continue to maintain unregistered information bases in spite of repeated warnings, which export information in spite of such warnings or formal notices, or people who knowingly flout the law by selling confidential personal information (eg

---

91 Recital 55 of the EU Directive which states as follows:
Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy: whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeur: whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

92 See footnote 11 above.

93 Article 24: **Sanctions**
The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

94 Sections 40 and 48 of the UK Data Protection Act,1998.

95 Korff ***Comparative Study*** at 181.

policemen who obtain access to criminal records or other confidential information on behalf of unauthorised third parties).[96]

8.6.5 It would not be unreasonable to say that the main function of the formal sanctions is to strengthen the hand of the authority during negotiations. In some countries, most notably Spain, the information protection authorities have, however, in the last few years, begun to enforce the law more strictly, by imposing very substantial fines of up to Euro 60,000. [97]

8.6.6 In the belief that the courts are not necessarily the most suitable institutions to deal with comparatively specialised and technical issues, some countries have established small tribunals, ad hoc groups of experts that perform a quasi-judicial function.[98] In Britain, for example, the 1998 Data Protection Act establishes a Data Protection Tribunal to which individuals or data users may appeal a decision of the Information Commissioner. This body is constituted from a panel of experts as necessary. In New Zealand, an aggrieved individual may appeal a finding of the Privacy Commissioner to the Complaints Review Tribunal established under the Human Rights Commission Act of 1977.[99]

b) Evaluation

8.6.7 It was argued that the penalty provided for in clause 91(a) of the Discussion Paper Bill is too excessive for a wide provision, such as clause 88 (dealing with the offence of obstruction of the Commission), since any offence, however minor, could possibly fall within the ambit of clause 88. It was proposed that a lesser penalty (eg five (5) years) may be more appropriate.[100]

8.6.8 It was, furthermore, noted that the concepts "hinder" and "obstruct" in clause 88 in this context are clear. However, it is unclear what the words "unduly influences" exactly means, or when legitimate representation or lobbying by interested parties becomes an "undue influence."

---

96 Korff ***Comparative Study*** at 209.

97 Ibid.

98 Bennett and Raab ***The Governance of Privacy*** at 118.

99 Section 82 of the New Zealand Privacy Act, 1993.

100 Provincial Administration, Western Cape; SNO Telecommunications.

It was recommended that the words "or unduly influences" be deleted.[101]

c) Recommendation

8.6.9 The Commission decides to confirm the proposals set out in the Discussion Paper Bill. Provision is made for any person on which an information or enforcement notice has been served, to appeal to the Court for a cancellation or variation of the notice. However, failure to comply with the notices, in the absence of an appeal, will be a criminal offence.

8.6.10 Other offences described in the Bill are firstly, the obstruction of the Commission, and secondly, the obstruction of the execution of a warrant. The penalty for the obstruction of the Commission is a fine or imprisonment for a period not exceeding ten years and for all the other offences, it is a fine or imprisonment for a period of 12 months or both. For the legislative enactment of these provisions, see Chapter 11 on page 612 below.

8.7 Compensation

a) Proposals in the Discussion Paper[102]

---

101 Banking Association.

102 **Civil remedies**

87. (1) Either the data subject(s), or the Commission, at the request of the data subject(s), may institute civil action in any court of competent jurisdiction against any responsible party who has contravened or not complied with any provision of this Act for payment of -
(a)an amount determined by the Court as compensation for patrimonial and non-patrimonial damages suffered by the data subject(s) in consequence of such contravention or non-compliance;
(b)an amount, for compensatory or punitive purposes, in a sum determined in the discretion of the Court but not exceeding three times the amount of any profit or gain which may have accrued to the person involved as a result of any such act or omission;
(c)interest; and
(d)costs of suit on such scale as may be determined by the Court.

(2) Any amount recovered by the Commission in terms of subsection (1) must be deposited by the Commission directly into a specially designated trust account established by the Commission with an appropriate financial institution, and thereupon-

(a)the Commission is, as a first charge against the trust account, entitled to reimbursement of all expenses reasonably incurred in bringing proceedings under subsection (1) and in administering the distributions made to the person(s) in terms of subsection (4);
(b)the balance, if any (hereinafter referred to as the 'distributable balance') must be distributed by the Commission to the person(s) referred to in subsection (4), any funds remaining, accruing to the Commission in the Commission's official capacity.

(3) Any amount not claimed within three years from the date of the first distribution of payments in terms of subsection (2), accrues to the Commission in the Commission's official capacity.

8.7.1 Article 23[103] of the EU Directive provides for compensation to the data subjects who have suffered damage.

8.7.2 All the EU Member States allow for the possibility of data subjects seeking redress, and corrective action, through the courts. This includes the possibility for data subjects to obtain damages by means of court action. There are, however, differences with regard to the kinds of damages for which a claim may be lodged and the way in which provision is made for exculpatory provisions specified by the Directive.[104]

8.7.3 Responsible parties may be exempted from this liability, in whole or in part, if they prove that they are not responsible for the event giving rise to the damage.[105] Examples of situations where the responsible party may be exempted are where the data subject was at fault, or in the case of force majeur.[106]

8.7.4 In the Netherlands the law says that the level of damages can be reduced depending on the extent to which the person being sued can be held accountable for the damage - this matter is to be determined in accordance with the ordinary rules on full or partial liability. [107]

---

(4) The distributable balance must be distributed on a pro rata basis to the data subject(s) referred to in subsection (1): Provided that no money may be distributed to a person who has contravened or failed to comply with any provision of this Act.

(5) A Court issuing any order under this section must order it to be published in the Gazette and by such other appropriate public media announcement as the Court considers appropriate.

(6) Any civil proceedings instituted under this section may be withdrawn, abandoned or compromised, but any agreement or compromise must be made an order of Court and the amount of any payment made in terms of any such compromise must be published in the Gazette and by such other public media announcement as the Court considers appropriate.

(7) Where civil proceedings have not been instituted, any agreement or settlement (if any) may, on application to the Court by the Commission after due notice to the other party, be made an order of Court and must be published in the Gazette and by such other public media announcement as the Court considers appropriate.

103 Article 23: **Liability**

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

104 Korff ***Comparative Study*** at 180.

105 Article 23 (20) fn 103 above. See also Roos thesis at 631, fn 472.

106 Recital para (55) of the EU Directive.

107 Ibid.

8.7.5 In the UK, too, the law provides for compensation for damage caused as a result of any failure on the part of a responsible party to comply with the law[108] - but the law is more restrictive as concerns "distress" (ie immaterial damage) than as concerns (material) damage: the former can only be awarded if material damage has been proven. In practice, few claims are ever made.[109] It is a defence for a responsible party (data controller) against such proceedings to prove that he or she had taken reasonable care to comply with the requirement in question (ie that he or she did not act wrongfully as a result of impossibility as a ground for justification).[110]

8.7.6 Under the USA Privacy Act actual damages can be claimed provided that the individuals can prove that the agency acted wilfully or intentionally and that the agency action affected them adversely.[111]

8.7.7 In South African law, fault is generally required for delictual liability. Strict liability (liability without fault) occurs as an exception to the general rule in limited instances only. An argument has been made in the Discussion Paper for establishing strict liability in actions for either satisfaction for non-patrimonial loss or compensation for patrimonial loss, where wrongful data processing caused the data subject harm.[112]

8.7.8 The other elements of a delict, namely conduct, wrongfulness, causation and harm, should of course still be present. Liability for the plaintiff can therefore be excluded by the presence of a ground of justification, or of defences such as vis major and fault on the part of the plaintiff.[113]

---

108 Section 13(1) of the Data Protection Act 1998.

109 Korff ***Comparative Study*** at 180.

110 Roos thesis at 631, fn 472.

111 Roos thesis at 631 and the reference to 5 USC section 552a(g)(4).

112 Clause 87 of the Discussion Paper Bill. Neethling 2002 ***THRHR*** 574, 584 provides the following reasons for this argument:

a)The collection and use of personal information (especially by means of electronic data banks) poses a serious threat to an individual's personality;
b)It is difficult to prove fault on the part of the responsible party;
c)The individual's right to privacy, which is protected as a fundamental right in the Bill of Rights, deserves th greatest measure of protection against unlawful data processing;
d)Strict liability serves as an encouragement for the data processing industry to act with as much care as possible;
e)The data processing industry is, from an economic point of view, in the best position to absorb and distribute the burden of harm.

113 Roos thesis at 631 and the reference to Neethling, Potgieter &Visser ***Delict*** 365.

b) Evaluation

8.7.9 The opinion was expressed that since the Commission is independent in the performance of its functions, it is suggested that such independence and related characteristics will be compromised severely if the Commission is authorised to institute civil actions against responsible parties on behalf of data subjects. The Commission should rather be perceived as an independent and objective entity, which may assist the court to reach fair and equitable determinations.[114]

8.7.10 It was stated that it would be considered inappropriate for an order of the Court to be published in the Gazette. This should be an ordinary legal decision which should be published in the relevant Law Reports.[115]

8.7.11 It was submitted that clause 87(1)(b) was impractical since it would be difficult to calculate "the amount.., not exceeding three times the amount of profit or gain which may have accrued to the person involved...". The opinion was expressed that an applicant must prove the loss he has suffered.[116]

8.7.12 One commentator argued that the term " patrimonial and non-patrimonial damages" was foreign to the South African legal system and that the word "damages" should suffice.[117]

8.7.13 It was argued that civil remedies (damages) should be imposed only in a case where there is proof of actual patrimonial or non-patrimonial damages suffered by the data subject (or other relevant party). The concept of "compensatory or punitive damages" in addition to or in the absence of, patrimonial and non-patrimonial damages is a concept that is relatively unknown as a form of legislative punishment or redress.[118] Inclusion of such a provision opens the door to vexatious claims by individuals seeking to make a quick profit and risks exposing responsible

---

114 SABRIC.

115 SAIA.

116 Department of Communications.

117 Department of Communications.

118 Vodacom (Pty) Ltd; SNO Communications (Pty)Ltd; SAIA.

parties to crippling amounts of false claims.[119]

8.7.14 The exact nature of the concept of "punitive damages" have been the subject of recent discussion. The argument has been put forward[120] that, although, at common law, the actio iniuriarum had a penal character, under the courts it has developed a dual function, namely to claim satisfaction, firstly as compensation (solatium) for injured feelings as a result of an intentional violation of personality rights, and secondly as a punishment (punitive damages) to assuage the plaintiff's feelings of outrage for the injustice he suffered.[121] However, it is extremely difficult in practice to distinguish between the compensatory and penal elements[122] and valid criticism has been levelled by academics[123] and the courts[124] against awarding punitive damages in a civil action.

8.7.15 It has, therefore, been submitted that aggravating compensatory damages should be used to do the work of punitive damages. In terms of this argument the increased amount of damages afforded is therefore not regarded as punishment for the defendant's conduct, but rather as compensation for outraged feelings. In this way justice is still done to the true concept of satisfaction.[125]

---

119 Banking Association.

120 Neethling J "The Law of Delict and Punitive Damages" 2008 ***Obiter***. (hereafter referred to as Neethling "Punitive Damages").

121 See eg ***Pauw v African Guarantee and Indemnity Co Ltd*** 1950 (2) SA 132 (SWA) 135 where the court stated: "Under the actio injuriarum damages are given in the form of a solatium for injured feelings and as a punishment of the defendant in order to assist in salving the injured feelings of the plaintiff"; See Neethling "Punitive Damages" at 3 and the references made therein.

122 See reference in Neethling "Punitive Damages" at 6 to Ackermann J in ***Fose v Minister of Justice*** 1997 (3) SA 786 (CC) 822 where he states "it is not always easy to draw the line between an award of aggavated but still basically compensatory damages, where the particular circumstances of or surrounding the infliction of the injuria have justified a substantial award, and the award of punitive damages in the strict and narrow sense of the word". See also Burchell JM ***The Law of Defamation in South Africa*** (1985) passim as referred to by Neethling "Punitive Damages" at 6.

123 Neethling "Punitve Damages" at 12 refers to Van der Walt JC's argument that penal features is foreign to the law of delict, since it is the criminal law that should punish and discourage conduct. He, furthermore, notes that Van der Merwe and Olivier suggests that the penal character of the actio iniuriarum should be relinquished.

124 See ***Dikoko v Mokhatla*** 2006 (6) SA 235 (CC) 263 where Mokgoro J states as follows: "...Even if a compensatory award may have a deterrent effect, its purpose is not to punish. Clearly, punishment and deterrence are functions of the criminal law.....In our law a damages award therefore does not serve to punish for the act of defamation. It principally aims to serve as compensation for damage caused by the defamation, vindicating the victim's dignity, reputation and integrity."

125 Neethling "Punitive Damages" at 10 explains that three dogmatic viewpoints can be discerned amongst South African writers: Firstly, Visser et al supports the view that the idea of punishment is inherent in the concept of satisfaction for personality infringement. The true concept of satisfaction is impossible and meaningless without the idea of somehow punishing the perpetrator; Criticism has, however, been levelled against this idea by academics and the courts; The third view, therefore, opts for a reconciliation of these two diametrically opposed viewpoints by accepting that there may be aggravating circumstances that may increase the amount awarded as compensation. The distinction between punitive and compensatory elements therefore becomes blurred.

c) Recommendation

8.7.16 The Commission recommends that provision should be made for a data subject to institute a civil action for damages against a responsible party for breach of any provision of the Bill.

8.7.17 It further recommends that a court may, apart from compensatory damages for patrimonial and non-patrimonial loss, also award aggravated damages that are just and equitable. The Commission, therefore, decides to change the word "punitive damages", as originally stated in the Discussion Paper Bil, to make provision for "aggravated damages" in clause 94(2) (b).

8.7.18 It should be noted that the meaning of the expression "punitive (penal) damages" is damages awarded to punish the defendant. Aggravated damages, on the other hand, may include punitive damages but may basically only be compensatory damages and may therefore differ from punitive damages.

8.7.19 The calculation referred to in clause 87(1)(b) of the Discussion Paper Bill has been omitted and the new clause 94(2) refers only to " an amount that is just and equitable".

8.7.20 Specific provision has been made to exclude the liability of the responsible party where a ground of justification or other defence is present.

8.8 Conclusion

8.8.1 The proposed legislation reads as follows:

CHAPTER 10

ENFORCEMENT

Interference with the protection of the personal information of a data subject

70. For the purposes of this Chapter, interference with the protection of the personal information of a data subject consists, in relation to that data subject, of -

(a) any breach of the information protection principles set out in Chapter 3 of this Act;

(b) non-compliance with any of sections 21, 47, 66, 67, 68 and 69;

(c) a breach of the provisions of a code of conduct issued in terms of section 57.

Complaints

71. Any person may submit a complaint to the Regulator in the prescribed manner and form-

(a) alleging interference with the protection of the personal information of a data subject; or

(b) in terms of subsection 61(3) if the data subject is aggrieved by the determination of an adjudicator.

Mode of complaint to Regulator

72.(1) A complaint to the Regulator may be made either orally or in writing.

(2) A complaint made orally must be put in writing as soon as reasonably practicable.

(3) The Regulator must give such reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Regulator, to put the complaint in writing.

Investigation by Regulator

73.(1) The Regulator, after receipt of a complaint made in terms of section 71, must --

(a) investigate any alleged interference with the protection of the personal information of a data subject in the prescribed manner;

(b) act, where appropriate, as conciliator in relation to any such interference in the prescribed manner; and

(c) take such further action as is contemplated by this Chapter of this Act.

(2) The Regulator may, on its own initiative, commence an investigation under subsection (1) of this section.

Action on receipt of complaint

74.(1) On receiving a complaint under this Chapter of this Act, the Regulator may -

(a) investigate the complaint; or

(b) decide, in accordance with section 75 of this Act, to take no action on the complaint.

(2) The Regulator must, as soon as is reasonably practicable, advise the complainant and the responsible party to whom the complaint relates of the procedure that the Regulator proposes to adopt under subsection (1) of this section.

Regulator may decide to take no action on complaint

75.(1) The Regulator, after investigating a complaint received in terms of section 71, may decide to take no action or, as the case may require, no further action, in respect of the complaint if, in the Regulator's opinion -

(a) the length of time that has elapsed between the date when the subject-matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(b) the subject-matter of the complaint is trivial;

(c) the complaint is frivolous or vexatious or is not made in good faith;

(d) the complainant does not desire that action be taken or, as the case may be, continued;

(e) the complainant does not have a sufficient personal interest in the subject-matter of the complaint; or

(f) in cases where the complaint relates to a matter in respect of which a code of conduct is in force and the code of conduct makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.

(2) Notwithstanding anything in subsection (1), the Regulator may in its discretion decide

not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Regulator that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

(3) In any case where the Regulator decides to take no action, or no further action, on a complaint, the Regulator must inform the complainant of that decision and the reasons for it.

Referral of complaint to regulatory body

76.(1) If, on receiving a complaint under this part of the Act, the Regulator considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body, the Regulator must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned.

(2) If the Regulator determines that the complaint should be dealt with by another body as described above, the Regulator must forthwith refer the complaint to this body to be dealt with accordingly and must notify the complainant of the action that has been taken.

Pre-investigation Proceedings of Regulator

77. Before proceeding to investigate any matter under this Chapter of this Act, the Regulator must, in the prescribed manner, inform -

- *(a) the complainant, the data subject to whom the investigation relates (if not the complainant) and any person alleged to be aggrieved (if not the complainant), of the Regulator's intention to conduct the investigation; and*
- *(b) the responsible party to whom the investigation relates of the --*
  - *(i) details of the complaint or, as the case may be, the subject-matter of the investigation; and*
  - *(ii) right of that responsible party to submit to the Regulator, within a reasonable time, a written response in relation to the complaint or, as the case may be, the subject-matter of the investigation.*

Settlement of complaints

78. If it appears from a complaint, or any written response made in relation to a complaint under section 77(b)(ii) of this Act, that it may be possible to secure a settlement between any of the parties concerned and, if appropriate, a satisfactory assurance against the repetition of any action that is the subject-matter of the complaint or the doing of further actions of a similar kind by the person concerned, the Regulator may, without investigating the complaint or, as the case may be, investigating the complaint further, in the prescribed manner, use its best endeavours to secure such a settlement and assurance.

Investigation proceedings of the Regulator

79. For the purposes of the investigation of a complaint the Regulator may -

(a) summon and enforce the appearance of persons before the Regulator and compel them to give oral or written evidence on oath and to produce any records and things that the Regulator considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Regulator sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, subject to section 80, enter and search any premises occupied by a responsible party;

(e) converse in private with any person in any premises entered under section 82 subject to section 80; and

(f) otherwise carry out in those premises any inquiries that the Regulator sees fit in terms of section 80.

Issue of warrants

80.(1) A Judge of the High Court, a regional magistrate or a magistrate, if satisfied by information on oath supplied by the Regulator that there are reasonable grounds for suspecting that -

(a) a responsible party is interfering with the protection of the personal information of a data subject, or

(b) an offence under this Act has been or is being committed,

and that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, that are within the jurisdiction of that judge or magistrate,

may, subject to subsection 2, grant a warrant to enter and search such premises.

(2) A warrant issued under subsection (1) authorises the Regulator or any of its officers or staff, subject to section 82, at any time within seven days of the date of the warrant to enter the premises as identified in the warrant, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal information and to inspect and seize any record, other material or equipment found there which may be such evidence as is mentioned in that sub-section.

Requirements for issuing of warrant

81.(1) A Judge or magistrate must not issue a warrant under section 80 unless satisfied -

(a) that the Regulator has given seven (7) days' notice in writing to the occupier of the premises in question demanding access to the premises;

(b) that either -

(i) access was demanded at a reasonable hour and was unreasonably refused, or

(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by any of the Regulator's members or officers or staff to permit the members or the officer or member of staff to do any of the things referred to in section 80(2), and

(c) that the occupier, has, after the refusal, been notified by the Regulator of the application for the warrant and has had an opportunity of being heard on the question whether the warrant should be issued.

(2) Subsection (1) does not apply if the judge or magistrate is satisfied that the case is one of urgency or that compliance with those provisions would defeat the object of the entry.

(3) A judge or magistrate who issues a warrant under section 80 must also issue two copies of it and certify them clearly as copies.

Execution of warrants

82.(1) A person executing a warrant issued under section 80 may use such reasonable force as may be necessary.

(2) A warrant issued under this section must be executed at a reasonable hour unless it

appears to the person executing it that there are reasonable grounds for suspecting that the evidence in question would not be found if it were so executed.

(3) If the person who occupies the premises in respect of which a warrant is issued under section 76 is present when the warrant is executed, he or she must be shown the warrant and supplied with a copy of it; and if that person is not present a copy of the warrant must be left in a prominent place on the premises.

(4) A person seizing anything in pursuance of a warrant under section 80 must give a receipt to the occupier or leave it on the premises.

(5) Anything so seized may be retained for so long as is necessary in all the circumstances but the person in occupation of the premises in question must be given a copy of any documentation that is seized if he or she so requests and the person executing the warrant considers that it can be done without undue delay.

(6) A person authorised to conduct an entry and search in terms of section 80 must be accompanied and assisted by a police officer.

(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard for each person's right to dignity, freedom, security and privacy.

(8) A person who enters and searches premises under this section, before questioning any person -

- *(a) must advise that person of the right to be assisted at the time by an advocate or attorney; and*
- *(b) allow that person to exercise that right.*

Matters exempt from search and seizure

83. If the Regulator has authorised the processing of personal information in terms of section 34, that information is not subject to search and seizure empowered by a warrant issued under section 80.

Communication between legal adviser and client exempt

84.(1) Subject to the provisions of this section, the powers of search and seizure conferred by a warrant issued under section 80 must not be exercised in respect of -

(a) any communication between a professional legal adviser and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights; or

(b) any communication between a professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the court) and for the purposes of such proceedings.

(2) Subsection (1) applies also to -

(a) any copy or other record of any such communication as is there mentioned; and

(b) any document or article enclosed with or referred to in any such communication if made in connection with the giving of any advice or, as the case may be, in connection with or in contemplation of and for the purposes of such proceedings as are there mentioned.

Objection to search and seizure

85. If the person in occupation of any premises in respect of which a warrant is issued under this Act objects to the inspection or seizure under the warrant of any material on the ground that it -

(a) contains privileged information and refuses the inspection or removal of such article or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the registrar of the High Court which has jurisdiction or his or her delegate, to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not; or

(b) consists partly of matters in respect of which those powers are not exercisable, he or she must, if the person executing the warrant so requests, furnish that person with a copy of so much of the material as is not exempt from those powers.

Return of warrants

86. A warrant issued under this section must be returned to the court from which it was issued-

(a) after being executed; or

(b) if not executed within the time authorised for its execution;

and the person who has executed the warrant must make an endorsement on it stating what powers have been exercised by him or her under the warrant.

Assessment

87.(1) The Regulator, on its own initiative, or at the request by or on behalf of the responsible party, data subject or any other person must make an assessment in the manner prescribed, whether an instance of processing of personal information complies with the provisions of this Act.

(2) The Regulator must make the assessment if it appears to be appropriate, unless, where the assessment is made on request, it has not been supplied with such information as it may reasonably require in order to -

(a) satisfy itself as to the identity of the person making the request, and

(b) enable it to identify the action in question.

(3) The matters to which the Regulator may have regard in determining whether it is appropriate to make an assessment include the extent to which the request appears to it to raise a matter of substance, and if the assessment is made on request -

(a) any undue delay in making the request; and

(b) whether or not the person making the request is entitled to make an application under Principle 8 (access) in respect of the personal information in question.

(4) If the Regulator has received a request under this section it must notify the requester -

(a) whether it has made an assessment as a result of the request; and

(b) to the extent that it considers appropriate, having regard in particular to any exemption from Principle 8 applying in relation to the personal information concerned, of any view formed or action taken as a result of the request.

Information notice

88.(1) If the Regulator -

(a) has received a request under section 87 in respect of any processing of personal information; or

(b) reasonably requires any information for the purpose of determining whether the responsible party has interfered or is interfering with the protection of the personal information of a data subject;

it may serve the responsible party with a notice (in this Act referred to as "an information notice") requiring the responsible party to furnish the Regulator, within a specified period, in a form specified in the notice, with an independent auditor's report indicating that the processing is taking place in compliance with the provisions of the Act, or with such information relating to the request or to compliance with the Act as is so specified.

