



**DISCUSSION PAPER 109
Project 124
OCTOBER 2005**

PRIVACY AND DATA PROTECTION

**CLOSING DATE FOR COMMENTS:
28 FEBRUARY 2006**

ISBN 0-621-36326-X

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 Madam Justice L Mailula (Vice-Chairperson)
Adv J J Gauntlett SC
The Honourable Mr Justice C T Howie
Prof I P Maithufi (full-time member)
Ms Z Seedat
The Honourable Mr Justice W L Seriti

The Secretary is Mr W Henegan. 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/salr/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.

PREFACE

This discussion paper, which reflects information accumulated up to the end of August 2005, has been prepared to provide background information, to elicit responses from key parties and to serve as a basis for the Commission's deliberations.

The views, conclusions and proposals in this paper are not to be regarded as the Commission's final views. The paper (which includes draft legislation) is published in full so as to provide persons and bodies wishing to comment or to make suggestions for the reform of this particular branch of the law with sufficient background information to enable them to place focussed submissions before the Commission. A summary of recommendations submitted for comment appears on page (vi). The proposed draft legislation is contained in ***Annexure B***.

The Commission will assume that respondents agree to the Commission quoting from or referring to comments and attributing comments to respondents, unless representations are marked confidential. Respondents should be aware that under sec 32 of the Constitution of the Republic of South Africa, 1996 and under the Promotion of Access to Information Act 2 of 2000 the Commission may have to release information contained in representations.

Respondents are requested to submit **written** comments, representations or requests to the Commission by **28 February 2006** at the address appearing on the previous page. Comment may be sent by e-mail or post.

The Discussion Paper is also available on the Internet at www.doj.gov.za/salrc/index.htm.

Any enquiries should be addressed to the Secretary of the Commission or the researcher allocated to this project, Ananda Louw. Contact particulars appear on the previous page.

SUMMARY OF PRELIMINARY RECOMMENDATIONS

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 our 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 thirty 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 as well as the initiative of the Commonwealth Law Ministers in this regard. In both 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.

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, still to be enacted, National Credit Bill [B18-2005]. All these Acts contain interim provisions regarding information protection in South Africa.

The preliminary recommendations of the Commission, as set out in the Bill accompanying this document as **Annexure B**, can be summarised as follows:¹

- a) Privacy and information protection should 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 should be developed and incorporated in the legislation. The proposed 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 [**Chapter 3, Part A, clauses 7-23**]. Exemptions are furthermore possible for specific sectors in applicable circumstances [**Chapter 4, clauses 32-33**]. Special provision has furthermore been made for the protection of special (sensitive) personal information [**Chapter 3, Part B, clauses 24-31**].
- c) A statutory regulatory agency should be established. Provision has been made for an independent Information Protection Commission with a full-time Information Commissioner to direct the work of the Commission [**Chapter 5, Part A, clauses 34-46**]. The Commission will be responsible for the implementation of both the Protection of Personal Information Act (see Annexure B) and the Promotion of Access to Information Act, 2000. Data subjects will be under an obligation to notify

¹ References in brackets are to the applicable clauses, parts and chapters in the **Protection of Personal Information Bill** set out in **Annexure B** to this Discussion Paper.

the Commission of any processing of personal information before they undertake such processing **[Chapter 6, Part A, clauses 47-51]** 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 52-53]**.

- d) Enforcement of the Bill will be through the Commission 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 Commission may furthermore assist a data subject in claiming compensation from a responsible party for any damage suffered. Obstruction of the Commission's work is regarded in a very serious light and constitutes a criminal offence **[Chapter 8, clauses 63-87 and Chapter 9, clauses 88-92]**.
- 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 Commission 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 Commission 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 54-62]**.
- f) 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 10, clause 94]**.

The preliminary recommendations and draft legislation need to be debated thoroughly. The Commission is seeking feedback regarding all its proposals as set out in the proposed draft Bill. Respondents are requested to respond as comprehensively as possible.

TABLE OF CONTENTS

	Page
INTRODUCTION	(iii)
PREFACE	(v)
SUMMARY OF PRELIMINARY RECOMMENDATIONS	(vi)
LIST OF SOURCES	(xiii)
TABLE OF CASES	(xxv)
SELECTED LEGISLATION	(xxx)
CONVENTIONS, DIRECTIVES, GUIDELINES AND DECLARATIONS	(xxxiv)
CHAPTER 1: INTRODUCTION	1
1.1 History of the investigation	1
1.2 Exposition of the problem	2
1.3 Terms of reference	13
1.4 Methodology	13
CHAPTER 2: RIGHT TO PRIVACY	15
2.1 Recognition of the right to privacy	15
2.2 Nature and scope of the right to privacy	24
2.3 Infringement of the right to privacy	30
2.4 Conclusion	53
CHAPTER 3: SUBSTANTIVE SCOPE OF THE PROPOSED LEGISLATION	56
3.1 General	56
3.2 Automatic and manual files	57
3.3 Sound/image information	59
3.4 Natural v juristic persons	59
3.5 Public v private sector	69
3.6 Critical information	73
3.7 Sensitive information (special personal information)	85
3.8 Household activity	87
3.9 Anonymised/ De-identified information	88
3.10 Professional information (including provider information)	91

3.11	Conclusion	93
CHAPTER 4: PRINCIPLES OF INFORMATION PROTECTION		98
4.1	Origins of the information protection principles	98
a)	Introduction	98
b)	Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention)	100
c)	Organisation for Economic Cooperation and Development Guidelines (OECD Guidelines)	102
d)	European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (EU Directive)	104
e)	United Nations Guidelines	108
f)	Commonwealth Guidelines	109
4.2	Discussion of Information Protection Principles	110
a)	Introduction	110
b)	Principles of Information Protection	112
4.3	Processing of special personal information (sensitive information)	204
4.4	Exemptions and exceptions	215
CHAPTER 5: MONITORING AND SUPERVISION		227
5.1`	Introduction	227
5.2	Enforcement systems	231
a)	Regulatory system	231
c)	Self-regulatory system	245
b)	Co-regulatory system	254
5.3	Submissions received: Evaluation of options identified	256
5.4	The proposed information protection system for South Africa	281
5.5	Notification, regulation and licencing schemes	294
5.6	Codes of conduct	309
5.7	Information matching (profiling)	321
CHAPTER 6: ENFORCEMENT		330

6.1	Introduction	330
6.2	Investigating complaints	333
6.3	Assessment/audit	334
6.4	Advisory approach	336
6.5	Enforcement powers	337
6.6	Courts/ judicial remedies	340
6.7	Compensation	342
6.8	Conclusion	343

CHAPTER 7: CROSS-BORDER INFORMATION TRANSFERS	359
------------------------------------------------------	------------

CHAPTER 8: COMPARATIVE LAW

372

8.1	Introduction	372
8.2	International Directives	373
8.3	United States of America	377
8.4	United Kingdom of Great Britain and Northern Ireland	385
8.5	Kingdom of the Netherlands	388
8.6	New Zealand	391
8.7	Canada	392
8.8	Commonwealth of Australia	397

CHAPTER 9: DRAFT BILL ON THE PROTECTION OF PERSONAL INFORMATION	403
------------------------------------------------------------------------	------------

LIST OF ANNEXURES

ANNEXURE A: LIST OF RESPONDENTS : ISSUE PAPER 24	406
ANNEXURE B: DRAFT LEGISLATION	408

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.

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.

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

Barnard F “Informal Notes from the DMA to the Law Commission re a Possible New Data Privacy Act for South Africa” 14 September 2001.

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.ca/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.ca/polisci/bennett>, accessed on 29/10/2002.

Bennett CJ “The Data Protection Authority: Regulator, Ombudsman, Regulator or Campaigner?” Presentation at 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 for Justice and Constitutional Development to Establish Security Requirements and Frameworks 23 September 2003.

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.

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 “Horizontalty” **Bill of Rights Compendium** Butterworths Constitutional Law Library.

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.

Computer Crime and Intellectual Property Section (CCIPS) “The Electronic Frontier: the Challenge ...Use of the Internet” US Department of Justice March 9 available at <http://www.usdoj.gov/criminal/cybercrime/unla>.

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.

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.

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 2003 accessed at <http://www.privacyinternational.org/survey/phr2004/> on 25/6/2005.

Electronic Privacy Information Centre (EPIC) ***Alert*** Vol 9.23 dated November 19, 2002 available at http://www.epic.org/alert/EPIC_Alert_9.23.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.html/>.