(2) An information notice must contain particulars of the rights of appeal conferred by section 92, and -

(a) in a case falling within subsection (1)(a), a statement that the Regulator has received a request under section 87 in relation to the specified processing; or

(b) in a case falling within subsection (1)(b), a statement that the Regulator regards the specified information as relevant for the purpose of determining whether the responsible party has complied, or is complying, with the information protection principles and the reasons for regarding it as relevant for that purpose.

(3) Subject to subsection (5), the period specified in an information notice must not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that the information is required as a matter of urgency, it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require the information to be furnished before the end of a period of three days beginning with the day on which the notice is served.

(6) An information notice may not require a responsible party to furnish the Regulator with any of the following information -

(a) any communication between a professional legal adviser and his or her client in connection with the giving of legal advice on the client's obligations, liabilities or

rights under this Act; or

(b) any communication between a professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the court) and for the purposes of such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser include any person representing such a client.

(8) An information notice may not require a responsible party to furnish the Regulator with information that would, by revealing evidence of the commission of any offence other than an offence under this Act, expose the responsible party to criminal proceedings.

(9) The Regulator may cancel an information notice by written notice to the responsible party on whom it was served.

(10) After completing the assessment referred to in section 87 the Regulator -

(a) must report to the responsible party the results of the assessment and any recommendations that the Regulator considers appropriate; and

(b) may, in appropriate cases, require the responsible party, within a specified time, to inform the Regulator of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(11) The Regulator may make public any information relating to the personal information management practices of a responsible party that has been the subject of an assessment under this section if the Regulator considers it in the public interest to do so.

(12) A report made by the Regulator under section 88(10) is deemed to be the equivalent of an enforcement notice served in terms of section 90 of this Act.

Parties to be informed of developments during and result of investigation

89. If an investigation is made following a complaint, and -

a) the Regulator believes that no interference with the protection of the personal information of a data subject has taken place and therefore does not serve an enforcement notice;

b) an enforcement notice is served in terms of section 90 ;

c) a served enforcement notice is cancelled in terms of section 91;

d) an appeal is lodged against the enforcement notice for cancellation or variation of the notice in terms of section 92; or

e) an appeal against an enforcement notice is allowed, the notice is substituted or the appeal is dismissed in terms of 93,

the Regulator must inform the complainant and the responsible party, as soon as reasonably practicable, in the manner prescribed of any new development in and the result of the investigation.

Enforcement notice

90.(1) If the Regulator is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject, the Regulator may serve the responsible party with a notice (in this Act referred to as "an enforcement notice") requiring the responsible party to do either or both of the following -

(a) to take specified steps within a period specified in the notice, or to refrain from taking such steps; or

(b) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice.

(2) An enforcement notice must contain -

(a) a statement indicating the nature of the interference with the protection of the personal information of the data subject and the reasons for reaching that conclusion; and

(b) particulars of the rights of appeal conferred by section 92.

(3) Subject to subsection (4), an enforcement notice may not require any of the provisions of the notice to be complied with before the end of the period within which an appeal may be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that an enforcement notice should be complied with as a matter of urgency it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require any of the provisions of the notice to be complied with before the end of a period of three days beginning with the day on which the notice is served.

Cancellation of enforcement notice

91.(1) A responsible party on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal may be brought against that notice, apply in writing to the Regulator for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the information protection principles.

(2) If the Regulator considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the information protection principle or principles to which it relates, it may cancel or vary the notice by written notice to the responsible party on whom it was served.

Right of appeal

92.(1) A responsible party on whom an information or enforcement notice has been served may, within thirty (30) days of receiving the notice, appeal to the High Court having jurisdiction for the setting aside or variation of the notice.

(2) A complainant, who has been informed of the result of the investigation in terms of section 75(3) or section 91, may, within thirty (30) days of receiving the result, appeal to the High Court having jurisdiction against the result.

Consideration of appeal

93.(1) If in an appeal under section 92 the court considers -

(a) that the notice against which the appeal is brought is not in accordance with the law; or

(b) to the extent that the notice involved an exercise of discretion by the Regulator, that it ought to have exercised its discretion differently;

the court must allow the appeal and may set aside the notice or substitute such other notice or decision as should have been served or made by the Regulator.

(2) In such an appeal, the court may review any determination of fact on which the notice in question was based.

Civil action for damages

94.(1) A data subject, or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act in terms of section 70, whether or not there is intent or negligence on the part of the responsible party.

(2) In the event of a breach the responsible party may raise any of the following defences against and action for damages -

(a) vis major;

(b) consent on the part of the plaintiff;

(c) fault on the part of the plaintiff;

(d) compliance was not reasonably practicable in the circumstances of the particular case; or

(e) the Regulator authorised the breach in terms of section 34 of this Act.

(3) A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable including -

(a) for payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;

(b) aggravated damages, in a sum determined in the discretion of the Court;

(c) interest; and

(d) costs of suit on such scale as may be determined by the Court.

(4) Any amount awarded to the Regulator in terms of subsection (3) must be dealt with in the following manner -

(a) the full amount must be deposited into a specially designated trust account established by the Regulator with an appropriate financial institution;

(b) as a first charge against the amount, the Regulator may recover all reasonable expenses incurred in bringing proceedings at the request of a data subject in terms of subsection (1) and in administering the distributions made to the data subject(s) in terms of subsection (5);

(c) the balance, if any remaining (referred to as the 'distributable balance') must be distributed by the Regulator to the data subject(s) at whose request the proceedings were brought.

(5) Any amount not distributed within three (3) years from the date of the first distribution of payments in terms of subsection (2), accrues to the Regulator in the Regulator's official capacity.

(6) The distributable balance must be distributed on a pro rata basis to the data subject(s) referred to in subsection (1).

(7) A Court issuing any order under this section must order it to be published in the Gazette and by such other appropriate public media announcement as the Court considers appropriate.

(8) Any civil action instituted under this section may be withdrawn, abandoned or compromised, but any agreement or compromise must be made an order of Court.

(9) If civil action has not been instituted, any agreement or settlement (if any) may, on application to the Court by the Regulator after due notice to the other party, be made an order of Court and must be published in the Gazette and by such other public media announcement as the Court considers appropriate.

CHAPTER 11
OFFENCES AND PENALTIES

Obstruction of Regulator

95. Any person who hinders, obstructs or unlawfully influences the Regulator or any person acting on behalf or under the direction of the Regulator in the performance of the Regulator's duties and functions under this Act, is guilty of an offence.

Breach of confidentiality

96. Any person who contravenes the provisions of section 47 is guilty of an offence.

Obstruction of execution of warrant

97. Any person who-

(a) intentionally obstructs a person in the execution of a warrant issued under section 80; or

(b) fails without reasonable excuse to give any person executing such a warrant such assistance as he may reasonably require for the execution of the warrant;

is guilty of an offence.

Failure to comply with enforcement or information notices

98.(1) A responsible party which fails to comply with an enforcement notice served in terms of section 90, is guilty of an offence.

(2) A responsible party which, in purported compliance with an information notice -

(a) makes a statement knowing it to be false in a material respect, or

(b) recklessly makes a statement which is false in a material respect;

is guilty of an offence.

Penal sanctions

99. Any person convicted of an offence in terms of this Act, is liable -

(a) in the case of a contravention of section 95, to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment; or

(b) in any other case, to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and imprisonment.

Magistrate's Court jurisdiction to impose penalties

100. Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in section 99.

CHAPTER 9: COMPARATIVE LAW [1]

9.1 Introduction

9.1.1 It is important to learn from the experiences of other countries.[2] In conducting comparative research it would, however, be dangerous to translate the experiences of other countries directly into your own law. Key areas of possible divergence which may have an influence on the data privacy model to be chosen may, for instance, include:[3]

- the legal framework and the protection afforded to data privacy;[4]
- cultural attitudes to openness and privacy and the role of the government;[5]
- historical events, which may have left an indelible impression on public attitudes to privacy;[6] and
- population size, which has an impact on the ease with which projects can be

---

1 Unless otherwise indicated, the information reflected in this Chapter is based on extracts from the Country Reports in Electronic Privacy Information Center (EPIC) in association with Privacy International ***Privacy and Human Rights 2003*: *An International Survey of Privacy Laws and Developments*** as updated in ***Privacy and Human Rights 2004 and 2006: An International Survey of Privacy Laws and Developments*** and the references therein. These annual reports published in the USA by EPIC and Privacy International, review the state of privacy in over seventy five countries around the world. It outlines legal protections for privacy, new challenges, and summarises important issues and events relating to privacy and surveillance. An electronic version of the report is available at http://www.privacyinternational.org/. See also http://www.epic.org/.

2 This Chapter only seeks to provide a broad outline of the information protection systems found in each of the different countries noted. Detailed comparisons between comparable jurisdictions can be found, where appropriate, under the specific subject headings in the Chapters above.

3 ***PIU Privacy and Data Sharing Report***" at 18.

4 Some countries may have a common law jurisdiction, as opposed to civil law elsewhere. Federal countries laws, standards or targets at the national level may differ from those covering provinces or regions. Overall frameworks may differ. While the US data protection law gives less protection to the citizen than EU laws, there is a specific tort of privacy, through which US citizens are able to sue in respect of breach of their privacy.

5 In Sweden it is accepted that everyone's tax return can be inspected by anyone who cares to do so. Similarly, in many countries it is accepted that drivers should carry their licence with them at all times, whereas it is a hotly debated topic in some other countries.

6 Dutch government files listing religious affiliation were used by the Nazis to identify Jews. So a reasonably innocent proposal concerning information on religion may nevertheless touch a nerve there.

implemented.[7]

9.1.2 Even taking into account these influences, it is clear that there has been a harmonisation in the implementation of information protection principles and that the international nature of these principles has already promoted, and will also in future promote, the development of global standards.

9.2 International Directives[8]

9.2.1 The first data protection laws in the world were enacted in the seventies.[9] By last count in 2002 there were already over thirty countries which had enacted data protection statutes at national or federal level. The number of such countries is steadily growing.[10]

9.2.2 Important international instruments evolved from these laws, most notably the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[11] and the 1981 Organisation for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[12]

9.2.3 These two agreements have had a profound effect on the enactment of laws around the world. Nearly thirty countries have signed the CoE convention. The OECD guidelines have also been widely used in national legislation, even outside the OECD member countries.

---

7 If a country already has a national ID card, it is relatively straightforward to issue a smart card version with functionality for public key cryptography. In the absence of such a pre-existing framework, however, options are more limited.

8 See discussion with regard to international instruments in paras 1.2.13 and 4.1 above.

9 An analysis of these laws is found in Flaherty D ***Protecting Privacy in Surveillance Societies*** University of North Carolina Press 1989.

10 Bygrave ***Data Protection*** at 30.

11 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 1981.

12 OECD Guidelines.

9.2.4 The Convention is the hereto sole international treaty dealing specifically with data protection. It entered into force on 1 October 1985.[13] The Convention is potentially open for ratification by States that are not members of the CoE;[14] concomitantly it is also envisaged to be potentially more than an agreement between European states. As yet, though it has not been ratified by any non-member states.[15]

9.2.5 The Convention is not intended to be self-executing. Article 4(10) of the Convention simply obliges Contracting States to incorporate the Convention's principles into their domestic legislation; individual rights cannot be derived from it.[16]

9.2.6 The OECD Guidelines incorporate eight principles relating to the collection, purpose, use, quality, security and accountability of organisations in relation to personal information. However, the OECD Guidelines do not set out requirements as to how these principles are to be enforced by member nations. As a result, OECD member countries have chosen a range of differing measures to implement the privacy principles.

9.2.7 In 1995, the European Union enacted the Data Protection Directive[17] in order to harmonise member states' laws in providing consistent levels of protection for citizens and ensuring the free flow of personal data within the European Union.

9.2.8 Articles 25 and 26 of the Directive stipulates that personal data should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection" (the so-called safe-harbour principles).[18]

---

13 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** at 9. It has been ratified by 30 CoE Member states.

14 Article 23.

15 Bygrave ***Data Protection*** at 32.

16 Bygrave ***Data Protection*** at 34.

17 EU Directive.

18 For further discussion see Chapter 6 above.

9.2.9 The Directive sets a baseline common level of privacy that not only reinforces current data protection law, but also establishes a range of new rights. The Directive contains strengthened protections over the use of sensitive personal data relating, for example, to health, sex life or religious or philosophical beliefs. In future, the commercial and government use of such information will generally require "explicit and unambiguous" consent of the data subject. The directive applies to the processing of personal information in electronic and manual files.[19] It provides only a basic framework which will require to be developed in national laws.[20]

9.2.10 The Directive was adopted with member states being required to implement its provisions by October 24, 1998. This time-table has proven difficult for Member States to comply with.

9.2.11 Some account should also be taken of the UN Guidelines.[21] The Guidelines are intended to encourage those UN Member States without information protection legislation in place to take steps to enact such legislation based on the Guidelines. The Guidelines are also aimed at encouraging governmental and non-governmental international organisations to process personal information in a responsible, fair and privacy-friendly manner. The Guidelines are not legally binding and seem to have had much less influence on information regimes than the other instruments.[22]

9.2.12 The Commonwealth Law Ministers have furthermore proposed that model legislation (Model Bills) to implement the Commonwealth commitment to freedom of information should be enacted for both the public and the private sectors.

9.2.13 The intent of the proposed model legislation is to ensure that governments and private organisations accord personal information an appropriate measure of protection, and also that such information is collected only for appropriate purposes and by appropriate means. The model seeks,

---

19 See par 3.3, Ch 3 above.

20 As referred to in Strathclyde LLM at 4. A good example is the Directive's requirement that member states shall appoint an independent supervisory agency. The particular form of the agency is not specified.

21 United Nations Guidelines Concerning Computerised Personal Data Files adopted by the UN General Assembly on 14 December 1990 .

22 Bygrave ***Data Protection*** at 33.

in accordance with general practice in member countries, only to deal with information privacy which is the most common aspect of privacy regulated by statute and which involves the establishment of rules governing the collection and handling of personal information such as those relating to status of credit or medical records. It also seeks to create a legal regime which can be administered by small and developing countries without the need to create significant new structures.[23]

9.2.14 In February 2003, Australia put forward a proposal for the development of APEC (Asia-Pacific Economic Cooperation) Privacy Principles, using the OECD Guidelines as a starting point.[24] The APEC ministers endorsed the APEC Privacy Framework on November 16, 2005. The Framework covers implementation mechanisms, including cross-border cooperation in investigation and enforcement and cooperative development of cross-border privacy rules.[25]

9.2.15 Although the expression of data protection in various declarations and laws varies, all require that personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.

These principles are known as the “Principles of Data Protection” and form the basis of both legislative regulation and self-regulating control.

---

23 The Law Ministers commended the Model law for the public sector as a useful tool which could be adopted to meet the particular constitutional and legal positions in member countries.

24 A Privacy Sub Group was set up comprising of Australia, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States.

25 Government of the United States of America submission on Discussion paper 109 (hereafter “USA submission”). See also discussion on APEC in Chapter 4 above.

9.3 United States of America[26]

9.3.1 The United States Constitution does not explicitly mention a right to privacy.[27] The Supreme Court has, however, ruled that there is a limited constitutional right of privacy based on a number of provisions in the Bill of Rights. This includes a right to privacy from government surveillance into an area where a person has a "reasonable expectation of privacy" [28] and also in so far as marriage, procreation, contraception, family relationships, child rearing and education are concerned.[29] Ten states within the country have incorporated explicit privacy protection in their constitutions.[30]

9.3.2 Two characteristics of American constitutional law should be kept in mind: Firstly, Constitutional rights are usually not applicable unless "state action" can be found. This means that the rights created by the Constitution protect the individual from the government and not from private entities. Secondly, the rights created by the Constitution are "negative rights" - they prevent certain kinds of governmental action, but place no affirmative duties on the state to protect the constitutional rights of individuals by actions such as the adoption of legislation. There is, therefore, no duty on the government to actively protect an individual against the invasion of his or her informational privacy rights.[31]

9.3.3 The Privacy Act of 1974 regulates the information practices of federal agencies. It requires

---

26 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** (as updated in 2004 and 2006) and the references made therein. See also the discussion regarding the self-regulatory system of the USA in para 7.2(a)(ii) in Chapter 7 above.

27 US submission stated as follows: Although it is correct that the U.S. Constitution does not "explicitly"include a right to privacy, it is now generally accepted that the U.S. Constitution does protect privacy (see the recent confirmation hearings of U.S. Supreme Court Chief Justice Roberts and Justice Alito for example), but debate remains over the limits of that protection (especially on matters not related to informational privacy).

28 ***Katz v United States*** 389 U.S. 347 (1967).

29 See e.g., ***Griswold v Connecticut***, 381 U.S. 479 (1965); ***Whalen v Roe*** 429 United States 589 (1977); ***Paul v Davis*** 424 U.S. 714 (1976).

30 Alaska; Arizona; California; Florida; Hawaii, Illinois; Louisiana; Montana; South Carolina and Washington.

31 Roos thesis at 38 and the references made therein; See, however, the US submission where it is stated that characterisation of constitutional rights as "negative rights" is misleading. It is argued that the U.S. Constitution is the supreme law of the land. The rights and protections provided in the Constitution (and likewise the state constitutions in the respective states) are themselves "positive" rights. Any governmental action, including legislation, that infringes those rights is constitutionally void.

agencies to apply basic fair information procedures.[32] The efficiency of the Act is, however, hampered by a weak remedial scheme and the lack of a proper information protection authority. Limits on the use of the Social Security Number have also been undercut in recent years because of wide-spread use of the identifier among governmental agencies and because the private sector employs the identifier for both identification and authentication purposes.[33]

9.3.4 The United States has no comprehensive privacy protection law for the private sector. The United States does, however, have a federal law that provides protection against the misuse of consumer data - the Federal Trade Commission Act (FTC Act). As a general consumer protection statute that prohibits unfair or deceptive acts or practices, it gives the Federal Trade Commission (FTC) authority to file cases against companies that are engaged in unfair or deceptive acts or practices in the area of consumer privacy. [34]To supplement the FTC Act, various federal laws cover some specific categories of personal information. These include financial records,[35] credit reports,[36] video rentals,[37] cable television,[38] children's (under age 13) online activities,[39] educational records,[40] motor vehicle registrations,[41] and telemarketing.[42]

9.3.5 There is no independent information protection authority in the United States. Oversight takes place on different levels, namely by the head of an agency, the Office of Management and Budget, the US President, Congress and the courts:

---

32 Privacy Act, Pub. L. No. 93-579 (1974), codified at 5 USC § 552a,.

33 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 1008 and the references made therein*.*

34 US submission.

35 Right to Financial Privacy Act, Pub. L. No. 95-630 (1978).

36 Fair Credit Reporting Act, Pub. L. No. 91-508 (1970), amended by PL 104-208 (1996).

37 Video Privacy Protection Act**,** Pub. L. No. 100-618 (1988).

38 Cable Privacy Protection Act, Pub. L. No. 98-549 (1984).

39 Children's Online Privacy Protection Act (COPPA), Pub. L. No. 105-277(1988) passed by Congress in 1998 and requiring parental consent before information is collected from children under the age of 13. It went into effect in April 2000; See also Center for Media Education, A Parent's Guide to Online Privacy.

40 Family Educational Rights and Privacy Act, Public Law 93-380, 1974.

41 Drivers Privacy Protection Act, PL 103-322, 1994.

42 Telephone Consumer Protection Act, PL 102-243, 1991.

- The Office of Management and Budget (OMB)[43]plays a limited role in setting policy for federal agencies under the Privacy Act, but it has not been particularly active or effective.[44] In a submission received form the US Government on Discussion paper 109 this fact was, however, disputed. It was submitted that privacy and security of data are important elements of planning, acquisition, and management of Federal Information technology systems. The Federal Information Security Management Act (FISMA) for eg provides significant privacy and security responsibilities for federal information technology system operators. Agencies report annually to the OMB and Congress on the effectiveness of their security programs in terms of the Act.[45]
- The Consolidated Appropriations Act of 2005[46] requires every federal agency to appoint its own privacy officer.
- In July 2007 the Government Accountability Office released a report on the progress of the Department of Homeland Security Privacy Office in complying with its statutory mandate.
- The Federal Trade Commission has oversight and enforcement powers for the laws protecting children's online privacy, consumer credit information and fair trading practices.[47] In recent years, the FTC has focused on enforcing existing law in the areas of telemarketing, spam, pretexting and children's privacy.[48] In January 2002, the FTC proposed changes to the Telemarketing Sales Rule to tighten use of individuals' account numbers, and to create a national do-not-call list for individuals who wish to opt-out of telemarketing.[49] Enrolment began in June 2003, and now approximately 120 million numbers have been added to the list.[50]

---

43 Part of the executive office of the President.

44 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 1014 and further reference in ftnt 5524.

45 US submission.

46 Transportation, Treasury, Independent Agencies and General Government Appropriations Act 8522,Pub. L. No. 108-447 (2004) enacted on December 8, 2004.

47 See FTC web site at http://www.ftc.gov/privacy/index.html.

48 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 1015 and the references made therein.

49 The Proposed National "DO NOT CALL" Registry, Amendment to the Telemarketing Sales Rule, January 2002.

50 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein. See also US submission.

9.3.6 Since Article 25 of the EU Directive prohibits the transfer of personal information from EU countries to third countries without adequate information protection, fears were raised in the USA that the free flow of information between the US and Europe would be hampered. A safe-harbour agreement was subsequently negotiated in 2002 which consists of a set of information principles agreed upon by the USA and the European Commission with which all parties have to comply voluntarily.[51]

9.3.7 The Gramm-Leach-Bliley Act,[52] which eliminated traditional ownership barriers between different financial institutions such as banks, securities firms and insurance companies, set limited protections on financial information that is likely to be shared among merged institutions. The privacy provisions became effective in July 2001. There are three principal parts to the privacy requirements: the Financial Privacy Rule,[53] the Safeguards Rule[54] and the pretexting provisions.[55] The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule.[56]

9.3.8 Protections for medical records were introduced in the United States in 2001. In October 1999, the Department of Health and Human Services issued draft regulations protecting medical privacy. The final rules were issued on December 20, 2000 and went into effect in April 2001. The large number of exemptions provided limits to the protection offered by the new rules. For example, patients' information can be used for marketing and fundraising purposes. Doctors, hospitals, and health services companies will be able to send targeted health information and product promotions to individual patients and there is no opt-out right to limit this marketing use of medical data. In April

---

51 See discussion in Ch 6 above.

52 The Financial Services Modernisation Act of 1999, also known as the “Gramm-Leach-Bliley Act”.

53 The FPR governs the collection and disclosure of customer’s personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, which receive such information. Further information is available on the FTC web site http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm.

54 The SGR requires all financial institutions to design, implement and maintain safeguards to protect customer information. The SGR applies not only to financial institutions that collect information from their own customers, but also to financial institutions “such as credit reporting agencies” that receive customer information from other financial institutions.

55 The pretexting provisions protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as “pretexting”.

56 US submission.

2003, the first federal regulation protecting individually identifiable health information became effective for enforcement. The Standards for Privacy of Individually Identifiable Health Information, commonly known as the "HIPAA Privacy Rule," provide basic protections for individually identifiable health information and give individuals rights with respect to the information about them. [57]The federal Privacy Rule contains civil penalties for non-compliance and will be enforced by the Office for Civil Rights within the Department of Health and Human Services. The Rule also contains criminal penalties for malicious misappropriation and misuse of health information, which will be enforced by the Department of Justice.[58]

9.3.9 In 2003, Congress passed legislation significantly amending the Fair Credit Reporting Act (FRCA)[59] and the nation's first spam regulation.[60] In 2006, the Privacy and Civil Liberties Oversight Board was established. It is responsible for reviewing the terrorism information sharing practices of executive branch departments and agencies to determine whether guidelines designed to appropriately protect privacy and civil liberties are being followed.[61]

9.3.10 There is also a variety of sectoral legislation on the state level that may give additional protection to citizens of individual states. The tort of breach of privacy was first adopted in 1905 and all but two of the 50 states recognise a civil right of action for invasion of privacy in their laws.[62] A number of court cases have dealt with the protection of the right to privacy and data.[63]

---

57 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein.

58 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the reference made to EPIC's Medical Privacy web page available at http://www.epic.org/privacy/medical/.