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

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

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

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

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.

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.

Gutwirth S (translated by Casert R) **Privacy and the Information Age** Rowan and 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.

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.

Jones C, Rankin M 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.

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/.

Loukidikes 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.

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

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

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.

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

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.

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

Neethling J, Potgieter JM & Visser PJ ***Law of Delict*** Butterworths Durban 2002.

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.

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 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 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 ***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/>

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.

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

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

Petzer N "Opinion: 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" Presentation 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*** 647-682.

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.

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.

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.

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

telegraph.co.uk Telegraph Group Limited (TGL) and its subsidiary Hollinger Telgraph Ne Media (HTNM) **Privacy Policy** Published on the Internet Tuesday 5 March 2002 .

Tilley A “Data Protection in South Africa and the Right to Access to Information: An Inescapable Clash?” Submission to the SA Law Reform Commission dated 26 August 2002.

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 Patient’s ‘Health Information’” **HHS Fact Sheet** May 9, 2001.

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

Valeri L “Is Technology a Privacy-enhancer or Privacy Threat? Some Thoughts” Presentation 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.

Van Heerden HJO & Neethling J **Unlawful Competition** Butterworths Durban 1995.

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.

Woolman S “Coetzee: The Limitations of Justice Sachs’s Concurrence” 1996 *SAJHR* 12.1 99.

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).

TABLE OF CASES

SOUTH AFRICA

Administrator, Natal v Edouard 1990(3) SA 581 (A).

Afrika v Metzler ao 1997 (4) SA 531 (NmHC).

Bernstein ao v Bester ao NNO 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC).

Boka Enterprises (Pvt) Ltd v Manatse ao NO 1990 (3) SA 626 (ZH).

Carmichele v Minister of Safety and Security ao (Centre for Applied Legal Studies Intervening) 2001 (4) SA 938 (CC).

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).

Culverwell v Beira 1992 (4) SA 490 (W).

Deutschmann NO ao v Commissioner for the South African Revenue Service; Shelton v Commissioner for the South African Revenue Service 2000 (2) SA 106 (E).

Esterhuizen v Administrator, Transvaal 1957 (3) SA 710 (T).

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).

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

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).

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

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).

Lampert v Hefer NO 1955 (2) SA 507 (A).

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

Lymbery v Jefferies 1925 AD 236.

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

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

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

Mistry v Interim Medical and Dental Council of South Africa 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 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).

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

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

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

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

Pharmaceutical Manufacturers Association of South Africa ao: In re Ex parte President of the Republic of South Africa 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 1999(4) SA 147 (CC).

Prinsloo ao v SA Associated Newspapers Ltd 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).

Stoffberg v Elliot 1923 CPD 148.

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

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.

CANADA

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

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

Companies Act 61 of 1973.

Constitution of the Republic of South Africa, 1996.

Criminal Procedure Act 51 of 1977.

Defence Act 42 of 2002

Electoral Act 73 of 1998

Electronic Communications and Transactions Act 25 of 2002.

Financial Advisory and Intermediary Services Act 37 of 2002.

Interception and Monitoring Prohibition Act 127 of 1992.

Intelligence Services Act 65 of 2002

Intelligence Services Oversight Act 40 of 1994

Local Government Municipal Electoral Act 27 of 2000

Local Government : Municipal Structures Act 117 of 1998.

National Archives of South Africa Act 43 of 1996.

National Credit Bill [B18-2005].

National Strategic Intelligence Act 39 of 1994.

Open Democracy Bill [B67-98]

Promotion of Access to Information Act 2 of 2000.

Protection of Information Act 84 of 1982.

Public Audit Act 25 of 2004.

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

SA Reserve Bank Act 90 of 1989.

Statistics Act 6 of 1999.

AUSTRALIA

Commonwealth of Australia Constitution Act.

Privacy Act, 1988.

Privacy Amendment (Private Sector) Act, 2000.

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.

USA

Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510 et seq (1995).

Fair And Accurate Credit Transactions Act (2003)

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

Family Educational Rights and Privacy Act, 20 U.S.C. 1232g (1974).

Freedom of Information Act, 5 U.S.C. 552 (1966).

Privacy Act 5 U.S.C. 552a (1974).

The Right to Financial Privacy Act, 12 U.S.C. 3401 (1978).

Video Privacy Protection Act 1988, 18 U.S.C. 2710.

UNITED KINGDOM

Consumer Credit Act, 1974.

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

Data Protection Act, 1998.

Freedom of Information Act, 2000.

Human Rights Act, 1998.

NETHERLANDS

Constitution of the Kingdom of the Netherlands, 1989.

Personal Data Protection Act 2000 (Wet Bescherming Persoonsgegevens)

NEW ZEALAND

Privacy Act, 1993.

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

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, 1981,(CoE Convention) available at <http://www.coe.fr/eng/legaltxt/108e.htm>.

Council of Europe Electronic Communications Privacy Directive June 25, 2002.

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 (ISDN Directive).

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.

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).

UN 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 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 2000² (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 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

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.

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

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. The Committee has had four meetings so far.

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.⁵

1.2.2 Data protection is an aspect of safeguarding a person's right to privacy. It provides for the legal protection of a person⁶ (the data subject) in instances where such a person's personal particulars (information) is being processed by another person or institution (the data user). Processing of information generally refers to the collecting, storing, using and communicating of information.

1.2.3 The processing of information by the data user/responsible party threatens the personality in two ways:⁷

- a) First, the compilation and distribution of personal information creates a direct threat

5 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.

6 Although here the primary concern is with data relating to an identified or identifiable living (natural) person, data 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.

7 **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.

- to the individual's privacy;⁸ and
- b) second, the acquisition and disclosure of false or misleading information may lead to an infringement of his identity.⁹

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 primitive, adopts mechanisms and structures that allows individuals to resist encroachment from other individuals or groups.¹⁰

1.2.5 The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights,¹¹ which also protects territorial and communications privacy. The right to privacy is also dealt with in various other international instruments.¹²

1.2.6 In South Africa the right to privacy is protected in terms of both our common law¹³ and in sec 14 of the Constitution.¹⁴ The common law protects rights of personality under the broad umbrella of

8 **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.

9 **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.

10 Westin, A **Privacy and Freedom** New York: Anthem 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** Thesis submitted in accordance with the requirements for the degree of Doctor of Laws at the University of South Africa October 2003 (hereafter referred to as "Roos-thesis") at 1 for examples of information collection through the ages.

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

12 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 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, 1950. The American Convention on Human Rights (Art 11,14) and the American Declaration on Rights and Duties of Mankind (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 "Implementation of Human Rights in South Africa: Constitutional and Pan-African Aspects: A South African and Belgian Perspective" in Vande Lanotte J, Sarkin J Haack 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.

13 In terms of the common law every person has personality rights such as the right to privacy, dignity, good name and bodily integrity (**Stoffberg v Elliot** 1923 CPD 148; **Lymbery v Jefferies** 1925 AD 235; **Lampert v Hefer** 1955 (2) SA 507 (A); **Esterhuizen v Administrator, Transvaal** 1957 (3) SA 710 (T)). See also **Neethling's Law of Personality** at 51.

14 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:

the *actio injuriarum*.¹⁵ In terms of the common law the right to privacy is limited by the rights of others and the public interest.¹⁶

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.¹⁷ 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 application¹⁸ and has to be balanced with other rights entrenched in the Constitution.¹⁹

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, our Constitution recognises every person's right to choose their trade, occupation or profession freely.²⁰ It is clear that in order to exercise this right properly,²¹ an individual may need personal information about others.²²
- 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

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.

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

15 See discussion in Ch 2 below.

16 See discussion in Ch 2 below.

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

18 S 36 of the Constitution.

19 See the discussion of ss 16, 22 and 32 of the Constitution in Ch 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 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.

20 See s 22 of the Constitution. See discussion Ch 2.

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

22 See ss 16 and 32 of the Constitution. See further discussion Ch 2.

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.²³ The most important private data users are credit bureaux, the health and medical profession, banks and financial institutions, the insurance industry and the 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 of information technology.²⁴ The surveillance potential of powerful computer systems prompted demands for specific rules²⁵ governing the collection and handling of personal information.²⁶ The question could no longer be whether the information could be obtained, but rather whether it should be obtained and, where it has been obtained, how it should be used.²⁷ A fundamental assumption underlying the answer to these questions would be 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.²⁸

23 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.