59 Fair and Accurate Credit Transactions Act of 2003 (FACTA).See http://www.ftc.gov/os/statutes/031224fcra.pdf; EPIC Fair Credit Reporting Act page available at http://www.epic.org/privacy/frca/.

60 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (known as the CAN-SPAM Act). See discussion on spam in Chapter 5 above.

61 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 1026 and the references made therein.

62 See ***Lake v WalMart Stores, Inc***., 582 N.W.2d 231 (Minn. 1998), for a review of state adoption of common law privacy torts.

63 See discussion of the following cases in EPIC and Privacy International ***Privacy and Human Rights Report 2003*** at 522: In January 2000, the Supreme Court heard ***Reno v Condon***,528 U.S. 141 (2000). a case addressing the constitutionality of the Drivers Privacy Protection Act (DPPA), a 1994 law that protects drivers' records held by state motor vehicle agencies. In a unanimous decision, the Court found that the information was "an article of commerce" and can be regulated by the federal government. In June 2001, the Supreme Court ruled in the case of ***Kyllo v United States*** 533 U.S. 27 (2001) that the use of a thermal imaging device, without a warrant, to detect heat emanating from a person's residence constituted an illegal search under the Fourth Amendment. ***City of Indianapolis v Edmond***, 531 U.S. 32 (2000). In November 2000, the Supreme Court ruled held that suspicionless vehicle checkpoints, used to discover and interdict illegal narcotics, violate the Fourth Amendment. Also, in March 2001, the Supreme Court held that a state

9.3.11 There has been significant debate in the United States in recent years about the development of privacy laws covering the private sector:[64]

a) The **White House and the private sector** maintain that self-regulation is sufficient and that no new laws should be enacted except for a limited measure on medical and genetic information.

b) There have been many **efforts in Congress** to improve privacy. Since January 2001, there have been well over 100 bills introduced in the House and Senate.[65]

c) There is also **substantial activity in the states**. In recent years, Massachusetts and Hawaii have considered comprehensive privacy bills for the private sector. California passed a Social Security Number Bill that will prevent the printing of the identifier on forms, invoices, and identification badges. The Bill also gives individuals greater power to control their credit report once fraud is suspected. [66] Minnesota enacted a Bill that requires ISPs to give notice and obtain user authorisation before using personal information for secondary purposes. [67] In a statewide referendum, North Dakota residents established opt-in protections for financial information.[68] Additionally, Georgia enacted a privacy law that prohibits private businesses from

---

hospital cannot perform diagnostic tests to obtain evidence of criminal conduct without the patient's consent as such a test is unreasonable and violates the Fourth Amendment. ***Ferguson v City of Charlestown,*** 532 U.S. 67 (2000). In the 2001 term, the Supreme Court addressed anonymity, searches on buses, and student privacy. In *Watchtower Bibl*e, the Court invalidated a law that required registration with the government before individuals could engage in door-to-door solicitation. The Court held that a pre-registration requirement violated the First Amendment and individuals' right to anonymity. ***Watchtower Bible & Tract Soc'y of N.Y. v. Village of Stratton***, 122 S. Ct. 2080 (2002). In ***United States v Drayto*n,** the Court held that the Fourth Amendment does not require police officers to advise bus passengers of their right not to cooperate and to refuse consent to searches. ***United States v Drayton***, 122 S. Ct. 2105 (2002). Student privacy was diminished in a series of cases involving drug testing, "peer grading," the practice of allowing a fellow student to score a test, and the right to sue under a federal student privacy law. In *Earl*s, the Court held that random, suspicionless drug testing of students involved in non-athletic extracurricular activities was justified under the "special needs" exception to the Fourth Amendment. ***Board of Education v Earls***, 122 S. Ct. 2559 (2002). In *Falv*o, the Court held that both peer grading and the reporting aloud of peer grades did not violate the Family Educational Rights and Privacy Act of 1974 (FERPA).***Owasso Indep. Sch. Dist. No. I-011 v Falvo***, 534 U.S. 426 (2001). In *Gonzag*a, the Court held that the FERPA does not give individuals a right to sue for violations of privacy ***Gonzaga Univ. v Doe***, 122 S. Ct. 2268 (2002).

64 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** at 529 and the references as indicated below***.***

65 See EPIC Bill Track.

66 California Senate Bill 168.

67 Minnesota S.F. 2908.

68 Friery T "Privacy Alert: North Dakota Votes for 'Opt-In' Financial Privacy," Privacy Rights Clearinghouse, June 21, 2002.

discarding documents or computer components that contain personal information[69].

d) **Internet privacy** has remained the hottest issue of the past few years. A number of profitable companies, including eBay.com, Amazon.com, drkoop.com, and yahoo.com have either changed users' privacy settings or have changed privacy policies to the detriment of users. [70] A series of companies, including Intel and Microsoft, were discovered to have released products that secretly track the activities of Internet users. [71] Users have filed several lawsuits under the wiretap and computer crime laws. In several cases, TRUSTe, an industry-sponsored self-regulation watchdog group ruled that the practices did not violate its privacy seal program.

e) Additionally, an **official Homeland Security Agency[72]** has been created and private-sector corporations are collaborating to use commercial marketing data for terrorism profiling.[73]

f) Recent years have seen a new trend towards the increased use of **video surveillance** cameras linked with facial recognition software in public places. [74] [75]

g) There have been a number of proposals to create a **National ID**[76] in the wake of the

---

69 Georgia Senate Bill 475.

70 Hoofnagle CJ ***Consumer Privacy In the E-Commerce Marketplace 2002*** Third Annual Institute on Privacy Law Practicing Law Institute G0-00W2 (June 2002).

71 See Big Brother Inside Campaign.

72 H.R. 5005, Homeland Security Act of 2002.

73 See Letter from the Center for Information Policy Leadership to Interested Parties, 2002.

74 O'Harrow R "Matching Faces with Mugshots: Software for Police, Others Stir Privacy Concerns," ***Washington Post***, July 31, 2001 at A1. See also EPIC's page on Face Recognition.

75 This kind of technology was first used at the 2001 Super Bowl in Tampa, Florida to compare the faces of attendees to faces in a database of mug shots. Public usage of the technology then spread to the Ybor City district of Tampa, where the technology encountered much public opposition. In August 2001, the Tampa City Council held a vote on whether they should terminate their contract with Visionics, but they narrowly decided to keep using the software. Virginia Beach, Virginia, received funding in 2001 from the Virginia Department of Criminal Justice Services to install a system that can scan and process the facial images of tourists visiting the town. Face recognition technology is still not reliable and remain unregulated by United States laws. Studies sponsored by the Defense Department have also shown the system is right only 54% of the time and can be significantly compromised by changes in lighting, weight, hair, sunglasses, subject cooperation, and other factors. Declan McCullagh and Robert Zarate, "Scanning Tech a Blurry Picture", See also ***Wired News***, February 16, 2002; ,American Civil Liberties Union Press Release "Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws," May 14, 2002; and Hiawatha Bray "'Face Testing' at Logan is Found Lacking," ***Boston Globe***, July 17, 2002.

76 See also the recommendations of the National Commission on Terror Attacks Upon the United States (911 Commission) regarding the need for secure indentification in the US.

September terrorist attacks. [77] Most of these efforts have sought the creation of a national identification system through the standardisation of state driver's licenses.[78] [79]

h) Several other programmes have been initiated in the past few years, such as the US-VISIT,[80] SEVIS,[81] CAPPSII,[82] MATRIX[83] and TIA[84](discontinued).[85]

9.4 United Kingdom of Great Britain and Northern Ireland[86]

9.4.1 English common law does not recognise the right to privacy and the United Kingdom does not have a written constitution. In 1998, the Parliament approved the Human Rights Act to incorporate the European Convention on Human Rights into domestic law, a process that established an enforceable right of privacy. The Act came into force on October 2, 2000. A number of cases, many related to celebrity privacy, have been decided or are pending in the courts.

---

77 Kent SY and Millett L I ***IDs -- Not That Easy: Questions About Nationwide Identity Systems*** Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2002.

78 ***Your Papers Please: From A State Driver's License to a System of National Identification***, EPIC Report, February 2002.

79 A Bill to create a National ID has been introduced in the House, but a companion Bill has yet to be introduced in the Senate.H.R. 4633. There are also more limited attempts to create national identification systems through "enhanced visa" documents and "trusted traveler" programs.

80 United States Visitor and Immigrant Status Indicator Technology programme which requires visitors to the USA to submit a biometric identifier to the government.

81 The Student and Exchange Visitor Information System is an Internet-based system that allows schools to transmit student information to the government for purposes of tracking and monitoring non-immigrant and exchange students.

82 The Computer Assisted Passenger Pre-screening System aims to conduct background risk assessments on all air travellers before they fly on commercial airliners. The intention was to link CAPSS II and US-VISIT when both prgrammes are fully operational. CAPSII was abandoned by late 2004 and replaced by “Secure Flight”.

83 Multi-state Anti-Terrorism Information Exchange is available to law enforcement agents in participating states and combines public and private records from multiple databases with data analysis tools.

84 Total Information Awareness was a programme of the Defence Advanced Research Projects Agency (DARPA) that intended to scan ultra-large databases of personal information to detect the “information signature” of terrorists.

85 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein***.***

86 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** (as updated in 2004 and 2006) and the references made therein.

9.4.2 The information protection provided by this Act is, however, not significant and protection is therefore provided through specific legislation. The Parliament approved the Data Protection Act in July 1998. [87] The legislation, which came into force on March 1, 2000, replaced the 1984 Data Protection Act.[88] It implements the requirements of the European Union's Data Protection Directive. It creates eight data protection principles based on the EU Directive to be followed. The Act covers records held by government agencies and private entities. It provides for limitations on the use of personal information, access to and correction of records and requires that entities that maintain records register with the Information Commissioner.

9.4.3 The Office of the Information Commissioner (formerly known as the Data Protection Commissioner and the Data Protection Registrar), is an independent agency that enforces both the Data Protection and Freedom of Information Acts.[89] Statistics are published in the Annual Report.[90]

9.4.4 The Commissioner is also responsible for enforcing the Telecommunications (Data Protection and Privacy) Regulations. These regulations came into force on March 1, 2000 and over 25 percent of cases before the Commissioner involves them. The Information Commissioner released the final version of the Employment Practices Data Protection Code in June 2005 issued a code of guidance for employer/employee relationships.[91]

9.4.5 The Information Tribunal (formerly the Data Protection Tribunal) can hear appeals of decisions and notices. It has, however, made only 14 decisions relating to data protection since 1990.

9.4.6 There are also a number of other laws containing privacy components, most notably those

---

87 Data Protection Act 1998 (c. 29).

88 Data Protection Act 1984 (c. 35).

89 Home page of the Information Commissioner, <http://www.dataprotection.gov.uk/>.

90 As of 2006 there were 276 000 databases registered with the Commission; the agency received 22 059 new cases in 2005-2006; there were 26 cases forwarded for prosecutions.

91 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 991 and the references made therein.

governing medical records[92] and consumer credit information.[93] Other laws with privacy components include the Rehabilitation of Offenders Act of 1974, the Telecommunications Act of 1984 (as amended by the Telecommunications Regulations of 1999), the Police Act of 1997, the Broadcasting Act of 1996, Part VI and the Protection from Harassment Act of 1997. Some of these acts are amended and repealed in part by the 1998 Data Protection Act. The Crime and Disorder Act of 1998 provides for information sharing and data matching among public bodies in order to reduce crime and disorder. The Data Protection Commissioner issued a report on the privacy implications of the Act.[94]

9.4.7 It has been noted[95] that the privacy picture in the United Kingdom is decidedly grim. There is, however, at some levels, a strong public recognition and defence of privacy. On the other hand, crime and public order laws passed in recent years have placed substantial limitations on numerous rights, including freedom of assembly, privacy, freedom of movement, the right of silence, and freedom of speech.[96]

9.4.8 The Identity Cards Act was approved in March 2006 after years of contention. There has been no national ID card in the UK since 1952. The Act requires biometric technologies, establishes a central National Identity Register and makes provision for the issuing of "voluntary" ID cards.[97]

9.4.9 The United Kingdom is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)[98] and the European Convention for the Protection of Human Rights and

---

92 Access to Medical Reports Act 1988, Access to Health Records Act 1990, The Health and Social Care Act 2001.

93 Consumer Credit Act, 1974.

94 Crime & Disorder Act 1998: Data protection implications for information-sharing.

95 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 992 and the references made therein.

96 See Criminal Justice and Public Order Act 1994.

97 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 1003 and the references made therein.

98 Signed May 14, 1981; ratified August 26, 1987; entered into Force December 1, 1987.

Fundamental Freedoms.[99] In November 2001, the United Kingdom signed the Council of Europe Convention on Cybercrime.[100] The United Kingdom is a member of the Organisation for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

9.5 Kingdom of the Netherlands[101]

9.5.1 The Dutch Constitution was amended in 1983 to include art 10 which grants citizens an explicit right to privacy.[102]

9.5.2 In May 2000, the government-appointed Commission for Constitutional Rights in the Digital Age presented proposals for changes to the Dutch Constitution to make constitutional rights more technologically independent. The Commission was set up after confusion about the legal status of e-mail under the constitutionally protected privacy of letters. In November 2004 the Dutch government announced that proposals to amend the Constitution would be delayed in order to incorporate upcoming intended developments.[103]

9.5.3 The Wet Bescherming Persoonsgegevens (WBP)(Personal Data Protection Act) of 2000

---

99 Signed November 11, 1950; ratified March 8, 1951; entered into Force September 3, 1953.

100 Signed November 23, 2001.

101 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** (as updated in 2004 and 2006) and the references made therein.

102 Constitution of the Kingdom of the Netherlands 1989. Article 10 states:

"(1) Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.
(2) Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.
(3) Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament."

103 The Council of Europe's recommendation "Human Rights and the Rule of Law in the Information Society" was adopted by the Council of Europe on May 13, 2005.

was approved by the Parliament in June 2000[104]. This Act is a revised and expanded version of the 1988 Data Registration Act and brought the Dutch law in line with the European Data Protection Directive. It also regulates the disclosure of personal data to countries outside of the European Union. The sectoral codes of conduct still enjoy a considerable degree of popularity.[105] Most of the existing codes are currently under revision for adaptation to the new legislation.

9.5.4 The WBP establishes an independent information protection authority entitled the College Bescherming Persoonsgegevens (CBP) which exercises supervision of the operation of personal data files in accordance with the Act.[106] Previously known as the Registratiekamer, the CBP's functions have remained largely the same with the implementation of the new Act, although it has been given new powers of enforcement. It can now apply administrative measures and impose fines for non compliance with a decision. It can also levy fines of up to 4540 Euro for breach of the notification requirements. Otherwise, the CBP continues to advise the government, deal with complaints submitted by data subjects, institute investigations and make recommendations to controllers of personal data files. [107]

9.5.5 In its 2003 annual report the CBP expressed its concern "about the erosion in public debate of the fundamental principle laid down in international treaties that the use of personal data and violation of personal privacy should be an actual necessity".[108]

9.5.6 Two decrees have been issued under the Data Registration Act. The Decree on Sensitive Data [109] sets out the limited circumstances when personal data on an individual's religious beliefs,

---

104 Personal Data Protection Act, Staatsblad 2000 302, July 6, 2000, unofficial translation.

105 In terms of the now repealed Data Protection Act of 1988 provision was made for the possibility to develop a code of conduct as means of implementation and to request the Data Protection Authority for its approval. The decision of the authority was non-binding, but in practice often seen as a seal of good quality. Under this regime, twelve codes of conduct were officially approved, which covered major sectors like banking and insurance, direct marketing, health and pharmaceutical research. The relevant provision of the Act served as a model for Article 27 of Directive 95/46/EC, which provides for implementation via sectoral codes of conduct, both on the national and on the European level.

106 Homepage <www.cbpweb.nl>.

107 In 2006, the CPB investigated 394 complaints and dealt with 42 ex-officio investigations, 3 complaints concerning codes of conduct and 40 advisories to government on new legislation.

108 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein.

109 Decree on Sensitive Data, March 5, 1993.

race, political persuasion, sexuality, medical, psychological and criminal history may be included in a personal data file. The Decree on Regulated Exemption[110] exempts certain organisations from the registration requirements of the Data Registration Act.

9.5.7 There are also, inter alia, sectoral privacy laws regulating the Dutch police,[111] medical exams,[112] medical treatment[113] and social security.[114]

9.5.8 Recent developments include the passing, in May 2004, of the law on e-commerce (Wet elektronische handel) that implements the EU E-commerce Directive (2000/31/EC) and the coming into force of compulsory identification for all persons from the age of 14 (in January 2005) which is intended to increase public safety.[115]

9.5.9 The Netherlands is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).[116] It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms. In November 2001, the Netherlands signed the Council of Europe Convention on Cybercrime.[117] It is a member of the Organisation for Economic Cooperation and Development and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

---

110 Decree on Regulated Exemption, July 6, 1993.

111 Dutch Police Registers Act,1990.

112 Dutch Medical Examinations Act,1997.

113 Dutch Medical Treatment Act, 1997.

114 Dutch Social Security System Act, 1997.

115 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein.

116 Signed May 7, 1982; ratified May 28, 1993; entered into Force September 1, 1993.

117 Signed November 23, 2001.

9.6 New Zealand[118]

9.6.1 Article 21 of the New Zealand Bill of Rights Act, 1990 states "everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise." [119] The New Zealand Court of Appeal has interpreted this provision in several cases as protecting the important values and interests that make up the right to privacy.[120]

9.6.2 New Zealand's Privacy Act of 1993 came into force on July 1, 1993. It was preceded by the Privacy Commissioner Act, 1991 which established the office of Privacy Commissioner. It regulates the collection, use and dissemination of personal information across both the public and private sectors. It also grants to individuals the right to have access to personal information held about them by any agency. The Privacy Act applies to "personal information," which means that it is directly concerned with any information about an identifiable individual, whether automatically or manually processed. The news media are exempt from the Privacy Act in relation to their news activities.

9.6.3 The Act contains twelve Information Privacy Principles generally based on the 1980 Organization for Economic and Cooperation Development (OECD) Guidelines and the information privacy principles in Australia's Privacy Act 1988. In addition, the legislation includes a new principle that deals with the assignment and use of unique identifiers. The Information Privacy Principles can be individually or collectively replaced by enforceable codes of practice for particular sectors or classes of information. These codes may modify the application of any of the information protection principles or exempt any action from the principles.[121]

9.6.4 In addition to the information privacy principles, the legislation contains principles relating to information held on public registers; it sets out guidelines and procedures in respect to

---

118 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** (as updated in 2004 and 2006) and the references made therein.

119 Bill of Rights Act, 1990, Chapter 4, Section 21, available at <http://www.oefre.unibe.ch/law/icl/nz01000_.html>.

120 Tim McBride, "Recent New Zealand Case Law on Privacy: Part I: Privacy Act and the Bill of Rights Act," Privacy Law & Reporter, January 2000, at 107.

121 At present there are three complete sector-specific codes of practice in force: the Health Information Privacy Code 1994; the Telecommunications Information Privacy Code,2003 and the Credit Reporting Privacy Code, 2004.

information matching programs run by government agencies, and it makes special provision for the sharing of law enforcement information among specialized agencies.

9.6.5 The Office of the Privacy Commissioner is an independent Crown entity which oversees compliance with the Privacy Act 1993, but does not function as a central data registration or notification authority.[122]

9.6.6 Complaints by individuals are initially filed with the Privacy Commissioner who attempts to conciliate the matter.[123] The Commissioner regards the power to investigate and to require answers during investigations as "a vital element" in securing a high conciliation rate. When conciliation fails, the Director of Human Rights Proceedings[124] or the complainant (if the Director of Human Rights Proceedings is unwilling) can bring the matter before the Human Rights Review Tribunal, which can issue decisions and award declaratory relief, issue restraining or remedial orders, and award special and general damages up to NZD 200,000. The Privacy Commissioner reports to Parliament through the Minister of Justice under the Public Finance Act.

9.6.7 New Zealand is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

9.7 Canada[125]

9.7.1 There is no explicit right to privacy in Canada's Constitution and Charter of Rights and

---

122 Homepage <http://www.privacy.org.nz.

123 A total of 636 formal complaints were received during the 2005-2006 fiscal year which is 300 less than the previous year. The Privacy Commissioner's Office attributes the continuing downward trend in the number of formal complaints registered to proactive handling of complaints and more targeted privacy training.

124 The Director is an official appointed under the Human Rights Act of 1993.

125 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** (as updated in 2004 and 2006) and the references made therein.

Freedoms.[126] However, in interpreting section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, Canada's courts have recognised an individual's right to a reasonable expectation of privacy.[127]

9.7.2 Privacy is regulated at both the federal and provincial level. At the federal level, privacy is protected by two acts:

a) the 1982 federal Privacy Act; and

b) the 2001 Personal Information and Electronic Documents Act (PIPEDA).

9.7.3 The federal Privacy Act of 1982 (which took effect on July 1,1983) imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information.[128] It provides individuals with a right to access and request correction of personal information about themselves held by those agencies, subject to some exceptions.[129] Individuals can appeal to a federal court for review if access to their records is denied by an agency, but are not authorised to challenge the collection, use, or disclosure of information.[130] The Act is based on the OECD Guidelines and is thus broadly similar to EU data protection legislation except that it only applies to the public sector.[131]

9.7.4 The Personal Information Protection and Electronic Documents Act (PIPEDA) was approved

---

126 Canadian Charter of Rights and Freedoms*,* Part I of the Constitution Act*, 1982,* being Schedule B to the Canada Act *1982* (United Kingdom), 1982, c. 11, s. 8, online: Department of Justice (date accessed: 25 May 2002).

127 ***Hunter v Southam***, 2 S.C.R. 145, 159-60 (1984).

128 In June 2006, the Privacy Commissioner of Canada released a document entitled "Government Accountability for Personal Information" containing suggestions on reforming the Privacy Act.

129 Privacy Act, c. P-21.

130 In 1999, in order to tighten exemptions and loopholes, the Privacy Commissioner finished an extensive review of the Act and recommended over 100 changes to the law to improve and update it. Some of the changes included giving the Commission primary authority over all information collected by the federal government, extending its coverage beyond "recorded" information, increasing notice of disclosures, expanding court reviews, creating rules on data matching, controlling "publicly available" information and expanding the mandate of the Privacy Commissioner; Privacy Commissioner 1999-2000 Annual Report, May 2000.

131 Privacy and Data Sharing Report fn 2 at 20.

by Parliament in April 2000.[132] The Act adopts the CSA International Privacy Code (a national standard: CAN/CSA-Q830-96) into law for private sector organisations that process personal information "in the course of a commercial activity," and for federally regulated employers with respect to their employees. It does not apply to information collected for personal, journalistic, artistic, literary, or non-commercial purposes.

9.7.5 PIPEDA sets out the ground rules for the collection, use, disclosure, retention, and disposal of personal information. It sets out 10 privacy principles as standards that organisations must comply with when dealing with personal information including: accountability, purpose, openness, consent, limiting use and collection, disclosure, retention, individual access, safeguards, accuracy, and challenging compliance.

9.7.6 In January 2001, the Data Protection Working Party of the European Commission issued a decision stating that PIPEDA provided an adequate level of protection for certain personal information transferred from the European Union to Canada.[133] This will allow certain personal information to flow freely from the European Union to recipients in Canada subject to PIPEDA without additional safeguards being needed to meet the requirements of the European Union Data Protection Directive.

9.7.7 However, the Commission's decision of adequacy does not cover any personal information held by federal sector or provincial bodies or information held by personal organisations and used for non-commercial purposes, such as data handled by charities or collected in the context of an employment relationship.[134] For this, transfers to recipients in Canada, operators in the European Union will have to put in place additional safeguards, such as the standard contractual clauses adopted by the Commission in June 2001 before exporting the information.

---

132 Bill C-6, Personal Information Protection and Electronic Documents Act; PIPEDA applies throughout the country with the exception of three provinces (Alberta, British Columbia and Quebec) that have enacted "substantially similar" provincial legislation of their own. Four provinces (Ontario, Manitoba, Saskatchewan, Alberta) have passed legislation for the protection of information in the health sector.

133 European Union Article 29 Working Party, ***Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act***, January 26, 2001.