24 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 bazaar of data available to nearly anyone for a price; Neethling *Huldigingsbundel WA Joubert* at 105 et seq.

25 Electronic Privacy Information Center (EPIC) and Privacy International *Privacy and Human Rights Report 2002* An International Survey of Privacy Laws and Developments United State 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.

26 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/>.

27 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.

28 Bennett *Government Foundation Paper* at 6.

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).²⁹ There are now well over thirty countries which have enacted information protection statutes at national or federal level and the number of such countries are steadily growing.³⁰

1.2.12 Early in the debates, it was, however, recognised that information privacy couldn't 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.³¹

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);³² 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.³³

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

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

30 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 5 below.

31 Bennett *Government Foundation Paper* at 6.

32 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>>.

33 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/>.

member nations. As a result, OECD member countries have chosen a range of differing measures to implement the privacy principles.³⁴

1.2.16 In 1995, the European Union enacted the Data Protection Directive³⁵ in order to harmonise member states' laws in providing consistent levels of protection for citizens and ensuring the free flow of personal information within the European Union. The Directive arose from the sense 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 principles).³⁶

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. 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. It provides only a basic framework which will require to be developed in national laws.³⁷

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.³⁸ 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

34 See para 8.2.14 in Ch 8 below for the developments in the APEC countries.

35 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").

36 For further discussion see Chapter 7 below.

37 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. 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.

38 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").

have had much less influence on information regimes than the other instruments.³⁹

1.2.20 The Commonwealth Law Ministers have 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 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 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 without the need to create significant new structures.⁴⁰

1.2.22 The international instruments referred to above will form the basis of discussion throughout this paper. The reasons for this 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.⁴¹

1.2.23 Although the expression of information protection in various declarations 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.

39 Bygrave *Data Protection* at 33.

40 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. They asked the Commonwealth Secretariat to prepare an amended draft which would be considered at the next planning meeting of Secretariat officials.

41 Bygrave *Data Protection* at 30.

These principles are known as the “Principles of Information Protection” and form the basis of both legislative regulation and self-regulating control.⁴²

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. South African commentators⁴³ are unanimous that the creation of such measures through legislation is a matter of great urgency.⁴⁴

1.2.25 It should be noted that the Promotion of Access to Information Act,⁴⁵ inter alia, recognises the information protection principle that personal information should be accessible to the subject. This Act as well as the Electronic Communications and Transactions Act⁴⁶ and the proposed National Credit Bill⁴⁷ have interim provisions dealing, respectively, with the correction of information, the voluntary adherence to information protection principles and, in the case of the credit legislation, a limited regulatory system for credit bureaux.⁴⁸ These sections are regarded as interim measures until specific information privacy legislation has been finalised. The promulgation of information protection legislation in South Africa will necessarily result in amendments to these and other South African legislation.⁴⁹

42 See discussion in Chapter 4 below.

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

44 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.

45 Act 2 of 2002, see s 88.

46 Act 25 of 2002, see ss 51 and 52.

47 B18-2005 as introduced in the National Assembly as a section 76 Bill published in GG 27529 of 26 April 2005.

48 The Department of Trade and Industry (dti) is currently involved in the development of consumer credit legislation in which a number of data protection principles have been embodied, specifically in so far as credit bureaux are concerned. The Bill also makes provision for a public register referred to as a national register of credit agreements. Both public registers and private bureaux will be subject to the data protection legislation.

49 Consequential amendments may 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.

1.2.26 Four models aimed at the protection of personal information can be identified.⁵⁰ 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.⁵¹

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 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 avoided enacting general information protection rules 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) Selfregulation

Information protection can also be achieved - at least in theory - through various forms of

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

51 See, however, the discussion in this regard in Chapter 5 below.

self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. However, in many countries, especially 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. This is currently the policy promoted by the governments of 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 of 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.⁵² They should be aware that 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 and other proposals for discussion and evaluation in the Issue Paper. It is clear that the process of establishing policy goes beyond the level of basic statutory information protection principles to include the ways in which these principles should be enforced, eg, through supervisory authorities. See a discussion of the submissions received in this regard in Chapter 5 below.

1.2.28 Governments may find that proposed measures to protect privacy 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.⁵³ The task of balancing these opposing interests is a delicate one and the main reason why the Commission's thorough consultation process is of such great importance in this investigation.⁵⁴

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

53 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.

54 The Hon Justice Michael Kirby AC CMG in a foreword to Bygrave *Data Protection* states that when a completely new

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 with 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 Moreover, considering the international trend and expectations, information privacy or data legislation⁵⁵ will ensure South Africa's future participation in the information market, if it is regarded as providing "adequate" information protection by international standards.⁵⁶

1.2.31 Marc Rotenberg (director of Computer Professionals for Social Responsibility) commented as follows in an online forum sponsored by the Wall Street Journal:⁵⁷

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."⁵⁸

1.3 Terms of reference

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 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.

55 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.

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

57 Piller *Macworld* at 7.

58 Bennett *Government Foundation Paper* at 28.

1.3.1 The terms of reference for this investigation can be 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 is therefore investigating 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.

1.4 Methodology

1.4.1 In accordance with the Commission's policy to consult as widely as possible, every effort is being 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.

1.4.2 In September 2003 the Commission published a comprehensive Issue Paper for information and comment.⁵⁹ 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.

1.4.3 Written comment was received from 34 persons and institutions.⁶⁰ Numerous follow-up discussions, meetings and presentations furthermore resulted from this publication.⁶¹

1.4.4 The Commission is now publishing a Discussion Paper with draft legislation. In this paper the preliminary proposals of the Commission will be set out and options for reform identified. The views, conclusions and recommendations which follow should, however, not, at this stage, be regarded as the Commission's final views.

1.4.5 The Discussion Paper will later be followed by a report with the Commission's final recommendations and proposed legislative proposals. The Law Reform Commission will also be

59 South African Law Reform Commission *Privacy and Data Protection* Project 124 Issue Paper 24 September 2003 (hereafter referred to as "Issue Paper 24").

60 A list of respondents is enclosed as Annexure A.

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

organising regional workshops in February 2006 at which members of the Project Committee will be present to explain and discuss proposed solutions and to note comments.

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

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 Massachusetts 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. See also reference to Moore B *Privacy: Studies in Social and Cultural History* 1984. 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 (sec 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 Philippines, 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).

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

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 On a 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 Fundamental Freedoms 1950¹¹ states:

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

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.

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.

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 of morals, or for the protection of the rights and freedoms of others.

- b) The American Convention on Human Rights¹² (Art 11,14) and the American Declaration on Rights and Duties of Mankind¹³ (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 Charter on Human and People's Rights¹⁴ 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

2.1.7 In South Africa the right to privacy is protected by both our common law¹⁷ and the Constitution.¹⁸ The Constitutional Court¹⁹ has emphasised the interdependency between the

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.

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

18 See discussion below.

19 **Bernstein ao v Bester NO ao** 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC) at 787 ff.

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 (sec 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(sec 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 (sec 8(1)) but also, if applicable, natural and juristic persons (sec 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 (sec 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 (secs 8(3) and 36(1)).²¹

20 See Neethling J, Potgieter JM & Visser PJ *Law of Delict* Butterworths Durban 2002 (hereafter referred to as "Neethling, Potgieter & Visser *Delict*") at 19-23; *Neethling's Law of Personality* 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).

2.1.10 By the indirect operation of the Bill of Rights is meant 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 (sec 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** case²⁴ 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 Visser²⁵ argue that in so far as the direct application of the

22 Cf **Carmichele v Minister of Safety and Security ao (Centre for Applied Legal Studies Intervening)** 2001 (4) SA 938 (CC) at 950-956. Sec 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 21-22; **Neethling's Law of Personality** at 75-76.

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.

Constitution is concerned, a distinction should, however, be made between a constitutional 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 Burchell²⁸ 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 secs 417 and 418 of the Companies Act³⁰ infringe sec 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 privacy.³³ It is therefore important to evaluate the right to privacy in the light of both the common

-
- 25 Neethling, Potgieter & Visser *Delict* at 22-23.
- 26 McQuoid-Mason DJ "Invasion of Privacy: Common Law v Constitutional Delict - Does it Make a Difference?" *Acta Juridica* 2000 at 227 (hereafter 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)
- 33 Note, however, that the Promotion of Access to Information Act 2 of 2002 (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 Bill 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 Data Protection 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. Sec 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; Sec 10 of the

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, 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 interpreted³⁷ 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

2.1.19 Very important is the fact that the court, in following ***Foulds v Smith***,³⁹ correctly rejected 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 the Issue Paper. 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 chs 3-9.

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) 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 par 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.

view that contumelia in the sense of "insult" is the "essence of an iniuria".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

2.1.21 It has, however, been argued⁴³ 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**

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 chapter 2 on the distinction between identity and privacy).

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).

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** 1993 (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

v Bester NO 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 personality⁴⁷ 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 sec 14, independent of the right to dignity in sec 10,⁵⁰ furthermore confirms the 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

Khumalo ao v Holomisa 2002 (5) SA 401 (CC); 202 (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 verskyningsvorme 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** 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 Sec 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 Sec 10 of the Constitution states:
Everyone has inherent dignity and the right to have their dignity respected and protected.

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.

other rights.⁵³

2.1.24 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.⁵⁴

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.⁵⁵ Definitions of privacy vary widely according to context and environment.⁵⁶ In **Bernstein ao v Bester NO ao**⁵⁷ 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. Gross⁵⁸ 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

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

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

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

56 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)).

57 *Supra* at 787-788.

58 "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.

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 Neethling⁵⁹) in **National Media Ltd ao v Jooste**⁶⁰

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 private⁶¹ (translation from the Afrikaans)

In the same year the Constitutional Court also referred to Neethling's definition in **Bernstein ao v Bester NO ao**.⁶²

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.⁶³ If such a will for privacy is absent, then a person usually has no interest in the legal protection of his privacy.⁶⁴

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;

59 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.

60 Supra at 271.

61 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; cf 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.

62 Supra at 789.

63 *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.

64 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.

- (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.⁶⁵

2.2.7 In *Mistry v Interim Medical and Dental Council of South Africa* ⁶⁶ the court assumed that even though breach of informational privacy was not expressly mentioned in sec 13 of the interim Constitution (the forerunner of sec 14 of the current Constitution), it would be covered by the broad protection of the right to privacy guaranteed by sec 13.

2.2.8 The list mentioned in sec 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)⁶⁷.

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

65 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.

66 1998 (4) SA 1127(CC); 1998 (7) BCLR 880 (CC) at para 14.

67 In *Klein v Attorney-General, Witwatersrand Local Division* 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 sec 13 of the interim Constitution.

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 three⁶⁸ groups:⁶⁹

- (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.

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.⁷⁰ Individuals therefore have control not only over who communicates with them but also who has access to the flow of information about them.⁷¹

68 Cf 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.

69 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).

70 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.

71 McQuoid-Mason **Law of Privacy** at 99. Neethling, Potgieter & Visser **Delict** at 333: "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.

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.⁷²

2.2.15 In terms of sec 39 of the Constitution,⁷³ 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 boni mores or legal convictions of the community in the law of delict.⁷⁴

2.2.16 Of importance is Ackermann J 's dictum in *Bernstein ao v Bester NO ao*⁷⁵ where he stated:

The nature of privacy implicated by the "right to privacy" relates only to the most personal

72 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.

73 Sec 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.

74 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 sec 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.

75 Supra at 789.

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:⁷⁶

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 Neethling⁷⁷ 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.⁷⁸ Thus in principle compiling the data record and obtaining knowledge thereof constitutes an intrusion into the private sphere.⁷⁹

2.2.19 His criticism was validated by Langa DP in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit NO*,⁸⁰ 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.⁸¹

76 At 788-789.

77 See Neethling 1997 *THRHR* at 140.

78 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.

79 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.

80 2001 (1) SA 545 (CC).

81 Para 16 at 557.

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.⁸² As a fundamental right it can be limited in accordance with the limitation clause of the Bill of Rights (sec 36), that is, by a law of general application which includes other fundamental rights.⁸³ 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 sec 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,⁸⁴ their fundamental right to access to information,⁸⁵ their undamental right to freedom of expression,⁸⁶ 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.

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

83 See Neethling, Potgieter and Visser *Delict* at 19.

84 As set out in sec 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.

85 As set out in sec 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.

It should be noted that sec 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 sec 32 in certain cases. See also PAIA.

86 As set out in sec 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.

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 sec 36 of the Constitution inform each other.⁸⁷

2.3.3 Although it is possible that a new constitutional delict may emerge in future,⁸⁸ the courts seem (in accordance with their obligation in terms of sec 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.⁸⁹ The discussion that follows will therefore focus on the common law elements while at the same time trying to accommodate the constitutional principles.

a) Essentials for liability

2.3.4 For a common-law action for invasion of privacy based on the *actio iniuriarum* to succeed, the plaintiff must prove the following essential elements: (i) impairment of the plaintiff's privacy, (ii) wrongfulness and (iii) intention (*animus iniuriandi*).⁹⁰

2.3.5 As shown above, the Constitutional Court has pointed out⁹¹ 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?^{92 93} (b) If so, is such an infringement justifiable in terms of the

87 See discussion above.

88 See discussion above.

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

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

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

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

requirements laid down in the limitation clause (sec 36) of the Constitution?⁹⁴ For this reason the Constitutional Court has cautioned against simply using common law principles to interpret fundamental rights and their limitations.⁹⁵

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 trivial.⁹⁶ They should also be in harmony with the intrinsic values set out in the Constitution.⁹⁷ 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*.⁹⁸

(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.⁹⁹ 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*.¹⁰⁰

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.¹⁰¹

93 Sec 36(2) states that only laws conforming to the test for valid limitations in sec 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.

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

95 McQuoid- Mason **Acta Juridica** 2000 at 246. See however supra fn 28.

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

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

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

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

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

101 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).

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.¹⁰²

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.¹⁰³

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,¹⁰⁴ but also that such violation was contra bonos mores or

102 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 into account the following factors:

- 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.

103 McQuoid-Mason in Chaskalson et al *Constitutional Law of South Africa* at 18---4. Cf also the reference above fn 64 to infringement of autonomy.

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

unreasonable.¹⁰⁵

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 as a criterion for wrongfulness.¹⁰⁶ This view is also apparent in South African case law.¹⁰⁷

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.”¹⁰⁸ Therefore the courts will not protect facts whose disclosure will not “cause mental distress and injury to anyone possessed of ordinary feelings and intelligence”.¹⁰⁹

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.¹¹⁰

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

105 See *Neethling’s Law of Personality* at 221, 273-274.

106 Joubert WA *Grondslae van die Persoonlikheidsreg* Balkema Cape Town 1953 at 136 says: “Daar is min gebiede van die persoonlikheidsreg waar die opvatting 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; cf McQuoid-Mason *Law of Privacy* at 118-122.

107 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 Appellate 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; cf 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.

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

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

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

- will play a major role in determining the “new” boni mores of South African society.¹¹¹ 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 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.¹¹²

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 intrusion¹¹³ 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.¹¹⁴ 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.¹¹⁵

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

112 See the discussion *supra*.

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

114 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.

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

2.3.19 Generally speaking no person has to tolerate information concerning him being collected.¹¹⁶ 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.¹¹⁷

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.¹¹⁸

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.¹¹⁹

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.¹²⁰ 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.¹²¹

116 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).

117 See **Neethling’s Law of Personality** at 274.

118 See **Neethling’s Law of Personality** at 258,275.

119 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.

120 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.

121 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 parties¹²² should also be regarded as unlawful.¹²³

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.¹²⁴ These examples mentioned should, however, not be regarded as a *numerus clausus*.¹²⁵ Whether a specific relationship deserves protection will depend entirely on the surrounding circumstances. Giesker¹²⁶ 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*).¹²⁷ In such instances disclosure of the private facts will, besides breach of contract, also constitute an infringement of the right to privacy.¹²⁸

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

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

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

125 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.

126 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.

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

128 Apart from confidential relationships, a duty not to disclose private facts in the present circumstances – 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.^{129 130}

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.¹³¹

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.¹³² 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.¹³³ 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 lacking¹³⁴ and she should go free.¹³⁵

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

130 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.

131 See *supra* fn 113 as to violation of identity (see also *Neethling's Law of Personality* at 275).

132 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*. Cf *S v A* *ao* *supra* at 297 where it was held that the accused had intention in the form of *dolus eventualis*. Cf 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.

133 Cf *Neethling's Law of Personality* at 57-59, 252-253.

134 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).