134 Commission Decision of December 20, 2001, Official Journal of the European Communities L 2/13.

9.7.8 Both the Privacy Act and PIPEDA are overseen by the independent Privacy Commissioner of Canada who is an Agent of Parliament and reports directly to the House of Commons and the Senate. [135] The Commissioner has the power to investigate, mediate, and make recommendations, but cannot issue orders or impose penalties. He or she also conducts periodic audits of federal institutions to determine compliance with the Privacy Act, and to recommend changes where necessary.

9.7.9 The Commissioner's powers under PIPEDA are very similar to those under the Privacy Act.

9.7.10 A number of the federal statutes address the privacy of personal information in specific sectors. The Bank Act,[136] Insurance Companies Act, [137] and Trust and Loan Companies Act[138] permit regulations regarding the use of information provided by customers. A poll in April 1999 found that 88 percent of people said the government should "not allow banks to use information about their customers' bank accounts and other investments to try to sell customers insurance."[139] There are sectoral laws for pensions,[140] video surveillance, [141] immigration, [142] and Social Security.[143] The Young Offenders Act [144] regulates the information that can be disclosed about offenders under the age of 18 while the Corrections and Conditional Release Act [145] speaks to the information that can be disclosed to victims and their families.

9.7.11 In May 2002 Canada became the first national government to make privacy assessments

---

135 In 2005-2006 the Privacy Commission received 1028 complaints and 6050 inquiries.

136 Bank Act**,** c. 46, ss. 242, 244, 459.

137 Insurance Companies Act, s. 489, s. 607.

138 Trust and Loan Companies Act, s. 444.

139 "88% of Canadians Oppose Banks Target-Marketing Insurance: Compass Poll," ***Canada Newswire***, April 27, 1999.

140 Canada Pension Plan, R.S.C. 1985, c. C-8, s. 104.07.

141 Criminal Code, c. C-46, s. 487.01.

142 Immigration Act, S.C. 1985, c. I-2, s. 110.

143 Old Age Security Act, c. O-9, s. 33.01.

144 Young Offenders Act, C. Y-1, s. 38.

145 Corrections and Conditional Release Act, 1992, c. 20, s. 26, 142.

of federal agencies mandatory. The Privacy Impact Assessment Policy means that all new and existing federal programmes with potential privacy risks will undergo a Privacy Impact Assessment (PIA).[146]

9.7.12 Canada is a member of the OECD and relied on the OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in the drafting of the federal Privacy Act of 1982. Canada also has observer status at the Council of Europe and although it was not a member, it was a key player in the negotiations on the Cybercrime Convention. It has signed, but not yet ratified the Convention. Canada is also a member of the Asia-Pacific Economic Community.

9.7.13 Privacy legislation on a provincial level is separated into three categories:

(a) public sector (data protection) law;

(b) private sector law; and

(c) sector-specific laws.

9.7.14 Public sector legislation covering government bodies exists in almost all provinces and territories.[147] Nearly every province has some sort of oversight body, but they vary in their powers and scope of regulation.

9.7.15 With respect to provincial sector-specific legislation, many provinces have specific laws to protect personal information, including health-specific privacy laws, consumer credit reporting laws, laws regulating information from credit unions, and legislation imposing restrictions on the disclosure of personal information held by private investigators and other professionals.[148]

---

146 EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein.

147 For a list of state laws and commissions see <http://infoweb.magi.com/~privcan/other.html>.

148 Alberta, Manitoba, and Saskatchewan have all passed health-specific privacy legislation, which sets rules for the collection, use, and disclosure of personal health information. These laws apply to personal health information held by hospitals, government ministries, regulated health professionals, and other health care facilities. Ontario is currently working on including health privacy legislation in its general private sector legislation. Sectoral laws, however, only provide a partial and fragmentary approach to the problem of regulation. Privacy Commissioner ***Report to Parliament on Substantially Similar Provincial Legislation***, May 2002.

9.8 Commonwealth of Australia[149]

9.8.1 Neither the Australian Federal Constitution[150] nor the Constitutions of the six States contain any express provisions relating to privacy. In 2004 the Australian Capitol Territory (ACT) became the first territory to incorporate a Bill of Rights. Section 12 of the Human Rights Act 2004 creates a right of ”privacy and reputation”.[151] The State of Victoria adopted a similar approach in 2006. The Constitution limits the legislative power of the Commonwealth (federal) government, with areas not expressly authorised being reserved for the States.

9.8.2 The constitutionality of federal laws imposing privacy rules on the private sector has been questioned, but not challenged so far. Most commentators believe that the Commonwealth could found any private sector privacy law on a 'cocktail' of constitutional powers including those giving authority over telecommunications, corporations and foreign affairs (e.g. treaties).

9.8.3 Privacy law in Australia comprises a number of Commonwealth (federal) statutes covering particular sectors and activities,[152] some State or Territory laws with limited effect, and the residual common law protections, which have very occasionally been used in support of privacy rights through actions for breach of confidence, defamation, trespass or nuisance.

9.8.4 The principal federal statute is the Privacy Act of 1988[153] which has four main areas of application, and which gives partial effect to Australia's commitment to the OECD Guidelines and to the International Covenant on Civil and Political Rights (ICCPR).

9.8.5 The Privacy Act provides for:

---

149 EPIC and Privacy International ***Privacy and Human Rights Report 2003*** (as updated in 2004 and 2006) and the references made therein.

150 The Commonwealth of Australia Constitution Act.

151 Section 12 states:
Everyone has the right -
(a) not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily; and
(b) not to have his or her reputation unlawfully attacked.

152 Such as the Telecommunications Act 1979 (Cth) which regulates the interception of telecommunications and the Crimes Act 1914 (Cth) which contains a variety of privacy-related measures including offences relating to unauthorised access to computers, interception of mail and telecommunications and the disclosure of Commonwealth government information.

153 Privacy Act 1988 (Cth).

a) eleven Information Privacy Principles (IPPs), based on those in the OECD Guidelines that apply to the activities of most federal government agencies.

b) a separate set of rules about the handling of consumer credit information, added to the law in 1989, that applies to all private and public sector organisations.

c) the monitoring of the processing of the government issued Tax File Number (TFN), by organisations authorised to record such information (the entire community is subject to Guidelines issued by the Privacy Commissioner which take effect as subordinate legislation).

9.8.6 The Privacy Act was extended by the Privacy Amendment (Private Sector) Act 2000 (Commonwealth) to cover the regulation of private sector organisations by the National Privacy Principles (NPPs), passed in December 2000 and which took effect in December 2001.

9.8.7 The law provides for ten National Privacy Principles (NPPs) based on the National Principles for Fair Handling of Personal Information originally developed by the Federal Privacy Commissioner in 1998 as a self-regulatory substitute for legislation. It applies to parts of the private sector and all the health service providers. Private companies are now required to observe these principles although they can apply to the Privacy Commissioner for approval of a self-developed Code of Practice containing principles that are an "overall equivalent" to the NPPs. The Act has been criticised as failing to meet international standards of privacy protection. [154]

9.8.8 It has been argued that the NPPs impose a lower standard of protection in several areas than the European Union Directive. For example:

a) organisations are required to obtain consent from customers for secondary use of their personal information for marketing purposes where it is "practicable"; otherwise, they can initiate direct marketing contact, providing they give the individual the choice to opt out of further communications;

b) controls on the transfer of personal information overseas are also limited, requiring only that organisations take "reasonable steps" to ensure personal information will be protected, or "reasonably believes" that the information will be subject to similar protection as applied under Australian law;

---

154 See Roger Clarke's Homepage <http://www.anu.edu.au/people/Roger.Clarke/>.

c) in addition, the Act provides for a number of broad exemptions for employee records (defined as a record of personal information relating to the employment of the employee including, for example, health information, contact details, salary or wages, performance and conduct, trade union membership, recreation and sick leaves, banking affairs etc); media organisations (defined to include organisations which provide information to the public and political parties); and small businesses (defined as receiving under $A3m annual turnover and not disclosing personal information for a benefit);[155]

d) there are also weaknesses in the enforcement regime including, for example, allowing privacy complaints to be handled by an industry-appointed code authority with limited oversight by the Privacy Commissioner.

9.8.9 The Act does, however, include an innovative principle of anonymity. Principle 8 states that: "Where it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation."

9.8.10 The Article 29 Data Protecting Working Party of the European Commission expressed many reservations about the Act in its report (dated March 2001), suggesting that it would not, as currently written, satisfy the adequacy test in Articles 25 and 26 of the European Union directive for data to flow to third countries.[156] The group recommended the introduction of additional safeguards to address these concerns.

9.8.11 In response, the Attorney General issued a press release stating that the Committee's comments "display an ignorance about Australia's law and practice and do not go to the substance of whether our law is fundamentally "adequate" from a trading point of view." He acknowledged that officials from Australia and Europe would "obviously" continue to talk but that "Australia will only

---

155 According to the Federal Government the small business exemption exempts about 94 percent of all Australian businesses but only 30 percent of total business sales. Gunning P "'Central Features of Australia's Private Sector Privacy Law' ***Privacy Law and Reporter*** Volume 7, Number 10, May 2001 at 1. Small businesses that are otherwise exempt from the Act may choose to "Opt-in" if they so wish. In January 2002, the Commissioner issued a news release detailing the relevant procedures for doing so. However, these companies retain the right to opt-out at a later stage. ***BNA World Data Protection Report*** Volume 2 Issue 2 February 2002.

156 European Union Article 29 Working Party ***Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000,*** March 2001.

look at options that do not impose unnecessary burdens on business." [157] The Australian Law Reform Commission (ALRC) has undertaken a comprehensive review of the Privacy Act and will report its findings in 2008.

9.8.12 The Office of Privacy Commissioner,[158] which has responsibilities under the Privacy Act, was initially established as a member of the Human Rights and Equal Opportunity Commission but has been operating as a separate statutory agency since 1st July 2000.

9.8.13 The Office has a wide range of functions, including handling complaints,[159] auditing compliance, promoting community awareness, and advising the government and others on privacy matters. The Commissioner may make formal determinations in relation to complaints received. However, the determinations are not legally binding on the respondents. The Commissioner, the complainant or the adjudicator for an approved privacy code can commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the determination.

9.8.14 The federal Privacy Commissioner is also the supervisory and complaint handling agency of Part VIIC of the Crimes Act enacted in 1989[160] and the Data-matching Program (Assistance and Tax) Act 1990.[161]

9.8.15 Spam legislation (Spam Act 2003) became effective in April 2004,outlawing unsolicited marketing messages on electronic mediums including e-mail, SMS and MMS. The Australian Communications and Media Authority (ACMA) will enforce the law.

---

157 The AG's Department has, however, begun a joint review with the Department of Employment, Workplace Relations and Small Business to examine State, Territory and Commonwealth workplace relations legislation and the privacy protection of employee records. The time line for this review is unclear, although it is expected to be completed within two years of the commencement of the legislation. The Department is also looking into the need for specific privacy protection for children's personal information.

158 Homepage <http://www.privacy.gov.au/>.

159 The Privacy Commission received a total number of 1183 complaints from July 2005 to June 2006.

160 Which provides some protection to individuals who have had criminal convictions in relation to so-called 'spent' convictions (i.e.: convictions for relatively minor offences which they are allowed to 'deny' or have discounted after a set period of time).

161 That provides detailed procedural controls over the operation of a major program of information matching between federal tax and benefit agencies.

9.8.16 On July 31, 2001 the Privacy Commissioner released the results of a comprehensive research project into public attitudes towards privacy issues that was commissioned earlier in the year.[162] The research findings were incorporated into three separate reports:

a) Privacy and the Community;

b) Privacy and Business; and

c) Privacy and Government.

9.8.17 The results showed overwhelming support for privacy protection.[163] The Privacy Commissioner indicated that the results of the survey would be used in the future planning of the office.

9.8.18 Some Australian States and Territories also enacted separate privacy laws.

9.9 Other countries

9.9.1 The following are examples of privacy measures that have been noted in countries outside the European Union and North America:

* **The Republic of Chile**[164] was the first Latin American country to enact a data protection law. The "Law for the Protection of Private Life" came into force on October 28, 1999. The EU has, however, expressed concerns about the data protection law as this law does not contain restrictions for transfers of personal data to third countries, nor does it have a data protection authority.

---

162 Office of the Federal Privacy Commissioner of Australia ***The Results of Research into Community, Business and Government Attitudes Towards Privacy in Australia*** July 31 2001.

163 For example, 91 percent of the public said that they would like businesses to seek permission before engaging in direct marketing; 89 percent would like organisations to advise them who would have access to their personal information and 92 percent would like to be told how it would be used; 42 percent have refused to deal with organisations they felt did not adequately protect their privacy. When asked what kind of data they considered most sensitive 40 percent identified financial details, 11 percent identified income, 7 percent identified medical or health information, 4 percent identified home address, 3 percent identified phone number and 3 percent identified genetic information. Office of the Federal Privacy Commissioner ***Privacy and the Community: Main Findings.***

164 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 325 and the references made therein.

* **Argentina**[165] passed the "Law for the Protection of Personal Data" (LPDP) in November 2000. It is in conformance with article 43 of the Constitution[166] and based on the European Union Data Protection Directive and the Spanish Data Protection Acts of 1992 and 1999. The European Union decided that Argentina could be considered as providing an adequate level of protection for personal data meeting the requirements of the Directive. Argentina is the first country in Latin America to obtain such approval. The LPDP has established a data protection authority within the Ministry of Justice which has a staff of 20 persons and is charged with receiving and processing complaints, enforcing the LPDP and endowed with powers of investigation and intervention.

* There is no general data protection law in the **Republic of India**,[167] though some provisions exist in other regulations. The rise of business outsourcing (BPO) operations and call centres in India has placed the government under increasing pressure to implement a data protection law that conforms to US and EU data protection standards or to implement a form of Safe-Harbor agreement similar to the US and EU privacy framework. NASSCOM (National Association of Software and Service Companies) has suggested changes to the Information Technology Act 2000 that would conform to US and EU privacy laws and allow India to negotiate with the EU for recognition as a country that offers an adequate level of protection for personal data. Foreign countries are currently relying on contractual obligations to impose privacy protection standards for customers.

* There is currently no general data protection law in the **Philippines.**[168] The Government Data Privacy Protection Act of 2007[169] and Administrative Order 8 are two pieces of pending legislation that will protect data privacy both in the public and private sectors. The DPPD ensures security of data in the government's possession, while the AO seeks to cover private sector data handling practices. Recognising the growing market for business data

---

165 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** at 210 and the references made therein.

166 Art 43, enacted in 1994, provides a right of "habeas data". Habeas data is a special, simplified and quick judicial remedy for the protection of personal data.

167 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** and the references made therein.

168 EPIC and Privacy International ***Privacy and Human Rights Report 2006*** and the references made therein.

169 Government Data Privacy Protection Act of 2007, Bill no 2678, Senate of Phillipines, 13th Congress.

processing outsourcing the Department of Trade issued the Administrative Order in 2006. The “Guidelines for the Protection of Personal Data in Information and Comm systems in the Private Sector” provides detailed principles and rules on personal data protection for the private sector entities and data protection certifiers.

CHAPTER 10: CONCLUSION: A DRAFT BILL ON THE PROTECTION OF PERSONAL INFORMATION

10.1 In the previous nine chapters the Commission has, in accordance with its brief,[1] investigated all aspects regarding the protection of the right to privacy of a person as it relates to the processing of his, her or its personal information by the State and private entities.

10.2 It has been noted that the protection of personal information seeks to uphold the right to privacy as protected by the common law, section 14 of the Constitution and other Human Rights Instruments.

10.3 From a practical perspective, it has been established that a person's personal information needs protection since -

* opportunities for the uncontrolled collection or personal information have increased exponentially in recent years due to, inter alia, the expansion of telecommunications technology;
* some of the information that is collected may unduly harm the subject of such collection by undermining his, her or its privacy, identity, dignity, integrity and independence as it may be inaccurate, incomplete, irrelevant, accessed and distributed without authorisation, used for purposes that are incompatible with the purpose for which it was collected or unlawfully destroyed;
* unprotected personal information may, furthermore, lead to identity theft and other criminal offences; the proliferation of spam and other direct marketing excesses;
* adequate privacy protection will result in the free flow of information, which will stimulate the economy and provide employment opportunities, for instance in the call-centre industry;
* children and other vulnerable parties are currently unprotected, especially in so far as the Internet and other electronic devices are concerned;
* information privacy legislation will provide a safe environment within which the e-

---

1 The terms of reference of the Privacy and Data Protection investigation (Project 124) was stated as follows in the Discussion Paper -

a) To investigate all aspects regarding the protection of the right to privacy of the individual in relation to the processing (collection, storage, use and communication) of his or her personal information by the State or another person; and

b) To recommend any legislative or other steps that should be taken in this regard.

government initiative can be developed.

A number of key users were identified[2] and specific instances of data protection discussed.[3]

10.4 It has been noted,[4] furthermore, that in information protection legislation, itself, two approaches can be identified:

a) The European Union approach which has a human rights perspective; and
b) The Organisation for Economic Cooperation and Development approach which has as its purpose the harmonisation of privacy laws worldwide in order to assist business development through the free flow of information across international borders.

10.5 What has transpired is that a balance between these two interests is of the utmost importance.[5] Information privacy is, therefore, about creating a trusted framework for the collection, exchange and use of personal information in commercial and governmental contexts. Information protection laws should permit, and even facilitate, the commercial and governmental use of personal information while providing to individuals-

a) control over what to collect and disclose;
b) awareness of how their personal information will be used;
c) rights to insist that information is accurate, complete, up-to-date and not misleading; and
d) protection when personal information is used to make decisions about a person.

---

2 Key users of information include the following:
* telephone companies;
* retailers;
* credit bureaux;
* transport companies;
* the health and medical profession;
* banks and financial institutions;
* the insurance industry;
* direct marketing industry;
* public bodies such as government departments and local authorities.

3 See Chapter 5 above.

4 IMS.

5 Global Internet Policy Initiative (GIPI) ***The International Legal Framework for Data Protection and Its Transposition to Developing and Transitional Countries*** December 2004 accessed at http://www.cdt.org/ on 15/1/07.

10.6 This view, already set out in the Discussion Papers, [6] have been strengthened by the overwhelming support received in written submissions and during numerous discussions with various stakeholders. These views were also confirmed through further research conducted and now form the basis of the proposed draft Bill set out in **Annexure C** to this report.

10.7 The Commission, therefore, recommends that privacy and data protection should be regulated by legislation. The Bill is a general information protection statute, which will be supplemented by codes of conduct for the various sectors and will be applicable to both the public and private sector. It provides a framework within which various other pieces of legislation can be interpreted. It covers both automatic and manual processing and will protect identifiable natural and juristic persons.

10.8 The Bill gives effect to eight core information protection principles, namely processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, individual participation and accountability. Provision is made for exceptions to the information protection principles. Exemptions are furthermore possible for specific sectors in applicable circumstances. Special provision has furthermore been made for the protection of special (sensitive) personal information.

10.9 Codes of conduct for individual sectors may be drawn up for specific sectors. This will include the possibility of making provision for an adjudicator to be responsible for the supervision of information protection activities in the sector. The Regulator will, however, retain oversight authority. The codes will accurately reflect the information protection principles as set out in the Act, but should furthermore assist in the practical application of the rules in a specific sector. The codes will also allow the regulation to be flexible in order to keep pace with technological development and evolving industry practices.

10.10 The Commission is of the opinion that it has addressed the major compliance challenges identified. Provision has been made for a commission-like, independent Information Protection

---

6 The preliminary proposals of the Commission were summarised as follows in the Discussion Paper:
a) privacy and data protection should be regulated by legislation;
b) general principles of data protection should be developed and incorporated in the legislation;
c) a statutory regulatory authority should be established;
d) a flexible approach should be followed in which industries will develop their own codes of practice (in accordance with the principles set out in the legislation) which will be overseen by the regulatory authority.

Regulator with a full-time Chairperson to direct the work of the Regulator.[7] The existence of a vigorous supervisory authority is indispensable for good privacy protection since laws are not self-implementing and the culture of privacy cannot securely establish itself without an authoritative champion.

10.11 The Regulator will be responsible for the implementation of both the Protection of Personal Information Act and the Promotion of Access to Information Act.[8] Data subjects are under an obligation to notify the Regulator of any processing of personal information before they undertake such processing and provision has also been made for prior investigations to be conducted where the information being collected warrants a stricter regime.

10.12 Enforcement should be through the Regulator, using as a first step a system of notices where conciliation or mediation has not been successful. Failure to comply with the notices is a criminal offence. The Regulator may furthermore assist a data subject in claiming compensation from a responsible party for damage suffered. Obstruction of the Regulator's work is regarded in a very serious light and constitutes a criminal offence.

10.13 The Bill will, therefore, address the current lack of operational guidance and ensure compliance by imposing penalties for failure to comply. It is the opinion of the Commission that the proposed regulatory authority will be an excellent alternative for the adversarial court processes that have proven ineffectual in implementing PAIA. Use of a regulator will promote access to justice for the ordinary person and will, in general, create a system of good governance.

10.14 It is the Law Commission's objective to ensure that the legislation provides an adequate level of information protection in terms of the EU Directive. In this regard a provision has been included that prohibits the transfer of personal information to countries that do not ensure an adequate level of information protection.

10.15 The recommendations and Bill prepared by the Law Commission are the result of an extensive consultative process conducted both nationally and internationally. Should these

---

7 Two options for the implementation of this recommendation have been set out above. The Commission's first choice is the establishment of a separate and independent entity. It would, however, be possible to use the structure as set out in the Bill as a separate ring-fenced entity with its own budget within an existing structure such as the SA Human Rights Commission.

8 See also the Regulator's responsibilities in terms of the National Credit Act as discussed in Chapter 5.

recommendations be adopted by Parliament, the protection of information privacy in South Africa will be brought into line with international requirements and developments.