135 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

2.3.29 Animus iniuriandi is presumed as soon as wrongful infringement of privacy has been proved.¹³⁶ The defendant may then rebut the presumption.¹³⁷

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 iniuriandi 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 sec 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.¹³⁸ 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.¹³⁹

2.3.32 Neethling¹⁴⁰ 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

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 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.

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

137 As far as liability of the mass media for the infringement of privacy is concerned, cf *Neethling’s Law of Personality* at 166-168; Neethling, Potgieter and Visser *Delict* at 337 fn 104, 348 fn 205 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.

138 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 sec 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 injuriarum (McQuoid-Mason *Acta Juridica* at 261).

139 McQuoid-Mason *Acta Juridica* at 234.

140 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 liability should also be considered.¹⁴¹

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 iniuriarum*.¹⁴² 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 36.¹⁴³

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).¹⁴⁴

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.¹⁴⁵

2.3.36. Sec 36 of the Constitution¹⁴⁶ is a general limitation clause and sets out specific criteria for

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

142 McQuoid-Mason *Acta Juridica* at 233 referring to Burchell *Personality Rights* at 388. At 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.

143 See discussion above.

144 McQuoid-Mason *Acta Juridica* at 254.

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

146 Sec 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

the limitation of the fundamental rights in the Bill of Rights.¹⁴⁷

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.¹⁴⁸

2.3.38 The following five factors are identified in sec 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 sec 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.¹⁴⁹ 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 to a sequential check-list.¹⁵⁰

-
- (e) less restrictive means to achieve the purpose.

- (1) 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.

147 Sec 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.

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

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

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

2.3.40 The High Court has explained that the criteria should be applied as follows:¹⁵¹

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 sec 36(1) (sec 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.¹⁵²

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.¹⁵³

Consent

2.3.44 Consent to infringement of privacy is a unilateral act. Therefore it may be revoked at any time preceding the defendant's injurious conduct.¹⁵⁴ Consent can be given expressly or tacitly.¹⁵⁵

151 **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.

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

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

154 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 toe-stemming herroep word mits dit tydig is. Die teenparty se remedie is om skadevergoeding weens kontrakbreuk te verhaal."

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

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.¹⁵⁶ 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.¹⁵⁷

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.¹⁵⁸ It is a question of fact whether consent was given in a particular instance.¹⁵⁹

*Necessity*¹⁶⁰

2.3.47 Necessity is present when the defendant by vis major is put into such a position that he can 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.¹⁶¹

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.¹⁶² The

156 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.

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

158 See *Neethling 's Law of Personality* at 251; see also supra fn 151.

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

160 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).

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

162 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).

need to process information which infringes the privacy of "innocent" data subjects demonstrates a particular application of necessity¹⁶³ 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.¹⁶⁴

2.3.49 For the processing of information to be deemed lawful under the present circumstances, the following requirements must be satisfied:¹⁶⁵

(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.¹⁶⁶ The same notion also forms the basis of the view¹⁶⁷ 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;¹⁶⁸ 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.

(ii) From the foregoing it follows that the information may be used or communicated only for the protection of the legitimate interest(s) involved,¹⁶⁹ 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.¹⁷⁰

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

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

165 Cf generally Neethling *Privaatheid* at 361-363, *Neethling's Law of Personality* at 275-277; cf 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 (cf Neethling *Huldigingsbundel WA Joubert* at 118-120).

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

167 See the comparative law discussion *infra* (chapter 6) with regard to "purpose specification" as data protection principle.

168 Which includes the public interest: see the discussion *infra*.

169 See the comparative law discussion *infra* (chapter 6) with regard to "limitation" as data protection principle. The ground of justification privileged occasion may also be applicable here (see *Neethling's Law of Personality* at 275 fn 98, 251-2; see also McQuoid-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 (sec 32(1)(b) of the Constitution) should not adversely affect the present principle since access may only be granted to persons for the exercise or protection of a right (see *Neethling's Law of Personality* at 275 fn 98).

170 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

(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.¹⁷¹ 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,¹⁷² 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.¹⁷³ 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.¹⁷⁴ If 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.¹⁷⁵

interest in the data. See Neethling *Huldigingsbundel WA Joubert* at 118 fn 90 91, *Neethling's Law of Personality* at 276 fn 101.

- 171 The unreasonable protection of an interest is in principle unlawful (cf Van Heerden HJO and Neethling J *Unlawful Competition* Butterworths Durban 1995 at 135-137; 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.
- 172 Cf again the discussion of *Gosschalk v Rossouw* supra at 490-492 (see previous fn). The comment there applies mutatis mutandis here.
- 173 See the comparative law discussion infra (chapter 6) with regard to "minimality" as data protection principle.
- 174 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 6) 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).
- 175 See the comparative law discussion infra (chapter 6) 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).

(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.¹⁷⁶ 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.¹⁷⁷

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.¹⁷⁸ Obviously, 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.¹⁷⁹ 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.¹⁸⁰

176 See the comparative law discussion infra (chapter 4) with regard to “fairness and lawfulness” as data protection principle. See also the discussion supra.

177 See *Neethling’s Law of Personality* at 243-4, 277-8.

178 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 sec 27 (articles other than letters may be opened for examination), sec 35 (articles addressed to persons conducting a lottery or sports pool or dealing in indecent or obscene matter may be opened) and especially sec 118 (detention of postal articles and telegrams suspected 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 sec 14 of the Constitution), like the ones mentioned above, will have to meet the requirements of s 36 (the limitation clause) of the Constitution.

179 Cf *Neethling’s Law of Personality* at 243-4.

180 A important case in this regard is *Gosschalk v Rossouw* supra. There the court recognised that police questioning may

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.¹⁸¹

(i) First, the state must be expressly authorised by a valid statutory provision to process information.¹⁸² As said, in view of the constitutional protection afforded the right to privacy,¹⁸³ any such legislation must be reasonable and justifiable in an open and democratic society based on freedom, human dignity and equality.¹⁸⁴

(ii) Second, the information may be used or communicated only for the purposes recognised by the statutory authorisation.

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 immunities *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 ch 2, and sec 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 (s 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.

181 See generally Neethling *Privaatheid* at 362-363, *Huldigingsbundel WA Joubert* at 120-121; Neethling's *Law of Personality* at 277-8.

182 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 (sec 36).

183 See the previous fn.

184 See sec 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).

(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.¹⁸⁵

(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 controller¹⁸⁶ acts wrongfully in terms of the abovementioned information protection principles, the ordinary delictual remedies,¹⁸⁷ 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.¹⁸⁸ 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 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 personality¹⁸⁹ that it is probably fair and justifiable to hold a information institution liable even where intention or negligence is not present.¹⁹⁰

Private defence

2.3.55 Private defence is present when the defendant defends himself against another's actual or

185 Cf the application of the criterion of reasonableness in **Gosschalk v Rossouw** supra at 490-492 (see on this supra fn 175).

186 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).

187 See **Neethling's Law of Personality** at 278; also Faul W **Grondslae van die Beskerming van die Bankgeheim** LLD thesis RAU Johannesburg 1991 at 536-537.

188 See McQuoid-Mason **Law of Privacy** at 198-199.

189 See also Neethling 2002 **THRHR** at 584. See generally on strict liability Neethling, Potgieter and Visser **Delict** at 363 ff.

190 See Neethling **Privaatheid** at 363, **Neethling's Law of Personality** at 278.

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.¹⁹¹ 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.¹⁹² 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.¹⁹³

(ii) Defences excluding intention

2.3.57 In the common law the general principles of the *actio injuriarum* 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.¹⁹⁴

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*.¹⁹⁵

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.¹⁹⁶

191 See *Neethling's Law of Personality* at 242-3.

192 See Neethling, Potgieter and Visser *Delict* at 92.

193 See *Neethling's Law of Personality* at 280 fn 136.

194 McQuoid-Mason *Law of Privacy* at 237 and references to courts cases therein.

195 McQuoid-Mason in Chaskalson et al *Constitutional Law of South Africa* at 18---8.

196 Cf McQuoid-Mason *Law of Privacy* at 237.

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.¹⁹⁷ It has also been decided that the disused common law remedy of a right to retraction and apology should be revived.¹⁹⁸

2.3.62 In the case of an infringement of or threat to the right to privacy as a fundamental right, in terms of sec 38 of the Constitution the prejudiced or threatened person is entitled to approach a competent court for appropriate relief, including a declaration of rights.¹⁹⁹ 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.²⁰⁰

iii) Actio iniuriarum

2.3.63 If a person's privacy is wrongfully and intentionally infringed, he may recover sentimental damages or satisfaction (solatium) for injured feelings.²⁰¹ In privacy cases the plaintiff is being compensated for the emotional suffering as a result of having his or her private life infringed.²⁰²

2.3.64 The amount of compensation is in the discretion of the court and is assessed on what is fair and reasonable.²⁰³ Factors which may play a role in the assessment of the amount of the satisfaction are still largely absent from case law.²⁰⁴ Also note that the Constitutional Court has held that additional constitutional punitive damages should not be awarded in terms of the Constitution for

197 See *Neethling's Law of Personality* at 250-254.

198 See *Mineworkers Investment Co (Pty) Ltd v Modibane* 2002 (6) SA 512 (W); see also Neethling J and Potgieter JM "Herlewing van die Amende Honorale as Remedy 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.

199 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).

200 See *Fose v Minister of Safety and Security* 1997 (3) SA 786 (CC) at 836-837; Neethling, Potgieter and Visser *Delict* at 23.

201 *Jansen van Vuuren ao NNO v Kruger* supra at 857-858.

202 McQuoid-Mason *Law of Privacy* at 170.

203 See *Neethling's Law of Personality* at 253; *Jansen van Vuuren ao NNO v Kruger* supra at 857-858.

204 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.

infringements of fundamental rights and freedoms.²⁰⁵ But because of the constitutional entrenchment, the amount of satisfaction may nevertheless be increased.²⁰⁶

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.²⁰⁷

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.²⁰⁸ Fault on the part of the perpetrator is not a requirement.²⁰⁹

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.²¹⁰ Otherwise they do not require a different approach from the previous common law position.²¹¹

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.²¹² This revival can be supported for various reasons, inter

205 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.

206 Cf *Africa v Metzler* 1997 (4) SA 531 (NmHC) at 539; see also Neethling, Potgieter and Visser *Delict* at 21.

207 See *Neethling's Law of Personality* at 254.

208 See *Rhodesian Printing and Publishing Co Ltd v Duggan* ao supra.

209 See in general Neethling, Potgieter and Visser *Delict* at 260-261.

210 *Mandela v Falati* 1995 (1) SA 251 (W) at 259-60.

211 McQuoid-Mason *Acta Juridica* at 236.

212 See *Mineworkers Investment Co (Pty) Ltd v Modibane* supra.

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.²¹³ 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,²¹⁴ as well as a factor in the assessment of the amount of satisfaction.²¹⁵

2.4 Conclusion

2.4.1 As stated in Chapter 1 above,²¹⁶ information protection is an aspect of safeguarding a person’s right to privacy. The so-called traditional principles examined in this Chapter should, therefore, be fully utilised. These principles are based on the ordinary delictual principles as influenced by the Constitution which regulate the area of privacy protection in South African law (the principles regarding the *actio iniuriarum*). Information protection should be seen merely as a particular application of those principles.

2.4.2 The Commission submits that effective information protection will, however, only be achieved through regulation by legislation.²¹⁷

2.4.3 Firstly, 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 is improbable that the application of the information principles by the courts will occur often or extensively enough in the near future to ensure the protection of personal information.²¹⁸ Moreover, since the major engine for law reform should be the legislature and not the judiciary, and, as will be seen, the introduction of a information protection regime will not merely involve incremental changes of the common law but radical law reform, it is a task for the legislature.

2.4.4 Secondly, the individual should also be able to exercise a measure of active control over his personal information.²¹⁹ In fact, the traditional protective measures have little value if

213 See Neethling & Potgieter 2003 *THRHR* at 333.

214 McQuoid-Mason *Acta Juridica* at 236 referring to Burchell *Personality Rights* at 496.

215 See Neethling and Potgieter 2003 *THRHR* at 333.

216 Para 1.2.2 and further.

217 See *Neethling’s Law of Personality* at 272-3 where these arguments are set out.

218 See also Neethling 2002 *THRHR* at 589.

219 This encompasses the following: 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

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.²²⁰ Consequently such measures can be created by legislation only.

2.4.5 The Commission therefore recommends that formal legislation on the protection of personal information be enacted and that the objects of the Act be set out as follows:

CHAPTER 1

General Provisions

Objects of the 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 which will be in harmony with international prescripts and which will, while upholding the right to privacy, at the same time

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 (see *Neethling's Law of Personality* at 278-9).

220 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).

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 **a** 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.

Comment is invited.

CHAPTER 3: SUBSTANTIVE SCOPE OF THE PROPOSED LEGISLATION

3.1 General

3.1.1 In the Issue Paper¹ the Commission's preliminary proposal was that the investigation into the protection of personal information should, as a starting point, include:

- 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; and
- d) sound and image information.

3.1.2 Personal information kept in the course of a purely personal or household activity was excluded. Critical information was included at that stage pending consultation in this regard. Comment was invited in all instances.

3.1.3 Some respondents² indicated that the scope of the inquiry and the legislative efforts to follow should pertain to all the areas listed.³ Others felt that only information kept in the course of personal or household activity should be excluded.⁴ A third group was of the opinion that information on household activity and critical information should be excluded.⁵ A proposal was also put forward by a health organization⁶ to the effect that a distinction should be drawn between personal information and professional information (which would also include provider

1 Issue Paper 24.

2 Strata; Financial Services Board.

3 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.

4 The Internet Service Providers' Association; Gerhard Loedolff, Corporate Consultant (Business Assessment) Eskom; SAHA; Vodacom; The Banking Council; Medical Research Council and Private Health Information Standards Committee. Gave example of x-rays as image data.

5 Liberty; Society of Advocates of Natal; SAFPS; SAPS.

6 IMS Health.

information) and that anonymising or de-identified information should be excluded from the scope of the legislation.

3.1.4 Specific arguments were raised in each case and will be discussed under the following headings:

- * automatic and manual files (para 3.2)
- * sound/image information (para 3.3)
- * natural v juristic persons (para 3.4)
- * public v private sector information (para 3.5)
- * critical information (para 3.6)
- * sensitive information (para 3.7)
- * household activity (para 3.8)
- * anonymised/ de-identified information (para 3.9)
- * professional information (including provider information) (para 3.10)

3.2 Automatic and manual files

3.2.1 Respondents⁷ unanimously supported the view of the Commission that information protection legislation should incorporate both manual and electronic files,⁸ in accordance with the EU Directive.^{9 10}

3.2.2 It was stated that all records should be incorporated regardless of the medium or form which they take,¹¹ especially since offline paper-based databases are as important as electronic

7 The Internet Service Providers' Association; Financial Services Board; Neo Tsholanku, Eskom Legal Department; SABC; LOA; ENF for Nedbank; Vodacom; Nedbank; The Banking Council.

8 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 this Bill.

9 Article 3 of the EU Directive furthermore 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.

10 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.

11 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.

3.2.3 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.¹² 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.¹³

3.2.4 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.

3.2.5 Finally, it was argued that the proposed Privacy Act should only apply from the date of promulgation. The SABC, for instance, has a database of broadcasting material that stretches back to the first decade of the previous century and it would be prohibitively costly and expensive for the SABC to have to categorise and audit the material that it has in its archives.¹⁴

3.2.6 The Commission confirms its proposal as set out in the Issue Paper and submits that both manual and automatic files should be dealt with in the legislation. See sec 3 set out at 94 below.

3.3 Sound/image information

12 LOA.

13 Liberty.

14 **Comment is requested on this aspect.** See definition of “record” which stipulates that the Act applies to a record regardless of when the record came into existence.

3.3.1 There appears to be consensus amongst respondents that the investigation should cover both sound and image information,¹⁵ 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.¹⁶ There is clearly a lacuna in the existing guidelines and legislation in South Africa with regard to this type of information.¹⁷

3.3.2 Sound and image information should include paper data, sound, video, but also other forms of electronic information such as ECGs, EEGs, CAT-scans, etc.¹⁸

3.3.3 The Commission therefore proposes to include sound/image information in the scope of the legislation. See sec 3 set out below at 94 as well as the definition of “record in sec 2 of the Bill.

3.4 Natural v juristic persons

3.4.1 In the Issue Paper the following points were made:

a) Firstly, that the South African courts apply the common law principles developed for the protection of the privacy of natural persons also to juristic persons:¹⁹

* In **Financial Mail (Pt) Ltd v Sage Holdings Ltd**²⁰ the court expressed the view that the *actio iniuriarum* 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 outraged or offended. The basis for this protection is that privacy, like reputation

15 The Internet Service Providers' Association; Financial Services Board; Neo Tsholanku, Eskom Legal Department; ENF for Nedbank; LOA; The Banking Council.