ANNEXURE A

LIST OF WRITTEN RESPONSES TO ISSUE PAPER 24

1. Banking Council, The
2. Brooks L
3. Credit Bureau Association (including the Consumer Credit Association and the Furniture Traders Association)
4. Department of Public Service and Administration (DPSA)
5. Edward Nathan and Friedland Attorneys
6. ESKOM, Legal Department
7. Financial Services Board
8. Gideonites
9. Harty Rushmere Attorneys
10. Hendriks, A
11. IMS Health SA Pty Ltd (Michalsons on behalf of)
12. Internet Service Providers' Association
13. Klaaren, Prof J
14. Liberty Group Ltd
15. Link Centre, University of the Witwatersrand and Centre for Innovation Law and Policy, University of Toronto
16. Life Offices' Association of South Africa, The (LOA)
17. Loedolff, G
18. Marketing Federation of Southern Africa
19. Medical Research Council
20. Munns, P

21. Nadasen, Dr S
22. National Archives and Records Service of South Africa
23. Nedbank Limited
24. Olivier, Prof M
25. Private Health Information Standards Committee
26. Rens, A
27. South African Broadcasting Corporation Limited (SABC)
28. South African Fraud Prevention Service (SAFPS)
29. South African History Archive (SAHA)
30. South African Human Rights Commission (SAHRC)
31. South African Police Service (SAPS)
32. Sanlam Life: Law Service
33. School of Public Health, University of Cape Town
34. Society of Advocates of KwaZulu-Natal
35. Strata
36. Strijdom, C
37. Tsholanku, N
38. US Department of Commerce
39. Vodacom (Pty) Ltd

ANNEXURE B

LIST OF WRITTEN RESPONSES TO DISCUSSION PAPER 109

1. Board of Health Care Funders
2. CAPES
3. Cell-C
4. Chetty,M
5. Commonwealth Human Rights Initiative
6. Credit Bureau Association No 1
7. Credit Bureau Association No 2
8. Deeds Office
9. Department of Communications
10. Department of Defence
11. Department of Home Affairs
12. Department of Land Affairs
13. Department of Premier, Western Cape
14. Department of Provincial and Local Government
15. Department of Public Works
16. Department of National Intelligence (Office of the DG)
17. Direct Marketing Association (Michalsons Attorneys) no 1
18. Direct Marketing Association (Michalsons Attorneys) no 2
19. Discovery Health
20. ESKOM
21. Foschini's (Michalsons Attorneys)
22. Hooflanddros, Welkom

23. IMS Health (Michalsons Attorneys)
24. IMSA (E Klinck)
25. Landbank
26. Law Reform Commission of Hong Kong
27. Law Society of South Africa (E-law committee)
28. Lawyers for Human Rights
29. Life Offices' Association of South Africa, The LOA
30. Medical Research Council
31. Metz, Prof T
32. MFRC
33. MIH Group (Werkmans Attorneys)
34. Milo, D (Webber Wentzel Bowens)
35. Momentum Health
36. Moony, John and Joan
37. Motlala, Dr MDC
38. MTN(Pty)Ltd
39. National Intelligence Agency Legal Services
40. Nedbank Limited
41. Ombudsman for Long-Term Insurance
42. Perry, Romain
43. Provincial Administrator, Western Cape
44. SABRIC
45. SACCOM
46. SA Chamber of Business
47. South African Fraud Prevention Service (SAFPS)
48. South African History Archives (SAHA)
49. South African Human Rights Commission (SAHRC)
50. South African Insurance Association (SAIA)
51. South African Police Services (SAPS)
52. SNO Telecommunications (Edward Nathan)

53. Society of Advocates, Kwa-Zulu Natal
54. Sovereign Health
55. Standard Bank
56. Stassen, Pieter
57. Statistics SA
58. TELKOM
59. The Banking Association
60. US Department of Commerce
61. Van der Merwe, Prof D
62. Vodacom (Pty) Ltd
63. Zion Christian Church

ANNEXURE C

BILL

An Act to promote the protection of personal information processed by public and private bodies; to provide for the establishment of an Information Protection Regulator; and to provide for matters incidental thereto

---

To be introduced by the Minister for Justice and Constitutional Development

---

Preamble

RECOGNISING THAT -

*****Section 14 of the Constitution provides that everyone has the right to privacy;

* The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information;

* The state must respect, protect, promote and fulfil the rights in the Bill of Rights;

AND BEARING IN MIND THAT -

* Consonant with the constitutional values of democracy and openness, the need for economic and social progress, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information;

AND IN ORDER TO -

* Regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives best effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests

BE IT THEREFORE ENACTED by the Parliament of the Republic of South Africa, as follows --

CONTENTS OF THE ACT

PRINCIPLE 2
PROCESSING LIMITATION

8. Lawfulness of processing
9. Minimality
10. Consent, justification and objection
11. Collection directly from data subject

PRINCIPLE 3
PURPOSE SPECIFICATION

12. Collection for specific purpose
13. Data subject aware of purpose of collection of information
14. Retention of records

PRINCIPLE 4
FURTHER PROCESSING LIMITATION

15. Further processing not incompatible with purpose of collection

PRINCIPLE 5
INFORMATION QUALITY

16. Quality of information to be ensured

PRINCIPLE 6
OPENNESS

17. Notification to Regulator and to data subject

PRINCIPLE 7
SECURITY SAFEGUARDS

18. Security measures to ensure integrity of personal information
19. Information processed by person acting under authority
20. Security measures regarding information processed by operator
21. Notification of security compromises

PRINCIPLE 8
DATA SUBJECT PARTICIPATION

Part B: Processing of special personal information

CHAPTER 4
EXEMPTIONS FROM INFORMATION PROTECTION PRINCIPLES

CHAPTER 5
SUPERVISION

Part A: Information Protection Regulator

CHAPTER 12
MISCELLANEOUS

SCHEDULE 1
Amendment of laws

CHAPTER 1

GENERAL PROVISIONS

Definitions

1. In this Act, unless the context indicates otherwise -

"automatic calling machine" means an automated calling system without human intervention;

"biometric" means techniques of personal identification that are based on physical characteristics including fingerprinting, DNA analysis, retinal scanning and voice recognition;

"child" means a natural person under the age of 18 years**;**

"code of conduct" means a code of conduct issued in terms of Chapter 7 of this Act;

"committee" means a committee of the National Assembly appointed in accordance with the Standing Orders of Parliament for the purpose of considering a matter contemplated in section 36(2)(a) and (b) of this Act;

"consent" means any voluntary, specific and informed expression of will in terms of which a data subject agrees to the processing of personal information relating to him or her;

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"data subject" means the person to whom personal information relates;

"de-identify" in relation to personal information of a data subject, means to delete any information that -

a) identifies the data subject;
b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
c) can be linked by a reasonably foreseeable method to other information that identifies the data subject or that can be manipulated by a reasonably foreseeable method to identify the data subject;

"electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"enforcement notice" means a notice issued in terms of section 90;

"filing system" means any structured set of personal information which is accessible according to specific criteria;

"head" of, or in relation to, a private body means a head of a body as defined in sec 1 of the Promotion of Access to Information Act 2 of 2000;

"information matching programme" means the comparison (whether manually or by means of any electronic or other device) of any document that contains personal information about ten or more data subjects with one or more other documents that contain personal information about ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

"information notice" means a notice issued in terms of section 88;

“information protection officer” of, or in relation to, a public body means an information officer or deputy information officer as contemplated in terms of the Promotion of Access to Information Act 2 of 2000 and of, or in relation to, a private body means the head of a private body or a person designated by the head in terms of section 48 of this Act;

“information protection principle” means any of the principles set out in Part A of Chapter 3 of this Act;

“Minister” means the Minister for Justice and Constitutional Development;

“operator” means a person who processes personal information for a responsible party in terms of a contract of mandate, without coming under the direct authority of that party;

“parent” includes either parent of a child or the child’s legal guardian;

“parental consent” means any voluntary, specific and informed expression of will in terms of which the parent of a child agrees to the processing of personal information relating to the child;

“person” means a natural person or a juristic person;

“personal information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to -

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
b) information relating to the education or the medical, financial, criminal or employment history of the person;
c) any identifying number, symbol, email address, physical address, telephone number or other particular assigned to the person;
d) the blood type or any other biometric information of the person;
e) the personal opinions, views or preferences of the person;
f) correspondence sent by the person that is implicitly or explicitly of a private or

confidential nature or further correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the person; and

h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

“prescribed” means prescribed by regulation or by a code of conduct;

“**prior investigation”** means an investigation conducted by the Regulator in terms of Part B of Chapter 6 of this Act;

“private body” means

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person,

but excludes a public body;

"processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, degradation, erasure or destruction of information;

“professional legal adviser” means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his, her or its request, with independent, confidential legal advice;

“**public body”** means -

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when -

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation;

(c) any other body designated by the Minister by regulation made under this Act to be a public authority for the purposes of this Act;

"public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

"public record" means a record that is accessible in the public domain and which is in the possession or under the control of a public body, whether or not it was created by that public body;

"record" means any recorded information -

(a) regardless of form or medium, including any of the following -

(i) writing on any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment (whether hardware or software or both), or other device; and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking, or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph, or drawing;

(v) photograph, film, negative, tape, or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

“Regulator” means the Information Protection Regulator established in section 35 of this Act;

“re-identify” in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that -

a) identifies the data subject;

b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

c) can be linked by a reasonably foreseeable method to other information that identifies the data subject or that can be manipulated by a reasonably foreseeable method to identify the data subject;

"responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

“subscriber” means any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services.

Purpose of the Act

2.(1) The purpose of this Act is to -

(a) give effect to the constitutional right to privacy, by safeguarding a person’s personal information when processed by responsible parties, subject to justifiable limitations that are aimed at -

(i) balancing the right to privacy against other rights, particularly the right of access to information;

(ii) protecting important interests, including the free flow of information within the Republic and across international borders;

(b) regulate the manner in which personal information may be processed, by establishing principles, in harmony with international standards, that prescribe

the minimum threshold requirements for lawful processing of personal information;

(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(d) establish voluntary and compulsory measures, including an Information Protection Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act;

(2) This Act must be interpreted in a manner that gives effect to the purposes of the Act set out in subsection (1).

CHAPTER 2

APPLICATION PROVISIONS

Application of this Act

3. This Act applies to the processing of personal information entered in a record, using automated or non-automated means, by or for a responsible party -

(a) domiciled in the Republic of South Africa; or

(b) which is not domiciled in South Africa, using automated or non-automated means situated in South Africa, unless those means are used only for forwarding personal information,

provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

Exclusions

4. This Act does not apply to the processing of personal information -

(a) in the course of a purely personal or household activity;

(b) that has been de-identified to the extent that it cannot be re-identified again;

(c) by or on behalf of the State and -

(i) which involves national security, defence or public safety; or

(ii) the purpose of which is the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures,

to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;

(d) for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;

(e) by the Cabinet and its committees, the Executive Council of a Province and a Municipal Council of a municipality;

(f) relating to the judicial functions of a court referred to in section 166 of the Constitution; or

(g) that has been exempted from the application of the information protection principles in terms of section 34.

Saving

5.(1) This Act does not affect the operation of any other legislation that regulates the processing of personal information and is capable of operating concurrently with this Act.

(2) If any other legislation provides for safeguards for the protection of personal information that are more extensive than those set out in the information protection principles, the more extensive safeguards will prevail.

This Act binds the State and the private sector

6. This Act binds the State and the private sector.

CHAPTER 3

CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A: Information Protection Principles

PRINCIPLE 1

Accountability

Responsible party to give effect to principles

7. The responsible party must ensure that the Principles set out in this Chapter and all the measures that give effect to the Principles are complied with.

PRINCIPLE 2

Processing limitation

Lawfulness of processing

8. Personal information must be processed -

(a) lawfully; and

(b) in a reasonable manner in order not to infringe the privacy of the data subject.

Minimality

9. Personal information may only be processed if, given the purpose(s) for which it is processed, it is adequate, relevant, and not excessive.

Consent, justification and objection

10.(1) Personal information may only be processed if -

(a) the data subject has consented to the processing;

(b) processing is necessary for the conclusion or performance of a contract to which the data subject is party, or to carry out actions that are necessary for the conclusion or performance of such a contract;

(c) processing is necessary to comply with an obligation imposed by law on the responsible party;

(d) processing is necessary to protect a legitimate interest of the data subject;

(e) processing is necessary for the proper performance of a public law duty by a public body; or

(f) processing is necessary for pursuing the legitimate interests of the responsible

party or of a third party to whom the information is supplied.

(2) A data subject may object, at any time, on reasonable grounds relating to his, her or its particular situation, in the prescribed manner, to the processing of personal information, in terms of subsection (1)(d) to (f), unless otherwise provided for in national legislation.

(3) If a data subject has objected to the processing of personal information in terms of subsection (2) the responsible party may no longer process the personal information.

Collection directly from data subject

11.(1) Personal information must be collected directly from the data subject, except as otherwise provided in this section.

(2) It is not necessary to comply with subsection (1) of this section if -

(a) the information is contained in a public record or has deliberately been made public by the data subject;

(b) the data subject has consented to the collection of the information from another source;

(c) collection of the information from another source would not prejudice a legitimate interest of the data subject;

(d) collection of the information from another source is necessary --

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) to enforce a law imposing a pecuniary penalty;

(iii) to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997;

(iv) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

(v) in the legitimate interests of national security; or

(vi) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

(e) compliance would prejudice a lawful purpose of the collection; or

(f) compliance is not reasonably practicable in the circumstances of the particular case.

PRINCIPLE 3

Purpose specification

Collection for specific purpose

12. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

Data subject aware of the purpose of collection of information

13. Steps must be taken in accordance with section 17(2) below to ensure that the data subject is aware of the purpose of the collection of the information as referred to in section 12 above.

Retention of records

14.(1) Subject to subsections (2) and (3), records of personal information must not be

retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless -

(a) retention of the record is required or authorised by law;

(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject has consented to the retention of the record.

(2) Records of personal information may be retained for periods in excess of those provided for under subsection (1) for historical, statistical or research purposes, and if the responsible party has established appropriate safeguards against the records being used for any other purposes.

(3) A responsible party that has used a record of personal information about a data subject to make a decision about the data subject must -

a) retain the record for such period as may be required or prescribed by law or a code of conduct; or

b) if there is no law or code of conduct prescribing a retention period, for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

(4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after it is no longer authorised to retain the record in terms of subsection (1) or (2).

(5) The destruction or deletion of a record of personal information in terms of subsection

(4) must be done in a manner that prevents its reconstruction in an intelligible form.

PRINCIPLE 4

Further processing limitation

Further processing to be compatible with purpose of collection

15.(1) Further processing of personal information must be compatible with the purpose for which it was collected in terms of principle 3.

(2) To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of the following -

(a) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

(b) the nature of the information concerned;

(c) the consequences of the intended further processing for the data subject;

(d) the manner in which the information has been collected, and

(e) any contractual rights and obligations between the parties.

(3) The further processing of personal information is not incompatible with the purpose of collection if -

(a) the data subject has consented to the further processing of the information;

(b) the information is available in a public record or has deliberately been made

public by the data subject;

(c) further processing is necessary -

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) to enforce a law imposing a pecuniary penalty;

(iii) to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997;

(iv) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

(v) in the legitimate interests of national security;

(d) the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to -

(i) public health or public safety; or

(ii) the life or health of the data subject or another individual;

(e) the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for these specific purposes and will not be published in an identified form; or

(f) the further processing of the information is in accordance with an authority granted under section 34 (exemptions) of this Act.

PRINCIPLE 5

Information quality

Quality of information to be ensured

16. The responsible party must take reasonably practicable steps, having regard to the purpose for which personal information is collected or further processed, to ensure that the personal information is complete, not misleading, accurate and updated where necessary.

PRINCIPLE 6

Openness

Notification to Regulator and to data subject

17.(1) Personal information may only be processed by a responsible party that has notified the Regulator in terms of Chapter 6 of this Act.

(2) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of -

(a) the fact that the information is being collected;

(b) the name and address of the responsible party;

(c) the purpose or purposes for which the information is being collected;

(d) whether or not the supply of the information by that data subject is voluntary or mandatory and the consequences of failure to provide the information;

(e) any particular law authorising or requiring the collection of the information; and

(f) any further information such as -

(i) the recipients or categories of recipients of the information;

(ii) the nature or categories of the information; or

(iii) the existence of the right of access to and the right to rectify the information collected;

which is necessary, having regard to the specific circumstances in which the

information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

(3) The steps referred to in subsection (2) of this section must be taken -

(a) if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in subsection 2(a) to (f); or

(b) in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

(4) A responsible party that compiles or has compiled a manual and made it available in terms of section 14 or section 51 of the Promotion of Access to Information Act 2 of 2000, does not have to comply with subsection (1) of this section, if all the particulars referred to in section 51 of this Act are contained in the manual.

(5) A responsible party that has previously taken the steps referred to in subsection (2) will comply with subsection (2) in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information is unchanged.

(6) It is not necessary for a responsible party to comply with subsection (2) if -

(a) the data subject has provided consent for the non-compliance;

(b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;

(c) non-compliance is necessary -

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) to enforce a law imposing a pecuniary penalty;

(iii) to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997;

(iv) for the conduct of proceedings in any court or tribunal that have been

commenced or are reasonably contemplated; or

(v) in the legitimate interests of national security;

(d) compliance would prejudice a lawful purpose of the collection;

(e) compliance is not reasonably practicable in the circumstances of the particular case; or

(f) the information will -

(i) not be used in a form in which the data subject may be identified; or

(ii) be used for historical, statistical or research purposes.

PRINCIPLE 7
Security safeguards

Security measures to ensure integrity of personal information

18.(1) A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent -

(a) loss of, or damage to, or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1) the responsible party must take reasonable measures to -

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risk identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Information processed by operator or person acting under authority

19.(1) An operator or anyone processing personal information on behalf of a responsible party or an operator, must -

(a) process such information only with the knowledge or authorisation of the responsible party, unless otherwise required by law; and

(b) treat personal information which comes to their knowledge as confidential and must not disclose it unless required by law or in the course of the proper performance of their duties.

Security measures regarding information processed by operator

20.(1) A responsible party must ensure that an operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 18 above.

(2) The processing of personal information for a responsible party by an operator on behalf of the responsible party must be governed by a written contract between the operator and the responsible party, which requires the operator to establish and maintain confidentiality and security measures to ensure the integrity of the personal information.

(3) If the operator is not domiciled in the Republic, the responsible party must take reasonably practicable steps to ensure that the operator complies with the laws, if any, relating to the protection of personal information of the territory in which the operator is domiciled .

Notification of security compromises

21.(1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party, or any third party processing personal information under the authority of a responsible party, must notify -

(a) the Regulator; and

(b) the data subject, unless the identity of such a data subject cannot be established.

(2) The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

(3) The responsible party may only delay notification if the South African Police Services, the National Intelligence Agency or the Regulator determine that notification will impede a criminal investigation.

(4) The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways -

(a) mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

(5) A notification must provide sufficient information to allow the data subject to take

protective measures against the potential consequences of the compromise, including if known to the responsible party, the identity of the unauthorised person(s) who may have accessed or acquired the personal information.

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

PRINCIPLE 8
Data subject participation

Access to personal information

22.(1) A data subject, after having provided adequate proof of identity, has the right to -

(a) request a responsible party, to confirm, free of charge whether or not the responsible party holds personal information about the data subject; and

(b) request from a responsible party, a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information -

(i) within a reasonable time;

(ii) at a prescribed fee, if any, that is not excessive;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) If, in accordance with subsection (1)(b) of this section, personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 23 to request the correction of information.

(3) If a data subject is required by a responsible party to pay a fee for services provided

to the data subject in terms of subsection 22(1)(b) to enable the responsible party to respond to a request, the responsible party -

(a) must give the applicant a written estimate of the fee before providing the services, and

(b) may require the applicant to pay a deposit for all or part of the fee.

(4) A responsible party may or must refuse to disclose any information requested in terms of subsection (1) to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act 2 of 2000 apply.

(5) If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of subsection (4), every other part must be disclosed.

Correction of personal information

23.(1) A data subject has the right to request a responsible party to -

(a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) destroy or delete a record of personal information about the data subject that it is no longer authorised to retain in terms of section 14.

(2) On receipt of a request in terms of subsection (1) a responsible party must do the following -

(a) correct the information;

(b) destroy or delete the information;

(c) provide the data subject, to his or her satisfaction, with credible evidence in

support of the information; or

(d) where agreement cannot be reached between the responsible party and the data subject, and if the data subject so request, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

(3) If the responsible party has taken steps under subsection (2) of this section that results in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of these steps.

(4) The responsible party must notify a data subject, who has made a request in terms of subsection (1) of the action taken as a result of the request.

Manner of access

24. The provisions of section 18 and section 53 of the Promotion of Access to Information Act 2 of 2000 apply to requests made in terms of sections 22 and 23 of this Act.

Part B

Processing of special personal information

Processing of special personal information (including information in respect of a child) prohibited

25. Unless specifically permitted by this Part, a responsible party may not process personal information -

a) concerning a child who is subject to parental control in terms of the law; or

b) concerning a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour.

Exemption to the prohibition on processing of personal information concerning a data subject's religious or philosophical beliefs

26.(1) The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs, referred to in section 25, does not apply if the processing is carried out by -

(a) spiritual or religious organisations, or independent sections of those organisations, provided that the information concerns data subjects belonging to those organisations;

(b) institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles, or

(c) other institutions provided that this is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.

(2) In the cases referred to under subsection(1)(a), the prohibition also does not apply to processing of personal information concerning the religion or philosophy of life of family members of the data subjects, if -

(a) the association concerned maintains regular contacts with these family members in connection with its aims; and

(b) the family members have not objected in writing to the processing.

(3) In the cases referred to in subsection (1) and (2), personal information concerning a data subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the data subject.

Exemption to the prohibition on processing of personal information concerning a data subject's race

27. The prohibition on processing personal information concerning a data subject's race, as referred to in section 25, does not apply if the processing is carried out to -

(a) identify data subjects and only when this is essential for that purpose; and

(b) comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

Exemption to the prohibition on processing of personal information concerning a person's trade union membership

28.(1) The prohibition on processing personal information concerning a person's trade union membership, as referred to in section 25, does not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which this trade union belongs, if this is necessary to achieve the aims of the trade union or trade union federation.
(2) In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

Exemption to the prohibition on processing of personal information concerning a data subject's political persuasion

29.(1) The prohibition on processing personal information concerning a data subject's political persuasion, as referred to in section 25, does not apply to processing by an institution founded on political principles, of the personal information of their members or employees or other persons belonging to the institution, provided that this is necessary to achieve the aims or

principles of the institutions.

(2) In the cases referred to under subsection(1), no personal information may be supplied to third parties without the consent of the data subject.

Exemption to the prohibition on processing of personal information concerning a data subject's health or sexual life

30.(1) The prohibition on processing personal information concerning a data subject's health or sexual life, as referred to in section 25, does not apply to the processing by -

(a) medical professionals, healthcare institutions or facilities or social services, if this is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

(b) insurance companies, medical aid schemes, medical scheme administrators and managed healthcare organisations, provided that this is necessary for -

(i) assessing the risk to be insured by the insurance company or covered by the medical aid scheme and the data subject has not objected to the processing;

(ii) the performance of an insurance or medical aid agreement; or

(iii) the enforcement of any contractual rights and obligations.

(c) schools, if this is necessary to provide special support for pupils or making special arrangements in connection with their health or sexual life;

(d) institutions for probation, child protection or guardianship, if this is necessary for the performance of their legal duties;

(e) the Ministers for Justice and Constitutional Development and of Correctional Services, if this is necessary in connection with the implementation of prison sentences or detention measures; or

(f) administrative bodies, pension funds, employers or institutions working for them, if this is necessary for -

(i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sexual life of the data subject; or

(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In the cases referred to under subsection (1), the information may only be processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.

(3) Responsible parties that are permitted to process information concerning a data subject's health or sexual life in terms of this section and are not subject to an obligation of confidentiality by virtue of office, profession or legal provision, are required to treat the information as confidential, unless they are required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information in accordance with subsection (1).

(4) The prohibition on processing any of the categories of personal information referred to in section 26, does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, as referred to under subsection (1)(a), with a view to the proper treatment or care of the data subject.

(5) Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless -

(a) a serious medical interest prevails; or

(b) the processing is necessary for the purpose of scientific research or statistics.

(6) More detailed rules may be prescribed concerning the application of subsection (1)(b) and (f).

Exemption to the prohibition on processing of personal information concerning a data subject's criminal behaviour

31.(1) The prohibition on processing personal information concerning a data subject's criminal behaviour, as referred to in section 25, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained this information in accordance with the law.

(2) The prohibition does not apply to responsible parties who process the information for their own lawful purposes to -

(a) assess an application by a data subject in order to take a decision about, or provide a service to, that data subject, or

(b) protect their legitimate interests in relation to criminal offences which have been, or can reasonably be expected to be, committed against them or against persons in their service.

(3) The processing of this information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

(4) The prohibition on processing any of the categories of personal information referred to in section 26 does not apply if this is necessary to supplement the processing of information on criminal behaviour permitted by this section.

General exemption to the prohibition on processing of special personal information

32. Without prejudice to sections 26 to 31, the prohibition on processing personal information referred to in section 25 does not apply if -

(a) processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law;

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

or

(d) the Regulator has granted authority in terms of section 34 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject's privacy;

and insofar as section 25(b) is concerned, if -

(a) processing is carried out with the consent of the data subject;

(b) the information has deliberately been made public by the data subject.

CHAPTER 4

EXEMPTIONS FROM INFORMATION PROTECTION PRINCIPLES

General

33. Processing of personal information is not in breach of an information protection principle if the processing is authorised by the Regulator in terms of section 34.

Regulator may authorise processing of personal information --

34.(1) The Regulator may authorise a responsible party to process personal information, even if that processing is in breach of an information protection principle if the Regulator is satisfied that, in the circumstances of the case -

(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from the processing; or

(b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data

subject or third party that could result from the processing.

(2) The public interest referred to in subsection (1) above includes -

(a) the legitimate interests of State security;

(b) the prevention, detection and prosecution of criminal offences;

(c) important economic and financial interests of the State and other public bodies;

(d) fostering compliance with legal provisions established in the interests referred to under (b) and (c); or

(e) historical, statistical or research activity.

(3) The Regulator may impose reasonable conditions in respect of any authority granted under subsection (1) of this section.

CHAPTER 5

SUPERVISION

Part A
Information Protection Regulator

Establishment of Information Protection Regulator

35. There is hereby established a juristic person to be known as the Information Protection Regulator which -

(a) has jurisdiction throughout the Republic;

(b) is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice; and

(c) must perform its functions and exercise its powers in accordance with this Act and the Promotion of Access to Information Act 2 of 2000.