16 ENF for Nedbank.

17 The Banking Council.

18 LOA.

19 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.

20 Supra.

(*fama*), can be infringed without injured feelings.²¹

* The court in **Janit v Motor Industry Fund Administrators (Pty) Ltd**²² 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.²³

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.²⁴

b) In the second place 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.

c) Thirdly, 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**²⁵ it was 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. 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.

21 At 462; *Neethling's Law of Personality* at 71.

22 1995 (4) SA 293 AD.

23 At 303.

24 At 305 B-D.

25 *Supra*.

d) Finally, it was noted that it would appear that only natural persons (ie not juristic persons) are protected by the provisions of the **Promotion of Access to Information Act**, since “personal information” is defined as information about an identifiable individual.^{26 27 28}

3.4.2 Most respondents to the Issue Paper 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.²⁹ In one submission³⁰ it was, however, held that the inclusion of juristic persons in this way may be unconstitutional.

3.4.3 The Commission was furthermore (in more than one submission) referred to two studies in this regard. 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 persons³¹ and the second an article written by S Nadasen entitled “Data Protection for

- 26 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.
- 27 Roos at 499.
- 28 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 the Promotion of Access to Information Act 2 of 2000 (PAIA) lists amongst the grounds on which the refusal to grant access to the records of private persons is 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.
- 29 Internet Service Providers’ Association; Liberty; Sagie Nadasan; Sanlam Life: Legal service; Financial Services Board; Neo Tsholanku, Eskom Legal department; ENF for Nedbank; SABC; LOA; The Banking Council.
- 30 IMS.
- 31 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 5/4/2004at
http://europa.eu.int/comm/internal_market/privacy/docs/studies/legal_en.pdf.

Companies: Natural v Juristic Persons: Privacy and More".³² Both will be discussed in some detail below.

3.4.4 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.

3.4.5 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.³³

3.4.6 The international information protection instruments remain somewhat ambiguous about

32 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.

33 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.³⁴ 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.³⁵ The ISDN Directive³⁶ gives formal expression to this increasingly explicitly recognised fact, and also confirms that, in certain contexts, a distinction between natural and juristic persons is difficult to make or justify in practice.³⁷

3.4.7 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

34 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)).

35 Whatever the limitations on the right to “private life” (further discussed below, at 2.3), 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.

36 Directive 97/66/EC of the European Parliament and of the Council dated 15/12/97 concerning the 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)). protection of personal data and the protection of privacy in the telecommunications sector.”

37 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)).

individuals, such as partnerships in England, lack independent juristic status but may 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.

3.4.8 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' (e.g. one-person businesses), in some respects, require less protection than other 'natural persons' (e.g. consumers), and some 'juristic persons' (e.g. religious, political, or trade union associations) require more protection than other 'juristic persons' (e.g. 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.

3.4.9 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.

3.4.10 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.

3.4.11 The main consideration appears to be that juristic entities as well as natural persons are affected by the increased processing of information on them, and that it is 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.

3.4.12 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 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;³⁸
- 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;³⁹
- 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.⁴⁰

3.4.13 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 DPD 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.

3.4.14 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

38 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 (e.g.) 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.

39 The LOA argued that if financial information regarding natural persons is protected, then the financial information of juristic persons should also be protected.

40 LOA.

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,⁴¹ but that the extent of the protection has to be judged in each case⁴² and acknowledges the fact that a company's right to privacy may be limited for several reasons.⁴³

41 **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.

42 **Investigating Directorate: serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit NO** supra.

43 In **Bernstein v Bester and Others NNO** supra 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 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 v Walters ao NNO** 2002 (5) SA 796 (CC) 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.

3.4.15 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 application, *in concreto*, of section 8 (4) of the Constitution.⁴⁴

3.4.16 He refers to the Korf analysis⁴⁵ 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.

3.4.17 One dissenting submission was received⁴⁶ in which the argument was posed that the statutory privacy protections do not usually apply to corporations and businesses.⁴⁷

3.4.18 It was argued that the incorporation of juristic bodies in privacy legislation would not conform to the Constitution, and is not in sync with the other legislation as it could not be reasonable and justifiable in an open and democratic society because of the effects such legislation would have.⁴⁸

3.4.19 The fact was reiterated that, rather than an attempt to protect a human right, these statutes represent a response to a perceived threat caused by increasing computerisation and the ability to process and aggregate information. Rather than a desire to protect the purported "privacy rights" of companies, the concern is to limit the uncontrolled uses of information technology.

44 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.

45 Douwe Korf *EC Study*.

46 Michalsons for IMS Health.

47 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."

48 Michalsons for IMS Health.

3.4.20 The position in the USA and Europe were furthermore discussed with reference to the European Commission's Data Protection Directive⁴⁹ (the "Directive") as well as to the position as set out by Korff referred to above regarding the different countries in Europe.

3.4.21 The Commission was referred to the position in the United States, where 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.⁵⁰

3.4.22 A distinction between juristic and natural persons is furthermore found in the Privacy Act of 1974⁵¹ which only protects natural persons.⁵² Similarly, the Fair Credit Reporting Act (the "FCRA") only protects consumer credit reports⁵³ of "individuals"— it specifically excludes so called commercial credit reports⁵⁴ and by definition any entity other than an "individual".⁵⁵ 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.

3.4.23 After evaluating the above arguments one could therefore in conclusion state that:

- a) The submissions received were mostly in favour of including juristic persons in the protection of information privacy legislation.⁵⁶

49 EU Directive.

50 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 has 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 prefatory 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 [hereinafter "HIPAA Final Rule"].

51 5 U.S.C. § 552a.

52 Supra at (a)(2).

53 "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). *Wrigley v. Dun & Bradstreet, Inc.*, 375 F. Supp. 969 (N.D. Ga. 1974); *Boothe*, 523 F. Supp. at 633." See Federal Trade Commission. FTC Staff Opinion – Medine-Tatelbaum. (26 July 2000), online: <http://www.ftc.gov/os/statutes/fcra/tatelbaum.htm>

54 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).

55 Ibid., 15 U.S.C. § 1681a ©.

56 See also the discussion in subpara (h) below regarding professional information.

- b) Internationally few countries provide privacy protection for juristic persons. However, there seems to be a movement towards broader protection.
- c) In terms of sec 8(4) of the Constitution a juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the right and the nature of the juristic person.
- d) In each case one would have to ascertain whether appropriate circumstances exist for companies to rely on to protect their privacy interests.

3.4.24 The Commission's preliminary proposal is, therefore, to include information pertaining to both natural and juristic persons in the ambit of the Act. See sec 3 at 94 below and the definition of "personal information" in sec 2 of the Bill. Since this is, however, a controversial issue, which has also not been conclusively determined in the international sphere, comment will be welcomed. This question will also be discussed at the forthcoming workshops.

3.5 Public v private sector

3.5.1 Most of the respondents agreed with the position as set out in the Issue Paper that the investigation should cover both the private and the public sector.⁵⁷

3.5.2 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.⁵⁸ Consumers would be adversely affected if governmental agencies were not subject to security protection.⁵⁹⁶⁰

57 The Internet Service Providers' Association; Sanlam Life: Legal Services; Neo Tsholanku, Eskom Legal Department; SABC; LOA; The Banking Council.

58 SABC.

59 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.

3.5.3 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.⁶¹

3.5.4 Taking into consideration the points made, it was, however, decided that the proposed Act will deal with both public and private sectors.

3.5.5 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 should these differences should be? ⁶²

3.5.6 Some commentators were of the view that no distinction should be drawn between the two entities.⁶³ They argued as follows:

- * Information privacy legislation needs to cater for everyone that collects information.⁶⁴
- * Unless the same principles apply in both the public and the private sector, there would be no consistency in the law.⁶⁵ Different rules will leave room for game playing and waste of public funds just to keep outside the reach of the law.⁶⁶
- * Both the public and the private sectors have in their possession innumerable personal records and both have responsibilities towards their data subjects.

60 LOA.

61 SAPS; See discussion on critical information below.

62 Question 4, Issue Paper 24.

63 See eg. Medical Research Council; Private health Information Standards Committee; LOA; Gerhtrud Loedolff, Eskom; Eskom Legal Department; SAFPS; Strata; Liberty; Society of Advocates of Kwa-Zulu Natal.