Constitution of Regulator and period of office of members

36.(1)(a) The Regulator consists of the following members -

(i) a Chairperson; and

(ii) four other persons as ordinary members of the Regulator;

(b) Members of the Regulator must be appropriately qualified, fit and proper persons for appointment on account of experience as a practising advocate or attorney or as a professor of law at any university, or on account of any other qualification relating to the objects of the Regulator;

(c) The Chairperson of the Regulator must perform his or her functions under this Act and the Promotion of Access to Information Act 2 of 2000 in a full-time capacity and must not be employed in any other capacity during the period in which he or she holds office as Chairperson;

(d) The other members of the Regulator must be appointed in a part-time capacity;

(e) The Chairperson must direct the work of the Regulator and the Secretariat; and

(f) No person will be qualified for appointment as a member of the Regulator if that person –

(i) is a member of a legislature;

(ii) is a councillor of a local authority;

(iii) is an unrehabilitated insolvent; or

(iv) has at any time been convicted of any offence involving dishonesty.

(2) Members of the Regulator referred to in sec 36(1)(a) must be appointed by the President and must be persons -

(a) nominated by a committee after considering proposals made by interested parties in terms of subsection (4); and

(b) approved by the National Assembly by a resolution adopted by a majority of the total number of members of the House: Provided that if any nomination is not approved as required in paragraph (b),the committee must nominate another person.[1]

(3) The President may appoint one or more additional members if he or she considers it necessary for the investigation of any particular matter or the performance of any duty by the Regulator.

(4) Before the members of the Regulator are appointed the Minister must invite interested parties through the media and by notice in the Gazette to propose candidates within 30 days of the publication of such notice, for consideration by the committee referred to in subsection (2)(a).

(5) The members of the Regulator will be appointed for a period of not more than five years and will, at the expiration of such period, be eligible for reappointment.

(6) A person appointed as a member of the Regulator may resign from office by writing under his or her hand addressed to the President and will in any case vacate office on attaining the age of seventy years.

(7) A member may be removed from office by the President on the request of Parliament only for inability to discharge the functions of the office (whether arising from infirmity of body or mind or any other cause) or for misbehaviour.

---

1 The appointment procedure is based on the procedure set out for the appointment of members of Chapter 9 institutions such as the SA Human Rights Commission. One of the options provided in the report is that the Information Regulator should be situated within the SAHRC as a ring-fenced entity .

Remuneration, allowances, benefits and privileges of members

37.(1) A member of the Regulator who is not subject to the provisions of the Public Service Act, 1994 (Proclamation103 of 1994), will be entitled to such remuneration, allowances (including allowances for reimbursement of traveling and subsistence expenses incurred by him or her in the performance of his or her functions under this Act and the Promotion of Access to Information Act 2 of 2000), benefits and privileges as the Minister in consultation with the Minister of Finance may determine.

(2) The remuneration, allowances, benefits or privileges of different members of the Regulator may differ according to -

(a) the different offices held by them in the Regulator; or

(b) the different functions performed, whether in a part-time or full-time capacity, by them from time to time.

(3) In the application of subsections (1) and (2), the President or the Minister, as the case may be, may determine that any remuneration, allowance, benefit or privilege contemplated in those subsections, will be the remuneration, allowance, benefit or privilege determined from time to time by or under any law in respect of any person or category of persons.

Secretary and staff

38.(1) The Secretary of the Regulator and such other officers and employees as are required for the proper performance of the Regulator's functions, will be appointed in terms of the Public Service Act, 1994 (Proclamation 103 of 1994).

(2) The Regulator may, with the approval of the Minister in consultation with the Minister of Finance, on a temporary basis or for a particular matter which is being investigated by it, employ any person with special knowledge of any matter relating to the work of the Regulator,

or obtain the co-operation of any body, to advise or assist the Regulator in the performance of its functions under this Act and the Promotion of Access to Information Act 2 of 2000 , and fix the remuneration, including reimbursement for travelling, subsistence and other expenses, of such person or body.

Committees of Regulator

39.(1) The Regulator may, if it considers it necessary for the proper performance of its functions -

(a) establish a working committee, which must consist of such members of the Regulator as the Regulator may designate;

(b) establish such other committees as it may deem necessary, and which must consist of -

(i) such members of the Regulator as the Regulator may designate; or

(ii) such members of the Regulator as the Regulator may designate and other persons appointed by the Minister for the period determined by the Minister.

(2) The Minister may at any time extend the period of an appointment referred to in subsection (1) (b) (ii) or, if in his or her opinion good reasons exist therefor, revoke any such appointment.

(3) The Regulator must designate the chairman and, if the Regulator deems it necessary, the vice-chairman of a committee established under subsection (1).

(4) (a) A committee referred to in subsection (1) must, subject to the directions of the Regulator, perform those functions of the Regulator assigned to it by the Regulator.

(b) Any function so performed by the working committee referred to in subsection (1) (a) will be deemed to have been performed by the Regulator.

(5) The Regulator may at any time dissolve any committee established by the Regulator.

(6) The provisions of sections 40 and 45(4) will with the necessary changes apply to a committee of the Regulator.

Meetings of Regulator

40.(1) Meetings of the Regulator must be held at the times and places determined by the chairperson of the Regulator.

(2) The majority of the members of the Regulator will constitute a quorum for a meeting.

(3) The Regulator may regulate the proceedings at meetings as it may think fit and must keep minutes of the proceedings.

Funding

41. (1) Parliament will appropriate annually, for the use of the Regulator, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Regulator, of its powers, duties and functions under this Act and the Promotion of Access to Information Act 2 of 2000.

(2) The financial year of the Regulator is the period from 1 April in any year to 31 March in the following year, except that the first financial year of the Regulator begins on the date that this Act comes into operation, and ends on 31 March next following that date.

(3) The Chairperson of the Regulator is the accounting authority of the Regulator for purposes of the Public Finance Management Act, 1999 (Act 1 of 1999) and will execute his or her duties in accordance with the Exchequer Act, 1975 (Act 66 of 1975).

(4) Within six months after the end of each financial year, the Regulator must prepare financial statements in accordance with established accounting practice, principles and procedures, comprising-

(a) a statement reflecting, with suitable and sufficient particulars, the income and expenditure of the Regulator during the preceding financial year; and

(b) a balance sheet showing the state of its assets, liabilities and financial position as at the end of that financial year.

(5) The Auditor General must audit the Regulator's financial records each year.

Protection of Regulator

42. The Regulator, and any person acting on behalf or under the direction of the Regulator is not civilly or criminally liable, for anything done, reported or said in good faith in the exercise or performance or purported exercise or performance of any power, duty or function of the Regulator in terms of this Act or the Promotion of Access to Information Act 2 of 2000.

Powers and duties of Regulator

43.(1) The powers and duties of the Regulator in terms of this Act are- --

education

(a) to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles;

(b) for the purpose of promoting the protection of personal information, to undertake educational programmes on the Regulator's own behalf or in co-operation with other persons or authorities acting on behalf of the Regulator;

(c) to make public statements in relation to any matter affecting the protection of the personal information of a data subject or of any class of data subjects;

monitor and enforce compliance

(d) to monitor and enforce compliance by public and private bodies of the provisions of this Act;

(e) to undertake research into, and to monitor developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of data subjects are minimised, and to report to the responsible Minister the results of such research and monitoring;

(f) to examine any proposed legislation (including subordinate legislation) or proposed policy of the Government that the Regulator considers may affect the protection of the personal information of data subjects, and to report to the responsible Minister the results of that examination;

(g) to report (with or without request) to Parliament from time to time on any matter affecting the protection of the personal information of a data subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the personal information of a data subject;

(h) on its own initiative or when requested to do so by a public or private body, to conduct an audit of personal information maintained by that body for the purpose of ascertaining whether or not the information is maintained according to the information protection principles;

(i) to monitor the use of unique identifiers of data subjects, and to report to Parliament from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the personal information of a data subject;

(j) to maintain, and to publish, make available and provide copies of such registers as are prescribed in this Act;

(k) to examine any proposed legislation that makes provision for -

(i) the collection of personal information by any public or private body; or

(ii) the disclosure of personal information by one public or private body to any other public or private body, or both, to have particular regard, in the course of that examination, to the matters set out in section 44(3) of this Act, in any case where the Regulator considers that the information might be used for the purposes of an information matching programme, and to report to the responsible Minister and Parliament the results of that examination;

consultation

(l) to receive and invite representations from members of the public on any matter affecting the personal information of a data subject;

(m) to consult and co-operate with other persons and bodies concerned with the protection of personal information principles;

(n) to act as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the personal information of a data subject;

(o) to provide advice (with or without a request) to a Minister or a public or private body on their obligations under the provisions, and generally, on any matter relevant to the operation, of this Act;

complaints

(p) to receive and investigate complaints about alleged violations of the protection of personal information of data subjects and in respect thereof make reports to complainants;

(q) to gather such information as in the Regulator's opinion will assist the Regulator in discharging the duties and carrying out the Regulator's functions under this

Act;

(r) to attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation;

(s) to serve any notices in terms of this Act and further promote the resolution of disputes in accordance with the prescripts of this Act;

research and reporting

(t) to report to Parliament from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a data subject;

(u) to report to Parliament on any other matter relating to protection of personal information that, in the Regulator's opinion, should be drawn to Parliament's attention;

codes of conduct

(v) to issue, from time to time, codes of conduct, amendment of codes and revocation of codes of conduct;

(w) to make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct;

(x) to review an adjudicator's decision under approved codes of conduct;

general

(y) to do anything incidental or conducive to the performance of any of the preceding functions;

(z) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Regulator by or under this Act or any other enactment;

(aa) to require the responsible party to disclose to any person affected by a compromise to the confidentiality or integrity of personal information, this fact in accordance with section 21 of this Act; and

(bb) to exercise the powers conferred upon the Commission by this Act in matters relating to the access of information as provided by the Promotion of Access to Information Act.

(2) The Regulator may, from time to time, in the public interest or in the legitimate interests of any person or body of persons, publish reports relating generally to the exercise of the Regulator's functions under this Act or to any case or cases investigated by the Regulator, whether or not the matters to be dealt with in any such report have been the subject of a report to the responsible Minister.

(3) The powers and duties of the Regulator in terms of the Promotion of Access to Information Act 2 of 2000 are set out in Part 5 of that Act.

Regulator to have regard to certain matters

44.(1) The Regulator is independent in the performance of its functions as set out in subsection 35 (b).

(2) In the performance of its functions, and the exercise of its powers, under this Act, the Regulator must -

(a) have due regard to the protection of personal information as set out in the information protection principles;

(b) have due regard for the protection of all human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the legitimate interest of government and business in achieving their objectives in an efficient way;

(c) take account of international obligations accepted by South Africa, including those concerning the international technology of communications; and

(d) consider any developing general international guidelines relevant to the better protection of individual privacy.

(3) In performing its functions in terms of section 43(1)(k) of this Act with regard to information matching programmes, the Regulator must have particular regard to the following matters -

(a) whether or not the objective of the programme relates to a matter of significant public importance;

(b) whether or not the use of the programme to achieve that objective will result in monetary savings that are both significant and quantifiable, or in other comparable benefits to society;

(c) whether or not the use of an alternative means of achieving that objective would give either of the results referred to in paragraph (b) of this section;

(d) whether or not the public interest in allowing the programme to proceed outweighs the public interest in adhering to the information protection principles that the programme would otherwise contravene; and

(e) whether or not the programme involves information matching on a scale that is excessive, having regard to -

(i) the number of responsible parties or operators that will be involved in the programme; and

(ii) the amount of detail about a data subject that will be matched under the programme.

Programmes of Regulator

45.(1) In order to achieve its objects in terms of this Act the Regulator must from time to time draw up programmes in which the various matters which in its opinion require consideration are included in order of preference, and must table such programmes in Parliament for information**.**

(2) The Regulator may include in any programme any suggestion relating to its objects received from any person or body.

(3) The Regulator may consult any person or body, whether by the submission of study documents prepared by the Regulator or in any other manner.

(4) The provisions of sections 2, 3, 4, 5 and 6 of the Commissions Act, 1947 (Act 8 of 1947), will apply with the necessary changes to the Regulator.

Reports of Regulator

46.(1) The Regulator must prepare a full report in regard to any matter investigated by it in terms of this Act and must submit such report to Parliament for information.

(2) The Regulator must within five (5) months of the end of a financial year of the Department for Justice and Constitutional Development submit to the Minister a report on all its activities in terms of this Act during that financial year.

(3) The report referred to in subsection (2) must be tabled in Parliament within fourteen days after it was submitted to the Minister, if Parliament is then in session, or, if Parliament is not then in session, within fourteen (14) days after the commencement of its next ensuing session.

Duty of confidentiality

47. A person acting on behalf or under the direction of the Regulator is required to treat as confidential the personal information which comes to his or her knowledge, except if the communication of such information is required by law or in the proper performance of his or her duties.

Part B

Information Protection Officer

Duties and responsibilities of Information protection officer

48.(1) An information protection officer's responsibilities include -

(a) the encouragement of compliance, by the body, with the information protection principles;

(b) dealing with requests made to the body pursuant to this Act;

(c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of this Act in relation to the body; and

(d) otherwise ensuring compliance by the body with the provisions of this Act.

(2) Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.

Designation and delegation of deputy information protection officers

49. Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act 2 of 2000, with the necessary changes, for -

(a) the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities set out in section 48(1) of this Act; and

(b) the delegation of any power or duty conferred or imposed on an information protection officer by this Act to a deputy information protection officer of that public or private body.

CHAPTER 6
NOTIFICATION AND PRIOR INVESTIGATION

Part A
Notification

Notification of processing

50. (1) A responsible party must notify the Regulator before commencing the -

(a) fully or partly automated processing of personal information or categories of personal information intended to serve a single purpose or different related purposes; or

(b) non-automated processing of personal information intended to serve a single purpose or different related purposes, must be notified if this is subject to a prior investigation.

(2) The notification referred to in subsection (1) must be noted in a register kept by the Regulator for this purpose.

Notification to contain specific particulars

51.(1) The notification must contain the following particulars -

(a) the name and address of the responsible party;

(b) the purpose or purposes of the processing;

(c) a description of the categories of data subjects and of the information or categories of information relating thereto;

(d) the recipients or categories of recipients to whom the personal information may be supplied;

(e) planned transborder flows of personal information; and

(f) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

(2) Subject to subsection (3) a responsible party will only have to give notice once, and not

each time personal information is received or processed.

(3) Changes in the name or address of the responsible party must be notified within one week and changes to the notification which concern subparagraphs (1)(b) to (f) must be notified in each case within one (1) year of the previous notification, if they appear to be of more than incidental importance.

(4) Any processing which departs from that which has been notified in accordance with the provisions of (1)(b) to (f) must be recorded and kept for at least three years.

(5) More detailed rules can be issued by or under regulation concerning the procedure for submitting notifications.

Exemptions to notification requirements

52.(1) The Regulator may by notice exempt certain categories of information processing which are unlikely to infringe the legitimate interests of the data subject from the notification requirement referred to in section 50.

(2) If processing of personal information is necessary in order to detect criminal offences in a particular case, it may be laid down by regulation that certain categories of processing by responsible parties who are vested with investigating powers by law, are exempt from notification.

(3) The notification requirement does not apply to public registers set up by law or to information supplied to a public body pursuant to a legal obligation.

(4) Any exemption granted to a responsible party from the provisions set out in sections 14 and 51 of the Promotion of Access to Information Act 2 of 2000 will also apply as an exemption of the notification requirements set out in terms of this Act.

Register of information processing

53.(1) The Regulator must maintain an up-to-date register of the information processing notified to it, which register must contain, as a minimum, the information provided in accordance with

section 51(1)(a) to (f).

(2) The register may be consulted by any person free of charge.

(3) The responsible party must provide any person who requests information referred to in section 50(l)(a) to (f) with the information so requested.

(4) The provisions of subsection (3) do not apply to -

(a) information processing which is covered by an exemption under Chapter 4; and

(b) public registers set up by law.

Failure to notify

54.(1) If section 50(1) is contravened, the responsible party is guilty of an offence and liable to a penalty as set out in section 99.

(2) Any responsible party who fails to comply with the duty imposed by notification regulations made by virtue of section 102 is guilty of an offence and liable to a penalty as set out in section 99.

Part B
Prior investigation

Processing subject to prior investigation

55.(1) The Regulator must initiate an investigation prior to any processing if a responsible party plans to -

(a) process a number identifying data subjects for a purpose other than the one for which the number is specifically intended with the aim of linking the information together with information processed by other responsible parties, unless the

number is used for the cases defined in Chapter 4;[2]

(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(c) process information for the purposes of credit reporting; and

(d) transfer special personal information, as referred to in section 26, to foreign countries without adequate information protection laws.

(2) The provisions of subsection (1) may be applied by the Regulator to other types of information processing by law or regulation if such processing carries a particular risk for the legitimate interests of the data subject.

(3) Part B of Chapter 6 will not be applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 of this Act in a specific sector or sectors of society.

Responsible party to notify Regulator if processing is subject to prior investigation

56.(1) Information processing under a code of conduct as contemplated in section 55(3) must be notified as such by the responsible party to the Regulator.

(2) Responsible parties may not carry out information processing that has been notified to the Regulator in terms of subsection (1) until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

(3) In the case of the notification of information processing to which section 55(1) is applicable, the Regulator must inform the responsible party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.

(4) In the event that the Regulator decides to conduct a more detailed investigation, it must indicate the period of time within which it plans to conduct this investigation, which period must not

---

2 Exemptions.

exceed thirteen weeks.

(5) On conclusion of the more detailed investigation referred to in subsection (4) the Regulator must issue a statement concerning the lawfulness of the information processing.

(6) A statement by the Regulator in terms of subsection (5) is deemed to be an enforcement notice served in terms of section 90 of this Act.

(7) A responsible party that has suspended its processing as required by subsection 2, and which has not received the Regulator's decision within the specified time limits in subsections (3) and (4), may presume a decision in its favour and continue with its processing.

CHAPTER 7
CODES OF CONDUCT

Issuing of codes of conduct

57.(1) The Regulator may from time to time issue a code of conduct.

(2) A code of conduct must -

(a) incorporate all the information protection principles or set out obligations that provide a functional equivalent of all the obligations set out in those principles; and

(b) prescribe how the information protection principles are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which the relevant responsible parties are operating.

(3) A code of conduct may apply in relation to any one or more of the following -

(a) any specified information or class or classes of information;

(b) any specified body or class or classes of bodies;

(c) any specified activity or class or classes of activities; or

(d) any specified industry, profession, or calling or class or classes of industries, professions, or callings.

(4) A code of conduct must also -

(a) in relation to any body that is not a public body, provide for controls in relation to the comparison (whether manually or by means of any electronic or other device) of personal information with other personal information for the purpose of producing or verifying information about an identifiable data subject;

(b) provide for the review of the code by the Regulator;

(c) provide for the expiry of the code.

Proposal for issuing of code of conduct

58.(1) The Regulator may issue a code of conduct under section 57 of this Act -

(a) on the Regulator's own initiative but in consultation with affected stakeholders or a body representing such stakeholders; or

(b) on the application of any person as provided in subsection (3) of this section.

(2) Without limiting subsection (1) of this section, but subject to subsection (3) of this section, any person may apply to the Regulator for the issuing of a code of conduct in the prescribed form submitted by the applicant.

(3) An application may be made pursuant to subsection (2) of this section only -

(a) by a body which is, in the opinion of the Regulator, sufficiently representative of any class or classes of bodies, or of any industry, profession, or calling as defined in the code; and

(b) if the code of conduct sought by the applicant is intended to apply in respect of the class or classes of body, or the industry, profession, or calling, that the applicant represents, in respect of such class or classes of body or of any such industry, profession, or calling.

(4) If an application is made to the Regulator pursuant to subsection (2) of this section, or if the Regulator intends to issue a code on its own initiative, the Regulator must give notice in the Gazette that the issuing of a code of conduct is being considered, which notice must contain a statement that -

(a) the details of the code of conduct being considered, including a draft of the proposed code, may be obtained from the Regulator; and

(b) submissions on the proposed code may be made in writing to the Regulator within such period as is specified in the notice.

(5) The Regulator must not issue a code of conduct unless it has considered the submissions made to the Regulator in terms of subsection (4) if any and is satisfied that all persons affected by the proposed code have had a reasonable opportunity to be heard.

(6) The decision as to whether an application for the issuing of a code has been successful must be made within a reasonable period of time which must not exceed thirteen (13) weeks.

Notification, availability and commencement of code

59.(1) If a code of conduct is issued under section 57 of this Act -

(a) the Regulator must ensure that there is published in the Gazette, as soon as reasonably practicable after the code is issued, a notice -
  (i) indicating that the code has been issued; and
  (ii) indicating where copies of the code are available for inspection free of charge and for purchase; and

(b) the Regulator must ensure that as long as the code remains in force, copies of it are available -

(i) on the Regulator's web site;

(ii) for inspection by members of the public free of charge at the Regulator's offices; and

(iii) for purchase or copying by members of the public at a reasonable price at the Regulator's offices.

(2) A code of conduct issued under section 57 of this Act comes into force on the 28th day after the date of its notification in the Gazette or on such later date as may be specified in the code and is binding on every class or classes of body, industry, profession or calling referred to therein.

Amendment and revocation of codes

60.(1) The Regulator may from time to time amend or revoke a code of conduct issued under section 57 of this Act.

(2) The provisions of sections 57 to 61 of this Act must apply in respect of any amendment or revocation of a code of conduct.

Procedure for dealing with complaints

61.(1) A code of conduct may prescribe procedures for making and dealing with complaints alleging a breach of the code, but no such provision may limit or restrict any provision of Chapter 8 of this Act.

(2) If the code sets out procedures for making and dealing with complaints, the Regulator must be satisfied that -

(a) the procedures meet the -

(i) prescribed standards; and

(ii) any guidelines issued by the Regulator in terms of section 62 relating to the making of and dealing with complaints;

(b) the code provides for the appointment of an independent adjudicator to whom complaints may be made;

(c) the code provides that, in performing his or her functions, and exercising his or her powers, under the code, an adjudicator for the code must have due regard to the matters listed in section 44(2);

(d) the code requires the adjudicator to prepare and submit a report (in a form satisfactory to the Regulator) to the Regulator within five (5) months of the end of a financial year of the Department for Justice and Constitutional Development on the operation of the code during that financial year; and

(e) the code requires the report prepared for each year to specify the number and nature of complaints made to an adjudicator under the code during the relevant financial year.

(3) A data subject who is aggrieved by a determination, including any declaration, order or direction that is included in the determination, made by an adjudicator (other than the Regulator) after investigating a complaint relating to the protection of personal information under an approved code of conduct, may lodge a complaint with the Regulator against the determination on payment of a prescribed fee.

(4) The adjudicator's determination continues to have effect unless and until the Regulator makes a determination under Chapter 10 relating to the complaint.

Guidelines about codes of conduct

62.(1) The Regulator may provide written guidelines -

(a) to assist bodies to develop codes of conduct or to apply approved codes of conduct;

(b) relating to making and dealing with complaints under approved codes of conduct; and

(c) about matters the Regulator may consider in deciding whether to approve a code of conduct or a variation of an approved code of conduct.

(2) Before providing guidelines for the purposes of paragraph (1)(b), the Regulator must give everyone the Regulator considers has a real and substantial legitimate interest in the matters covered by the proposed guidelines an opportunity to comment on them.

(3) The Regulator must publish guidelines provided under subsection (1) in the Government Gazette.

Register of approved codes of conduct

63.(1) The Regulator must keep a register of approved codes of conduct.

(2) The Regulator may decide the form of the register and how it is to be kept.

(3) The Regulator must make the register available to the public in the way that the Regulator determines.

(4) The Regulator may charge reasonable fees for -

(a) making the register available to the public; or

(b) providing copies of, or extracts from, the register.

Review of operation of approved code of conduct

64.(1) The Regulator may, at its own instance, review the operation of an approved code of conduct.

(2) The Regulator may do one or more of the following for the purposes of the review -

(a) consider the process under the code for making and dealing with complaints;

(b) inspect the records of an adjudicator for the code;

(c) consider the outcome of complaints dealt with under the code;

(d) interview an adjudicator for the code; and

(e) appoint experts to review those provisions of the code that the Regulator believes require expert evaluation.

(3) The review may inform a decision by the Regulator under section 60 to revoke the approved code of conduct with immediate effect or at a future date to be determined by the Regulator.

Effect of failure to comply with code

65. If a code of conduct issued under section 57 of this Act is in force, failure to comply with the code is deemed to be a breach of an information protection principle.

CHAPTER 8
RIGHTS OF DATA SUBJECTS RELATING TO UNSOLICITED ELECTRONIC COMMUNICATIONS AND AUTOMATED DECISION MAKING

Unsolicited electronic communications

66.(1) The processing of personal information of a data subject for the purpose of direct marketing by means of automatic calling machines, facsimile machines, SMSs or electronic mail is prohibited unless the data subject -

(a) has given his, her or its consent to the processing; or

(b) is a customer of the responsible party, subject to the provisions set out in section 66(2).

(2) A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of sec 66(1)(b) -

(a) if the responsible party has obtained the contact details of the data subject in the

context of the sale of a product or service;

(b) for the purpose of direct marketing of the responsible party's own similar products or services; and

(c) if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details -

(i) at the time when the information was collected; and

(ii) on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

(3) Any communication for the purpose of direct marketing must contain -

(a) details of the identity of the sender or the person on whose behalf the communication has been sent; and

(b) an address or other contact details to which the recipient may send a request that such communications cease.

Directories

67.(1) A data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its personal information is included, must be informed, free of charge and before the information is included in the directory -

(a) about the purpose(s) of the directory; and

(b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.

(2) A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.

(3) Subsections (1) and (2) do not apply to editions of directories that were produced in printed or off-line electronic form prior to the entry into force of this section.

(4) If the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the information protection principles prior to the entry into force of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received the information required by section 67(1) above.

Automated decision making

68.(1) Subject to subsection 2, no one may be subject to a decision to which are attached legal consequences for him or her, or which affects him or her to a substantial degree, that has been taken solely on the basis of the automated processing of personal information intended to provide a profile of certain aspects of his or her personality or personal habits.

(2) The provisions of subsection (1) do not apply if the decision -

(a) has been taken in connection with the conclusion or execution of a contract, and -
  (i) the request of the data subject in terms of the contract has been met; or
  (ii) appropriate measures have been taken to protect the data subject's legitimate interests; or

(b) is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

(3) The appropriate measures, referred to in subsection 2(a)(ii), must -

(a) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and

(b) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of subsection

(a).

CHAPTER 9
TRANSBORDER INFORMATION FLOWS

Transfers of personal information outside the Republic

69. A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless -

(a) the recipient of the information is subject to a law, binding code of conduct or contract which -
  (i) effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles; and
  (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

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

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

(e) the transfer is for the benefit of the data subject, and -
  (i) it is reasonably impracticable to obtain the consent of the data subject to that transfer; and
  (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

CHAPTER 10

ENFORCEMENT

Interference with the protection of the personal information of a data subject

70. For the purposes of this Chapter, interference with the protection of the personal information of a data subject consists, in relation to that data subject, of -

(a) any breach of the information protection principles set out in Chapter 3 of this Act;

(b) non-compliance with any of sections 21, 47, 66, 67, 68 and 69;

(c) a breach of the provisions of a code of conduct issued in terms of section 57.

Complaints

71. Any person may submit a complaint to the Regulator in the prescribed manner and form -

(a) alleging interference with the protection of the personal information of a data subject; or

(b) in terms of subsection 61(3) if the data subject is aggrieved by the determination of an adjudicator.

Mode of complaint to Regulator

72.(1) A complaint to the Regulator may be made either orally or in writing.

(2) A complaint made orally must be put in writing as soon as reasonably practicable.

(3) The Regulator must give such reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Regulator, to put the complaint in writing.

Investigation by Regulator

73.(1) The Regulator, after receipt of a complaint made in terms of section 71, must –

(a) investigate any alleged interference with the protection of the personal information of a data subject in the prescribed manner;

(b) act, where appropriate, as conciliator in relation to any such interference in the prescribed manner; and

(c) take such further action as is contemplated by this Chapter of this Act.

(2) The Regulator may, on its own initiative, commence an investigation under subsection (1)of this section.

Action on receipt of complaint

74.(1) On receiving a complaint under this Chapter of this Act, the Regulator may -

(a) investigate the complaint; or

(b) decide, in accordance with section 75 of this Act, to take no action on the complaint.

(2) The Regulator must, as soon as is reasonably practicable, advise the complainant and the responsible party to whom the complaint relates of the procedure that the Regulator proposes to adopt under subsection (1) of this section.

Regulator may decide to take no action on complaint

75.(1) The Regulator, after investigating a complaint received in terms of section 71, may decide to take no action or, as the case may require, no further action, in respect of the complaint if, in the Regulator's opinion -

(a) the length of time that has elapsed between the date when the subject-matter of the

complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(b) the subject-matter of the complaint is trivial;

(c) the complaint is frivolous or vexatious or is not made in good faith;

(d) the complainant does not desire that action be taken or, as the case may be, continued;

(e) the complainant does not have a sufficient personal interest in the subject-matter of the complaint; or

(f) in cases where the complaint relates to a matter in respect of which a code of conduct is in force and the code of conduct makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.

(2) Notwithstanding anything in subsection (1), the Regulator may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Regulator that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

(3) In any case where the Regulator decides to take no action, or no further action, on a complaint, the Regulator must inform the complainant of that decision and the reasons for it.

Referral of complaint to regulatory body

76.(1) If, on receiving a complaint under this part of the Act, the Regulator considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body, the Regulator must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned.

(2) If the Regulator determines that the complaint should be dealt with by another body as

described above, the Regulator must forthwith refer the complaint to this body to be dealt with accordingly and must notify the complainant of the action that has been taken.

Pre-investigation Proceedings of Regulator

77. Before proceeding to investigate any matter under this Chapter of this Act, the Regulator must, in the prescribed manner, inform -

(a) the complainant, the data subject to whom the investigation relates (if not the complainant) and any person alleged to be aggrieved (if not the complainant), of the Regulator's intention to conduct the investigation; and

(b) the responsible party to whom the investigation relates of the --

(i) details of the complaint or, as the case may be, the subject-matter of the investigation; and

(ii) right of that responsible party to submit to the Regulator, within a reasonable time, a written response in relation to the complaint or, as the case may be, the subject-matter of the investigation.

Settlement of complaints

78. If it appears from a complaint, or any written response made in relation to a complaint under section 77(b)(ii) of this Act, that it may be possible to secure a settlement between any of the parties concerned and, if appropriate, a satisfactory assurance against the repetition of any action that is the subject-matter of the complaint or the doing of further actions of a similar kind by the person concerned, the Regulator may, without investigating the complaint or, as the case may be, investigating the complaint further, in the prescribed manner, use its best endeavours to secure such a settlement and assurance.

Investigation proceedings of the Regulator

79. For the purposes of the investigation of a complaint the Regulator may -

(a) summon and enforce the appearance of persons before the Regulator and compel them to give oral or written evidence on oath and to produce any records and things that the Regulator considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Regulator sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, subject to section 80, enter and search any premises occupied by a responsible party;

(e) converse in private with any person in any premises entered under section 82 subject to section 80; and

(f) otherwise carry out in those premises any inquiries that the Regulator sees fit in terms of section 80.

Issue of warrants

80.(1) A Judge of the High Court, a regional magistrate or a magistrate, if satisfied by information on oath supplied by the Regulator that there are reasonable grounds for suspecting that -

(a) a responsible party is interfering with the protection of the personal information of a data subject, or

(b) an offence under this Act has been or is being committed,

and that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, that are within the jurisdiction of that judge or magistrate, may, subject to subsection 2, grant a warrant to enter and search such premises.

(2) A warrant issued under subsection (1) authorises the Regulator or any of its officers or staff, subject to section 82, at any time within seven days of the date of the warrant to enter the premises as identified in the warrant, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal information and to inspect and seize any record, other material or equipment found there which may be such evidence as is mentioned in that sub-section.

Requirements for issuing of warrant

81.(1) A Judge or magistrate must not issue a warrant under section 80 unless satisfied -

(a) that the Regulator has given seven (7) days' notice in writing to the occupier of the premises in question demanding access to the premises;

(b) that either -

(i) access was demanded at a reasonable hour and was unreasonably refused, or

(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by any of the Regulator's members or officers or staff to permit the members or the officer or member of staff to do any of the things referred to in section 80(2),

(c) that the occupier, has, after the refusal, been notified by the Regulator of the application for the warrant and has had an opportunity of being heard on the question whether the warrant should be issued.

(2) Subsection (1) does not apply if the judge or magistrate is satisfied that the case is one of urgency or that compliance with those provisions would defeat the object of the entry.

(3) A judge or magistrate who issues a warrant under section 80 must also issue two copies of it and certify them clearly as copies.

Execution of warrants

82.(1) A person executing a warrant issued under section 80 may use such reasonable force as may be necessary.

(2) A warrant issued under this section must be executed at a reasonable hour unless it appears to the person executing it that there are reasonable grounds for suspecting that the evidence in question would not be found if it were so executed.

(3) If the person who occupies the premises in respect of which a warrant is issued under section 76 is present when the warrant is executed, he or she must be shown the warrant and supplied with a copy of it; and if that person is not present a copy of the warrant must be left in a prominent place on the premises.

(4) A person seizing anything in pursuance of a warrant under section 80 must give a receipt to the occupier or leave it on the premises.

(5) Anything so seized may be retained for so long as is necessary in all the circumstances but the person in occupation of the premises in question must be given a copy of any documentation that is seized if he or she so requests and the person executing the warrant considers that it can be done without undue delay.

(6) A person authorised to conduct an entry and search in terms of section 80 must be accompanied and assisted by a police officer.

(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard for each person's right to dignity, freedom, security and privacy.

(8) A person who enters and searches premises under this section, before questioning any person -

(a) must advise that person of the right to be assisted at the time by an advocate or attorney; and

(b) allow that person to exercise that right.

Matters exempt from search and seizure

83. If the Regulator has authorised the processing of personal information in terms of section 34, that information is not subject to search and seizure empowered by a warrant issued under section 80.

Communication between legal adviser and client exempt

84.(1) Subject to the provisions of this section, the powers of search and seizure conferred by a warrant issued under section 80 must not be exercised in respect of -

(a) any communication between a professional legal adviser and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights; or

(b) any communication between a professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before a court) and for the purposes of such proceedings.

(2) Subsection (1) applies also to -

(a) any copy or other record of any such communication as is there mentioned; and

(b) any document or article enclosed with or referred to in any such communication if made in connection with the giving of any advice or, as the case may be, in connection with or in contemplation of and for the purposes of such proceedings as are there mentioned.

Objection to search and seizure

85. If the person in occupation of any premises in respect of which a warrant is issued under this Act objects to the inspection or seizure under the warrant of any material on the ground that it -

(a) contains privileged information and refuses the inspection or removal of such article

or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the registrar of the High Court which has jurisdiction or his or her delegate, to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not; or

(b) consists partly of matters in respect of which those powers are not exercisable, he or she must, if the person executing the warrant so requests, furnish that person with a copy of so much of the material as is not exempt from those powers.

Return of warrants

86. A warrant issued under this section must be returned to the court from which it was issued-

(a) after being executed; or

(b) if not executed within the time authorised for its execution;

and the person who has executed the warrant must make an endorsement on it stating what powers have been exercised by him or her under the warrant.

Assessment

87.(1) The Regulator, on its own initiative, or at the request by or on behalf of the responsible party, data subject or any other person must make an assessment in the manner prescribed, whether an instance of processing of personal information complies with the provisions of this Act.

(2) The Regulator must make the assessment if it appears to be appropriate, unless, where the assessment is made on request, it has not been supplied with such information as it may reasonably require in order to -

(a) satisfy itself as to the identity of the person making the request, and

(b) enable it to identify the action in question.

(3) The matters to which the Regulator may have regard in determining whether it is appropriate to make an assessment include the extent to which the request appears to it to raise a matter of substance, and if the assessment is made on request -

(a) any undue delay in making the request; and

(b) whether or not the person making the request is entitled to make an application

under Principle 8 (access) in respect of the personal information in question.

(4) If the Regulator has received a request under this section it must notify the requester -

(a) whether it has made an assessment as a result of the request; and

(b) to the extent that it considers appropriate, having regard in particular to any exemption from Principle 8 applying in relation to the personal information concerned, of any view formed or action taken as a result of the request.

Information notice

88.(1) If the Regulator -

(a) has received a request under section 87 in respect of any processing of personal information; or

(b) reasonably requires any information for the purpose of determining whether the responsible party has interfered or is interfering with the protection of the personal information of a data subject;

it may serve the responsible party with a notice (in this Act referred to as "an information notice") requiring the responsible party to furnish the Regulator, within a specified period, in a form specified in the notice, with an independent auditor's report indicating that the processing is taking place in compliance with the provisions of the Act, or with such information relating to the request

or to compliance with the Act as is so specified.

(2) An information notice must contain particulars of the rights of appeal conferred by section 92, and -

(a) in a case falling within subsection (1)(a), a statement that the Regulator has received a request under section 87 in relation to the specified processing; or

(b) in a case falling within subsection (1)(b), a statement that the Regulator regards the specified information as relevant for the purpose of determining whether the responsible party has complied, or is complying, with the information protection principles and the reasons for regarding it as relevant for that purpose.

(3) Subject to subsection (5), the period specified in an information notice must not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that the information is required as a matter of urgency, it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require the information to be furnished before the end of a period of three days beginning with the day on which the notice is served.

(6) An information notice may not require a responsible party to furnish the Regulator with any of the following information -

(a) any communication between a professional legal adviser and his or her client in connection with the giving of legal advice on the client's obligations, liabilities or rights under this Act; or

(b) any communication between a professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before a court) and for the purposes of such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser include any person representing such a client.

(8) An information notice may not require a responsible party to furnish the Regulator with information that would, by revealing evidence of the commission of any offence other than an offence under this Act, expose the responsible party to criminal proceedings.

(9) The Regulator may cancel an information notice by written notice to the responsible party on whom it was served.

(10) After completing the assessment referred to in section 87 the Regulator -

(a) must report to the responsible party the results of the assessment and any recommendations that the Regulator considers appropriate; and

(b) may, in appropriate cases, require the responsible party, within a specified time, to inform the Regulator of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(11) The Regulator may make public any information relating to the personal information management practices of a responsible party that has been the subject of an assessment under this section if the Regulator considers it in the public interest to do so.

(12) A report made by the Regulator under section 88(10) is deemed to be the equivalent of an enforcement notice served in terms of section 90 of this Act.

Parties to be informed of developments during and result of investigation

89. If an investigation is made following a complaint, and -

a) the Regulator believes that no interference with the protection of the personal information of a data subject has taken place and therefore does not serve an enforcement notice;

b) an enforcement notice is served in terms of section 90;

c) a served enforcement notice is cancelled in terms of section 91;

d) an appeal is lodged against the enforcement notice for cancellation or variation of the notice in terms of section 92; or

e) an appeal against an enforcement notice is allowed, the notice is substituted or the appeal is dismissed in terms of 93,

the Regulator must inform the complainant and the responsible party, as soon as reasonably practicable, in the manner prescribed of any new development in and the result of the investigation.

Enforcement notice

90.(1) If the Regulator is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject, the Regulator may serve the responsible party with a notice (in this Act referred to as "an enforcement notice") requiring the responsible party to do either or both of the following -

(a) to take specified steps within a period specified in the notice, or to refrain from taking such steps; or

(b) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice.

(2) An enforcement notice must contain -

(a) a statement indicating the nature of the interference with the protection of the personal information of the data subject and the reasons for reaching that conclusion; and

(b) particulars of the rights of appeal conferred by section 92.

(3) Subject to subsection (4), an enforcement notice may not require any of the provisions of the notice to be complied with before the end of the period within which an appeal may be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that an enforcement notice should be complied with as a matter of urgency it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require any of the provisions of the notice to be complied with before the end of a period of three days beginning with the day on which the notice is served.

Cancellation of enforcement notice

91.(1) A responsible party on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal may be brought against that notice, apply in writing to the Regulator for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the information protection principles.

(2) If the Regulator considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the information protection principle or principles to which it relates, it may cancel or vary the notice by written notice to the responsible party on whom it was served.

Right of appeal

92.(1) A responsible party on whom an information or enforcement notice has been served may, within thirty (30) days of receiving the notice, appeal to the High Court having jurisdiction for the setting aside or variation of the notice.

(2) A complainant, who has been informed of the result of the investigation in terms of section 75(3) or section 91, may, within thirty (30) days of receiving the result, appeal to the High Court

having jurisdiction against the result.

Consideration of appeal

93.(1) If in an appeal under section 92 the court considers -

(a) that the notice against which the appeal is brought is not in accordance with the law; or

(b) to the extent that the notice involved an exercise of discretion by the Regulator, that it ought to have exercised its discretion differently;

the court must allow the appeal and may set aside the notice or substitute such other notice or decision as should have been served or made by the Regulator.

(2) In such an appeal, the court may review any determination of fact on which the notice in question was based.

Civil action for damages

94.(1) A data subject, or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act in terms of section 70, whether or not there is intent or negligence on the part of the responsible party.

(2) In the event of a breach the responsible party may raise any of the following defences against an action for damages -

(a) vis major;

(b) consent of the plaintiff;

(c) fault on the part of the plaintiff;

(d) compliance was not reasonably practicable in the circumstances of the particular case; or

(e) the Regulator authorised the breach in terms of section 34 of this Act.

(3) A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable including -

(a) for payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;

(b) aggravated damages, in a sum determined in the discretion of the Court;

(c) interest; and

(d) costs of suit on such scale as may be determined by the Court.

(4) Any amount awarded to the Regulator in terms of subsection (3) must be dealt with in the following manner -

(a) the full amount must be deposited into a specially designated trust account established by the Regulator with an appropriate financial institution;

(b) as a first charge against the amount, the Regulator may recover all reasonable expenses incurred in bringing proceedings at the request of a data subject in terms of subsection (1) and in administering the distributions made to the data subject(s) in terms of subsection (5);

(c) the balance, if any remaining (referred to as the 'distributable balance') must be distributed by the Regulator to the data subject(s) at whose request the proceedings were brought.

(5) Any amount not distributed within three (3) years from the date of the first distribution of payments in terms of subsection (2), accrues to the Regulator in the Regulator's official capacity.

(6) The distributable balance must be distributed on a pro rata basis to the data subject(s)

referred to in subsection (1).

(7) A Court issuing any order under this section must order it to be published in the Gazette and by such other appropriate public media announcement as the Court considers appropriate.

(8) Any civil action instituted under this section may be withdrawn, abandoned or compromised, but any agreement or compromise must be made an order of Court.

(9) If civil action has not been instituted, any agreement or settlement (if any) may, on application to the Court by the Regulator after due notice to the other party, be made an order of Court and must be published in the Gazette and by such other public media announcement as the Court considers appropriate.

CHAPTER 11
OFFENCES AND PENALTIES

Obstruction of Regulator

95**.** Any person who hinders, obstructs or unlawfully influences the Regulator or any person acting on behalf or under the direction of the Regulator in the performance of the Regulator's duties and functions under this Act, is guilty of an offence.

Breach of confidentiality

96. Any person who contravenes the provisions of section 47 is guilty of an offence.

Obstruction of execution of warrant

97. Any person who-

(a) intentionally obstructs a person in the execution of a warrant issued under section 80; or

(b) fails without reasonable excuse to give any person executing such a warrant such assistance as he may reasonably require for the execution of the warrant;

is guilty of an offence.

Failure to comply with enforcement or information notices

98.(1) A responsible party which fails to comply with an enforcement notice served in terms of section 90, is guilty of an offence.

(2) A responsible party which, in purported compliance with an information notice -

(a) makes a statement knowing it to be false in a material respect, or

(b) recklessly makes a statement which is false in a material respect;

is guilty of an offence.

Penal sanctions

99. Any person convicted of an offence in terms of this Act, is liable -

(a) in the case of a contravention of section 95, to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment; or

(b) in any other case, to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and imprisonment.

Magistrate's Court jurisdiction to impose penalties

100. Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in section 99.

CHAPTER 12
MISCELLANEOUS

Repeal and amendment of laws

101. The laws mentioned in the Schedule to this Act are amended to the extent indicated in the third column of the Schedule.

Regulations

102. The Minister for Justice and Constitutional Development may make regulations on –

(a) any matter which this Act requires or permits to be prescribed;
(b) the monitoring of this Act and the establishment of the Regulator; and
(c) any other matter which may be necessary for the application of this Act.

Transitional arrangements

103.(1) Processing which is taking place on the date when this Act comes into force and does not conform to it must within one year of such date, be made to conform and thereafter be notified to the Regulator in terms of section 17(1).

(2) The period of one year referred to in subsection (1) may be extended by regulation to a maximum of three (3) years.

(3) Section 56(2) does not apply to processing referred to in section 55, which is taking place on the date of commencement of this Act, or as the case may be, of the legislation, regulations or codes of conduct applying to such processing.

Short title and commencement

104.(1) This Act is the Protection of Personal Information Act, 2008, and commences on a date determined by the President by Proclamation.

(2) Different dates of commencement may be determined in respect of different provisions of this Act or in respect of different class or classes of information and bodies.

SCHEDULE

AMENDMENT OF LAWS

No and year of law	Short title	Extent of amendment
Act No 25 of 2002	Electronic Communications and Transactions Act	**1.** The repeal of section 45. **2.** The repeal of sections 50 and 51 of Chapter VIII. **3.** The amendment of section 1 by substituting the definition of “personal information” for the following definition - **“personal information”** means information relating to an identifiable natural person, including, but not limited to - a) information relating to the race, gender,

		sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; b) information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, email address, physical address, telephone number or other particular assigned to the person; d) the blood type or any other biometric information of the person; e) the personal opinions, views or preferences of the person; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person. but excludes information about an individual who has been dead for more than 20 years.
Act No 18 of 2005	National Credit Act	**4.** Amendment of section 55 by -

		(a) the creation of a paragraph (a) in subsection (2) by the insertion of the letter (a) at the beginning of the subsection; (b) the insertion after the newly created paragraph(a) of the following paragraph: "(b) The information protection provisions as set out in sections 68 and 70(1)-(4) will be subject to the compliance procedures set out in Chapters X and XI of the Protection of Personal Information Act, 2008." **5.** Amendment of section 68 by the deletion of subsection (2).
Act No 2 of 2000	Promotion of Access to Information Act	**6.** Amendment of section 1 by the substitution of the definition of "personal information" for the following definition **-** **"personal information"** means information relating to an identifiable natural person, including, but not limited to - a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; b) information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, email

		address, physical address, telephone number or other particular assigned to the person; d) the blood type or any other biometric information of the person; e) the personal opinions, views or preferences of the person; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person. but excludes information about an individual who has been dead for more than 20years. **7.** Amendment of section 1 by the insertion after the definition of “record” of the following definition- **“Regulator”** means the Information Protection Regulator established in section 35 of the Protection of Personal Information Act, 2008. **8.** Amendment of section 11 by substituting the word “includes” with the word “excludes”. **9.** Amendment of section 22 by -

		(a) deleting the words “other than a personal requester” in subsection (1); (b) deleting the words “other than a personal requester” in subparagraphs (a) and (b) of subsection (2).
	Promotion of Access to Information Act (continued)	**10**. Amendment of section 54 by - (a) deleting the words “other than a personal requester” in subsection (1); (b) deleting the words “other than a personal requester” in subparagraph (a) and after the words “require the requester” in subsection (2). **11.** The repeal of section 88. **12.** Amendment of the heading of Part 5 by substituting the words “Human Rights Commission” with the words “Information Protection Regulator”. **13.** Amendment of sections 1,10, 32, 83, 84 and 85 by substituting the words “Human Rights Commission” wherever they appear, with the word “Regulator”.

ANNEXURE D

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Official Journal L 281 , 23/11/1995 P. 0031 - 0050

1. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion

and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to

coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is

necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the

rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured

according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public

administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority

responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas

the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member

States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply

with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the

controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of

operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a

necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve

those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of 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 demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must

consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of 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 provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority,

Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the

light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject

and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) 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

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) 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.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces 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; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,

- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national

provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(1) OJ No L 197, 18. 7. 1987, p. 33.

ANNEXURE E

OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

1. PREFACE

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23rd September, 1980.

The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23rd September, 1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS:

That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

1. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

2. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

3. That Member countries agree as soon as possible on specific procedures of consultation

and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA PART ONE.

GENERAL DEFINITIONS.

1. For the purposes of these Guidelines:

a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

b) "personal data" means any information relating to an identified or identifiable individual (data subject);

c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

a) as few as possible, and

b) made known to the public.

5 . In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

* within a reasonable time;
* at a charge, if any, that is not excessive;
* in a reasonable manner; and
* in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;
b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
c) provide for reasonable means for individuals to exercise their rights;

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

information exchange related to these Guidelines, and

mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

EXPLANATORY MEMORANDUM: INTRODUCTION

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.
The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the

Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions. The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

I. GENERAL BACKGROUND

The Problems

1. The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

2. The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex

synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

3. As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, e.g. those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

Activities at national level

4. Of the OECD Member countries more than one-third have so far enacted one or several laws which, among other things, are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness. In federal states, laws of this kind may be found both at the national and at the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (*lois sur la protection des données*), whereas in English speaking countries they are usually known as "privacy protection laws". Most of the statutes were enacted after 1973 and this present period may be described as one of continued or even widened legislative activity. Countries which already have statutes in force are turning to new areas of protection or are engaged in revising or complementing existing statutes. Several other countries are entering the area and have bills pending or are studying the problems with a view to preparing legislation. These national efforts, and not least the extensive reports and research papers prepared by public committees or similar bodies, help to clarify the problems and the advantages and implications of various solutions. At the present stage, they provide a solid basis for international action.

5. The approaches to protection of privacy and individual liberties adopted by the various countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of

data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions. Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning with the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

6. Differences between national approaches as apparent at present in laws, bills or proposals for legislation refer to aspects such as the scope of legislation, the emphasis placed on different elements of protection, the detailed implementation of the broad principles indicated above, and the machinery of enforcement. Thus, opinions vary with respect to licensing requirements and control mechanisms in the form of special supervisory bodies ("data inspection authorities"). Categories of sensitive data are defined differently, the means of ensuring openness and individual participation vary, to give just a few instances. Of course, existing traditional differences between legal systems are a cause of disparity, both with respect to legislative approaches and the detailed formulation of the regulatory framework for personal data protection.

International aspects of privacy and data banks

7. For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

8. One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.

9. There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in

view of the international mobility of people, goods and commercial and scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

Relevant international activities

10. There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (e.g. with regard to the taking of evidence).

11. A number of international agreements deal in a more general way with the issues which are at present under discussion, viz. the protection of privacy and the free dissemination of information. They include the European Convention of Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).

12. However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions.

13. In 1973 and 1974 the Committee of Ministers of the Council of Europe adopted two resolutions concerning the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sectors respectively. Both resolutions recommend that the governments of the Member states of the Council of Europe take steps to give effect to a number of basic principles of protection relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities.

14. Subsequently the Council of Europe, on the instructions of its Committee of Ministers, began to prepare an international Convention on privacy protection in relation to data processing abroad and transfrontier data processing. It also initiated work on model regulations for medical data banks and rules of conduct for data processing professionals. The Convention was adopted by the Committee of Ministers on 17th September 1980. It seeks to establish basic principles of data protection to be enforced by Member countries, to reduce restrictions on transborder data flows between the Contracting Parties on the basis of reciprocity, to bring

about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the convention.

15. The European Community has carried out studies concerning the problems of harmonization of national legislations within the Community, in relation to transborder data flows and possible distortions of competition, the problems of data security and confidentiality, and the nature of transborder data flows. A sub-committee of the European Parliament held a public hearing on data processing and the rights of the individual in early 1978. Its work has resulted in a report to the European Parliament in spring 1979. The report, which was adopted by the European Parliament in May 1979, contains a resolution on the protection of the rights of the individual in the face of technical developments in data processing.

Activities of the OECD

16. The OECD programme on transborder data flows derives from computer utilisation studies in the public sector which were initiated in 1969. A Group of Experts, the Data Bank Panel, analysed and studied different aspects of the privacy issue, e.g. in relation to digital information, public administration, transborder data flows, and policy implications in general. In order to obtain evidence on the nature of the problems, the Data Bank Panel organised a Symposium in Vienna in 1977 which provided opinions and experience from a diversity of interests, including government, industry, users of international data communication networks, processing services, and interested intergovernmental organisations.

17. A number of guiding principles were elaborated in a general framework for possible international action. These principles recognised (a) the need for generally continuous and uninterrupted flows of information between countries, (b) the legitimate interests of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens, (c) the economic value of information and the importance of protecting "data trade" by accepted rules of fair competition, (d) the needs for security safeguards to minimise violations of proprietary data and misuse of personal information, and (e) the significance of a commitment of countries to a set of core principles for the protection of personal information.

18. Early in 1978 a new ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD which was instructed to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonization of national legislations, without this precluding at a later date the establishment of an international Convention. This work was to be carried out in close co-operation with the Council of Europe and the European Community and to be completed by lst July 1979.

19. The Expert Group, under the chairmanship of the Honourable Mr. Justice Kirby, Australia, and with the assistance of Dr. Peter Seipel (Consultant), produced several drafts and discussed various reports containing, for instance, comparative analyses of different approaches to legislation in this field. It was particularly concerned with a number of key issues set out below.

a) The specific, sensitive facts issue

The question arose as to whether the Guidelines should be of a general nature or whether they should be structured to deal with different types of data or activities (e.g. credit reporting). Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive.

b) The ADP issue

The argument that ADP is the main cause for concern is doubtful and, indeed, contested.

c) The legal persons issue

Some, but by no means all, national laws protect data relating to legal persons in a similar manner to data related to physical persons.

d) The remedies and sanctions issue

The approaches to control mechanisms vary considerably: for instance, schemes involving supervision and licensing by specially constituted authorities might be compared to schemes involving voluntary compliance by record-keepers and reliance on traditional judicial remedies in the Courts.

e) The basic machinery or implementation issue

The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions (protection of data against unauthorised interference, fire, and similar occurrences) should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level "machinery" questions which should be left to domestic implementation.

f) The choice of law issue

The problems of choice of jurisdiction, choice of applicable law and recognition of foreign

judgements have proved to be complex in the context of transborder data flows. The question arose, however, whether and to what extent it should be attempted at this stage to put forward solutions in Guidelines of a non-binding nature.

g) The exceptions issue

Similarly, opinions may vary on the question of exceptions. Are they required at all? If so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated?

h) The bias issue

Finally, there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.

20. During its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was made to avoid unnecessary differences between the texts produced by the two organisations; thus, the set of basic principles of protection are in many respects similar. On the other hand, a number of differences do occur. To begin with, the OECD Guidelines are not legally binding, whereas the Council of Europe has produced a convention which will be legally binding among those countries which ratify it. This in turn means that the question of exceptions has been dealt with in greater detail by the Council of Europe. As for the area of application, the Council of Europe Convention deals primarily with the automatic processing of personal data whereas the OECD Guidelines apply to personal data which involve dangers to privacy and individual liberties, irrespective of the methods and machinery used in their handling. At the level of details, the basic principles of protection proposed by the two organisations are not identical and the terminology employed differs in some respects. The institutional framework for continued co-operation is treated in greater detail in the Council of Europe Convention than in the OECD Guidelines.

21. The Expert Group also maintained co-operation with the Commission of the European Communities as required by its mandate.

II. THE GUIDELINES

A. PURPOSE AND SCOPE

General

22. The Preamble of the Recommendation expresses the basic concerns calling for action. The Recommendation affirms the commitment of Member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.

23. The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, i.e. principles which are chiefly concerned with relationships between Member countries.

24. Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries.

Objectives

25. The core of the Guidelines consists of the principles set out in Part Two of the Annex. It is recommended to Member countries that they adhere to these principles with a view to:

a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;

b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;

c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and

d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.

As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.

26. Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:

a) effective national measures for the protection of privacy and individual liberties;

b) avoidance of practices involving unfair discrimination between individuals; and

c) bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data.

Level of detail

27. The level of detail of the Guidelines varies depending upon two main factors, viz. (a) the extent of consensus reached concerning the solutions put forward, and (b) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation. To conclude, there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly.

Non-Member countries

28. The Recommendation is addressed to Member countries and this is reflected in several provisions which are expressly restricted to relationships between Member countries (see Paragraphs 15, 17 and 20 of the Guidelines). Widespread recognition of the Guidelines is, however, desirable and nothing in them should be interpreted as preventing the application of relevant provisions by Member countries to non-Member countries. In view of the increase in transborder data flows and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-Member countries and appropriate international organisations.

The broader regulatory perspective

29. It has been pointed out earlier that the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data. The Guidelines constitute a new instrument, in addition to other, related international instruments governing such issues as human rights, telecommunications, international trade, copyright, and

various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies.

30. Some Member countries have emphasized the advantages of a binding international Convention with a broad coverage. The Mandate of the Expert Group required it to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises.

Legal persons, groups and similar entities

31. Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.

32. Similarly, it is debatable to what extent people belonging to a particular group (i.e. mentally disabled persons immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group.

33. On the other hand, the Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals and it is left to Member countries to draw dividing lines and decide policies with regard to corporations, groups and similar bodies (cf. paragraph 49 below).

Automated and non-automated data

34. In the past, OECD activities in privacy protection and related fields have focused on automatic data processing and computer networks. The Expert Group has devoted special

attention to the issue of whether or not these Guidelines should be restricted to the automatic and computer-assisted processing of personal data. Such an approach may be defended on a number of grounds, such as the particular dangers to individual privacy raised by automation and computerised data banks, and increasing dominance of automatic data processing methods, especially in transborder data flows, and the particular framework of information, computer and communications policies within which the Expert Group has set out to fulfil its Mandate.

35. On the other hand, it is the conclusion of the Expert Group that limiting the Guidelines to the automatic processing of personal data would have considerable drawbacks. To begin with, it is difficult, at the level of definitions, to make a clear distinction between the automatic and non-automatic handling of data. There are, for instance, "mixed" data processing systems, and there are stages in the processing of data which may or may not lead to automatic treatment. These difficulties tend to be further complicated by ongoing technological developments, such as the introduction of advanced semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control. Moreover, by concentrating exclusively on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive.

36. Because of the difficulties mentioned, the Guidelines do not put forward a definition of "automatic data processing" although the concept is referred to in the preamble and in paragraph 3 of the Annex. It may be assumed that guidance for the interpretation of the concept can be obtained from sources such as standard technical vocabularies.

37. Above all, the principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties.

38. It should be noted, however, that the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance, candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data. Thus, the Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes. It should be emphasized that the Guidelines are neutral with regard to the particular technology used; automatic methods are only one of the problems

raised in the Guidelines although, particularly in the context of transborder data flows, this is clearly an important one.

B. DETAILED COMMENTS

General

39. The comments which follow relate to the actual Guidelines set out in the Annex to the Recommendation. They seek to clarify the debate in the Expert Group.

Paragraph 1: Definitions

40. The list of definitions has been kept short. The term "data controller" is of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body. The definition excludes at least four categories which may be involved in the processing of data, viz. (a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes; (b) data processing service bureaux which carry out data processing on behalf of others; (c) telecommunications authorities and similar bodies which act as mere conduits; and (d) "dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities. Paragraphs 14 and 19 of the Guidelines provide a basis for efforts in this direction.

41. The terms "personal data" and "data subject" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person.

42. The term "transborder flows of personal data" restricts the application of certain provisions of the Guidelines to international data flows and consequently omits the data flow problems

particular to federal states. The movements of data will often take place through electronic transmission but other means of data communication may also be involved. Transborder flows as understood in the Guidelines includes the transmission of data by satellite.

Paragraph 2: Area of application

43. The Section of the Memorandum dealing with the scope and purpose of the Guidelines introduces the issue of their application to the automatic as against non-automatic processing of personal data. Paragraph 2 of the Guidelines, which deals with this problem, is based on two limiting criteria. The first is associated with the concept of personal data: the Guidelines apply to data which can be related to identified or identifiable individuals. Collections of data which do not offer such possibilities (collections of statistical data in anonymous form) are not included. The second criterion is more complex and relates to a specific risk element of a factual nature, viz. that data pose a danger to privacy and individual liberties. Such dangers can arise because of the use of automated data processing methods (the manner in which data are processed), but a broad variety of other possible risk sources is implied. Thus, data which are in themselves simple and factual may be used in a context where they become offensive to a data subject. On the other hand, the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (e.g. personal notebooks). The dangers referred to in Paragraph 2 of the Guidelines should relate to privacy and individual liberties. However, the protected interests are broad (cf. paragraph 2 above) and may be viewed differently by different Member countries and at different times. A delimitation as far as the Guidelines are concerned and a common basic approach are provided by the principles set out in Paragraphs 7 to 13.

44. As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the public sector. These notions may be defined differently by different Member countries.

Paragraph 3: Different degrees of sensitivity

45. The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved. The framework provided by the basic principles in Part Two of the Guidelines permits Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented, and with respect to the scope of the measures to be taken. In particular, Paragraph 3(b) provides for many "trivial" cases of collection and use of personal data (cf. above) to be completely excluded from the application of the Guidelines. Obviously this does not mean that Paragraph 3 should be regarded as a vehicle for demolishing the standards set up by the Guidelines. But, generally speaking, the Guidelines do not presuppose their uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general

public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth. To conclude, some Member countries may find it appropriate to restrict the application of the Guidelines to the automatic processing of personal data. Paragraph 3(c) provides for such a limitation.

Paragraph 4: Exceptions to the Guidelines

46. To provide formally for exceptions in Guidelines which are part of a non-binding Recommendation may seem superfluous. However, the Expert Group has found it appropriate to include a provision dealing with this subject and stating that two general criteria ought to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public (e.g. through publication in an official government gazette). General knowledge of the existence of certain data or files would be sufficient to meet the second criterion, although details concerning particular data etc. may have to be kept secret. The formula provided in Paragraph 4 is intended to cover many different kinds of concerns and limiting factors, as it was obviously not possible to provide an exhaustive list of exceptions - hence the wording that they include national sovereignty, national security and public policy ("ordre public"). Another overriding national concern would be, for instance, the financial interests of the State ("crédit public"). Moreover, Paragraph 4 allows for different ways of implementing the Guidelines: it should be borne in mind that Member countries are at present at different stages of development with respect to privacy protection rules and institutions and will probably proceed at different paces, applying different strategies, e.g. the regulation of certain types of data or activities as compared to regulation of a general nature ("omnibus approach").

47. The Expert Group recognised that Member countries might apply the Guidelines differentially to different kinds of personal data. There may be differences in the permissible frequency of inspection, in ways of balancing competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him, and so forth. Some examples of areas which may be treated differently are credit reporting, criminal investigation and banking. Member countries may also choose different solutions with respect to exceptions associated with, for example, research and statistics. An exhaustive enumeration of all such situations and concerns is neither required nor possible. Some of the subsequent paragraphs of the Guidelines and the comments referring to them provide further clarification of the area of application of the Guidelines and of the closely related issues of balancing opposing interests (compare with Paragraphs 7, 8, 17 and 18 of the Guidelines). To summarise, the Expert Group

has assumed that exceptions will be limited to those which are necessary in a democratic society.

Paragraph 5: Federal countries

48. In Federal countries, the application of the Guidelines is subject to various constitutional limitations. Paragraph 5, accordingly, serves to underscore that no commitments exist to apply the Guidelines beyond the limits of constitutional competence.

Paragraph 6: Minimum standards

49. First, Paragraph 6 describes the Guidelines as minimum standards for adoption in domestic legislation. Secondly, and in consequence, it has been agreed that the Guidelines are capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level.

Paragraph 7: Collection Limitation Principle

50. As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. Paragraph 7 deals with two issues, viz. (a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and (b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited. There are precedents in European legislation to this effect (race, religious beliefs, criminal records, for instance). On the other hand, it may be held that no data are intrinsically " private" or "sensitive" but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.

51. The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. For one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is

understood that the limits may relate to:

- data quality aspects (i.e. that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc.);

- limits associated with the purpose of the processing of data (i.e. that only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfil the specified purpose);

- "earmarking" of specially sensitive data according to traditions and attitudes in each Member country;

- limits to data collection activities of certain data controllers;

- civil rights concerns.

52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder ("where appropriate") that there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary. Criminal investigation activities and the routine up-dating of mailing lists may be mentioned as examples. Finally, Paragraph 7 does not exclude the possibility of a data subject being represented by another party, for instance in the case of minors, mentally disabled person, etc.

Paragraph 8: Data Quality Principle

53. Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of

archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.

Paragraph 9: Purpose Specification Principle

54. The Purpose Specification Principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time data collection it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g. by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.

Paragraph 10: Use Limitation Principle

55. This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative - see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.

Paragraph 11: Security Safeguards Principle

56. Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasized that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. Paragraph 11 has

a broad coverage. The cases mentioned in the provision are to some extent overlapping (e.g. access/ disclosure). "Loss" of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. "Modified" should be construed to cover unauthorised input of data, and "use" to cover unauthorised copying.

Paragraph 12: Openness Principle

57. The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle (Paragraph 13); for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

Paragraph 13: Individual Participation Principle

58. The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual sub-paragraphs, the following explanations are called for:

59. The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from one situation to another depending on circumstances such as the nature of the data processing activity. Communication of such data "in a reasonable manner" means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable.

The extent to which data subjects should be able to obtain copies of data relating to them is a matter of implementation which must be left to the decision of each Member country.

60. The right to reasons in Paragraph 13(c) is narrow in the sense that it is limited to situations where requests for information have been refused. A broadening of this right to include reasons for adverse decisions in general, based on the use of personal data, met with sympathy in the Expert Group. However, on final consideration a right of this kind was thought to be too broad for insertion in the privacy framework constituted by the Guidelines. This is not to say that a right to reasons for adverse decisions may not be appropriate, e.g. in order to inform and alert a subject to his rights so that he can exercise them effectively.

61. The right to challenge in 13(c) and (d) is broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure (compare with Paragraph 19 of the Guidelines). The right to challenge does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.): such matters will be decided by domestic law and legal procedures. Generally speaking, the criteria which decide the outcome of a challenge are those which are stated elsewhere in the Guidelines.

Paragraph 14: Accountability Principle

62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly. it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Paragraphs 15-18: Basic Principles of International Application

63. The principles of international application are closely interrelated. Generally speaking, Paragraph 15 concerns respect by Member countries for each other's interest in protecting personal data, and the privacy and individual liberties of their nationals and residents. Paragraph 16 deals with security issues in a broad sense and may be said to correspond, at the

international level, to Paragraph 11 of the Guidelines. Paragraphs 17 and 18 deal with restrictions on free flows of personal data between Member countries; basically, as far as protection of privacy and individual liberties is concerned, such flows should be admitted as soon as requirements of the Guidelines for the protection of these interests have been substantially, i.e. effectively, fulfilled. The question of other possible bases of restricting transborder flows of personal data is not dealt with in the Guidelines.

64. For domestic processing Paragraph 15 has two implications. First, it is directed against liberal policies which are contrary to the spirit of the Guidelines and which facilitate attempts to circumvent or violate protective legislation of other Member countries. However, such circumvention or violation, although condemned by all Member countries, is not specifically mentioned in this Paragraph as a number of countries felt it to be unacceptable that one Member country should be required to directly or indirectly enforce, extraterritorially, the laws of other Member countries. -- It should be noted that the provision explicitly mentions the re-export of personal data. In this respect, Member countries should bear in mind the need to support each other's efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent.

65. Secondly, Member countries are implicitly encouraged to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved. By way of illustration, a situation may arise where data on foreign nationals are made available for purposes which serve the particular interests of their country of nationality (e.g. access to the addresses of nationals living abroad).

66. As far as the Guidelines are concerned, the encouragement of international flows of personal data is not an undisputed goal in itself. To the extent that such flows take place they should, however, according to Paragraph 16, be uninterrupted and secure, i.e. protected against unauthorised access, loss of data and similar events. Such protection should also be given to data in transit, i.e. data which pass through a Member country without being used or stored with a view to usage in that country. The general commitment under Paragraph 16 should, as far as computer networks are concerned, be viewed against the background of the International Telecommunications Convention of Malaga-Torremolinos (25th October, 1973). According to that convention, the members of the International Telecommunications Union, including the OECD Member countries, have agreed, inter alia, to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications. Moreover, the members of ITU have agreed to take all possible measures compatible with the telecommunications system used to ensure the secrecy of international correspondence. As regards exceptions, the

right to suspend international telecommunications services has been reserved and so has the right to communicate international correspondence to the competent authorities in order to ensure the application of internal laws or the execution of international conventions to which members of the ITU are parties. These provisions apply as long as data move through telecommunications lines. In their context, the Guidelines constitute a complementary safeguard that international flows of personal data should be uninterrupted and secure.

67. Paragraph 17 reinforces Paragraph 16 as far as relationships between Member countries are concerned. It deals with interests which are opposed to free transborder flows of personal data but which may nevertheless constitute legitimate grounds for restricting such flows between Member countries. A typical example would be attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines. Paragraph 17 establishes a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects. As in Paragraph 15, the re-export of personal data is specifically mentioned - in this case with a view to preventing attempts to circumvent the domestic privacy legislation of Member countries. - The third category of grounds for legitimate restrictions mentioned in Paragraph 17, concerning personal data of a special nature, covers situations where important interests of Member countries could be affected. Generally speaking, however, paragraph 17 is subject to Paragraph 4 of the Guidelines which implies that restrictions on flows of personal data should be kept to a minimum.

68. Paragraph 18 attempts to ensure that privacy protection interests are balanced against interests of free transborder flows of personal data. It is directed in the first place against the creation of barriers to flows of personal data which are artificial from the point of view of protection of privacy and individual liberties and fulfil restrictive purposes of other kinds which are thus not openly announced. However, Paragraph 18 is not intended to limit the rights of Member countries to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment, and related economic conditions for intentional data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

Paragraph 19: National Implementation

69. The detailed implementation of Parts Two and Three of the Guidelines is left in the first place to Member countries. It is bound to vary according to different legal systems and traditions, and Paragraph 19 therefore attempts merely to establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guidelines into effect. The opening sentence shows the different approaches which might be taken by countries, both generally and with respect to control mechanisms (e.g. specially set up

supervisory bodies, existing control facilities such as courts, public authorities, etc.).

70. In Paragraph 19(a) countries are invited to adopt appropriate domestic legislation, the word "appropriate" foreshadowing the judgement by individual countries of the appropriateness or otherwise of legislative solutions. Paragraph 19(b) concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action. Paragraph 19(c) should be given a broad interpretation; it includes such means as advice from data controllers and the provision of assistance, including legal aid. Paragraph 19(d) permits different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise. Paragraph 19(e) dealing with discrimination is directed against unfair practices but leaves open the possibility of "benign discrimination" to support disadvantaged groups, for instance. The provision is directed against unfair discrimination on such bases as nationality and domicile, sex, race, creed, or trade union affiliation.

Paragraph 20: Information Exchange and Compatible Procedures

71. Two major problems are dealt with here, viz. (a) the need to ensure that information can be obtained about rules, regulations, decisions, etc. which implement the Guidelines, and (b) the need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate framework of procedures and compliance requirements. The first problem arises because of the complexity of privacy protection regulation and data policies in general. There are often several levels of regulation (in a broad sense) and many important rules cannot be laid down permanently in detailed statutory provisions; they have to be kept fairly open and left to the discretion of lower-level decision-making bodies.

72. The importance of the second problem is, generally speaking, proportional to the number of domestic laws which affect transborder flows of personal data. Even at the present stage, there are obvious needs for co-ordinating special provisions on transborder data flows in domestic laws, including special arrangements relating to compliance control and, where required, licences to operate data processing systems.

Paragraph 21: Machinery for Co-operation

73. The provision on national procedures assumes that the Guidelines will form a basis for continued co-operation. Data protection authorities and specialised bodies dealing with policy issues in information and data communications are obvious partners in such a co-operation. In particular, the second purpose of such measures, contained in Paragraph 21(ii), i.e. mutual aid in procedural matters and requests for information, is future-oriented: its practical significance is

likely to grow as international data networks and the complications associated with them become more numerous.

Paragraph 22: Conflicts of Laws

74. The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

75. As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best, indicate one applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

76. In view of these difficulties, and considering that problems of conflicts of laws might best be handled within the total framework of personal and non-personal data, the Expert Group has decided to content itself with a statement which merely signals the issues and recommends that Member countries should work towards their solution.

Follow-up

77. The Expert Group called attention to the terms of Recommendation 4 on the Guidelines which suggests that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of the Guidelines.