64 LOA.

65 LOA.

66 Gerhard Loedolff, Eskom.

- * 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.^{67 68}
- * 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.⁶⁹

3.5.7 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:⁷⁰⁷¹

- * 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 very little, 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.⁷²
- * One should recognise 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.⁷³
- * The private sector, on the other hand, should be allowed flexibility through the development and application of self-regulatory measures such as codes of

67 Liberty.

68 LOA.

69 Society of Advocates of Kwazulu Natal (JC King); SAFPS.

70 Sanlam Life: Legal Services.

71 Vodacom; The Banking Council; SAHA; Internet Service Provider's Association.

72 SAPS; Financial Services Board.

73 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.

conduct.⁷⁴ 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.⁷⁵

3.5.8 There were also commentators who drew the attention of the Commission to the fact that the distinction between public and private bodies is not always very clear:⁷⁶

- * 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.⁷⁷
- * In many instances the SABC, for instance, is faced with an overlap regarding 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.⁷⁸
- * 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.⁷⁹

3.5.9 The preliminary conclusion of the Commission is, therefore, that no distinction should be drawn between information processed by public and private bodies. The proposed Bill will therefore deal with both sectors. See definition of “record” in sec 2 of the Bill as well as sec 3 at 94 below. Comment is invited in this regard.

74 The Banking Council.

75 SABC.

76 SABC; ISPA.

77 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.

78 SABC.

79 SABC.

3.6 Critical information

3.6.1 Most information protection laws 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.

3.6.2 This position is in accordance with the EU Directive⁸⁰ which 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 Community law, such as those provided for by Titles V and VI 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 security matters) and the activities of the State in areas of criminal law.

3.6.3 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.⁸¹

3.6.4 Two points are of importance here. First of all, one should determine what the definition of critical information is.⁸² Secondly, one would have to decide whether critical information should be excluded from all the information protection principles, only some of them, or whether the scope of the obligations and rights provided for in the principles should be restricted in specific circumstances.

Definition of critical information

80 Article 3 (2).

81 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.

82 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.

3.6.5 What is important to note is that “critical information” and “sensitive information” should be distinguished in terms of our discussion. Whereas critical information deals with state security and crime, sensitive information is concerned with confidential aspects of information of a personal kind such as race, ethnicity, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of information concerning health or sex life or criminal record. Sensitive 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 para 3.7.

3.6.6 The so-called “critical information” or “security information” should furthermore not be equated with information that is kept secure in terms of the security principle. All 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.⁸³ All personal information is subject to the privacy principles.⁸⁴

3.6.7 In this section we are specifically dealing with critical information. In our research it was immediately clear that there is currently confusion regarding the definition of critical information as well as with the protection of critical information. This is mainly as a result of the numerous Acts dealing with these issues.

3.6.8 Terms used in other legislation 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”⁸⁵ or “information kept, used, made, obtained or related to a prohibited place”,⁸⁶ as well as “intelligence/security information”.⁸⁷

83 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 2004/11/12.

84 See discussion in Chapter 4: Principle 6: security safeguards.

85 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.; See also the new Draft National Information Security Regulations compiled by the National Intelligence Agency.

86 Protection of Information Act, Act 84 of 1982.

87 Intelligence Services Oversight Act 40 of 1994 and National Strategic Intelligence Act 39 of 1994.

3.6.9 The Protection of Information Act 84 of 1982 is currently the principal Act concerned with the restriction of the disclosure of information.⁸⁸ 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).⁸⁹ The MISS is to be implemented by each public institution as well as some private institutions working with public ones. According to its preface the MISS “must be maintained by all institutions who handle sensitive/classified material of the Republic”.

3.6.10 Classified information is defined to be :

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.

3.6.11 It seems that no reference has been made in this definition to “national security”, in stead the term “sensitive nature ” seems to have replaced it.

3.6.12 This definition differs from that in a separate specific policy which governs information security within the South African Defence Force.⁹⁰ 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.

3.6.13 The Intelligence Services Oversight Act 40 of 1994 defines “intelligence” in sec 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;⁹¹

88 See a full discussion by 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.

89 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 are, however, being drafted by the National Intelligence Agency. Klaaren at 196.

91 Services’ means the Agency, the South African Secret Service, the Intelligence Division of the National Defence Force

Security information is not defined.

3.6.14 Various initiatives regarding the protection of critical information have been noted. The Electronic Communications and Transactions Act (the ECT Act)⁹² 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".⁹³ The Act then sets out the special treatment that these databases will enjoy.⁹⁴

3.6.15 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.⁹⁵ The purpose of this is 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.⁹⁶

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.

92 Sec 53 of Act 25 of 2002.

93 **Identification of critical data and critical databases**

53. The Minister may by notice in the Gazette -

- a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data for the purposes of this Chapter; and
- b) establish procedures to be followed in the identification of critical databases for the purposes of this Chapter.

94 Chapter IX of the Act deals with the registration of critical databases (sec 54), the management of critical databases (sec 55), restrictions on disclosure of information (sec 56), the right of inspection (sec 57) and non-compliance with the chapter (sec 58).

95 LOA; The Department of Communications has awarded a tender to consultants KPMG, Gobodo, ICT Works and Sizwe Ntsaluba VSP to compile an inventory of all major databases in the country, including those operated by banks, medical companies and other private firms to assess whether information they hold is relevant to national security (Lesley Stones, Information Technology Editor Business Day November 18, 2003, accessed at <http://allafrica.com/stories/200311180262.html> on 2003/11/27.

96 Department of Communications Deloitte & Touche and Michalsons "Guide to the Electronic Communications and Transactions Act, 2002" 2002-2003 accessed from www.michalson.com at 3.

3.6.16 Following an inquiry in this regard, the Department of Communications indicated that this issue is still under consideration and that a report on the implementation of Chapter IX will be published later in 2005.⁹⁷

3.6.17 It is therefore unsure what the effect of the ECT Act will be,⁹⁸ especially since sec 55 dealing with the management of critical databases also provides as follows in sec 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.

3.6.18 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.

3.6.19 Existing legislation will 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.

97 Discussion with Palesa Banda, Department of Communications on 8 November 2004.

98 This Act only applicable to electronic documents; In his submission to the Commission Mr Mark Heyink furthermore noted that the Minister only has the power to deal with information and identify critical databases. Thus, on the wording of the Act, the Minister has no jurisdiction over networks, often the most vulnerable component of an information system. Internationally the approach has been different in that comparable legislation has focused on "critical infrastructure" as opposed to "databases". This would include networks. Further, critical data may be stored in various databases and it is the sensitivity or criticality of the information as opposed to the repository which should determine the information security requirements applicable to the repository. In the circumstances the Act should therefore not affect the manner in which criticality of information is viewed in other legislative instruments.

3.6.20 The South African Law Reform Commission has, furthermore, been requested to include a review of the Protection of Information Act in its programme.⁹⁹

3.6.21 The National Strategic Intelligence Act 39 of 1994 provides in sec 6 that the Minister (member of cabinet designated by the President to assume the responsibility for intelligence services as contemplated in sec 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, are being discussed at present.

3.6.22 It seems imperative that critical information should be defined properly.¹⁰⁰ It is furthermore important that any legislation regarding privacy and information protection should complement each other.¹⁰¹ The Commission would appreciate inputs regarding the definition of critical information as well as the harmonisation and co-ordination between the different pieces of legislation dealing with information regarding state security and criminal law issues.

Full exclusion of critical information from privacy legislation

3.6.23 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

99 Request in this regard from the Minister for Safety and Security as part of the review and rationalisation of South Africa's security legislation.

100 A similar argument was posed by Liberty.

101 See also ENF for Nedbank.

laws.¹⁰² Denmark, Ireland, the UK (for national security)¹⁰³ 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 enforcement.

Separate laws excluded

3.6.24 Some countries subject some or most processing in the areas listed to separate laws.¹⁰⁴ 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 basis principles in the information protection law. See for instance the Netherlands, Italy, Luxembourg, Germany, Portugal, Sweden.

3.6.25 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.¹⁰⁵

3.6.26 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 safeguard the public interest in question. In terms of the Directive, compliance with these

102 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.

103 Sec 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).....

104 See Art 2 of the Personal Data Protection Act 2000 of the Netherlands.

105 Korff **Comparative Study** at 142.

requirements should furthermore be subject to monitoring by a “supervisory authority” fulfilling the requirements of Art 28 of the Directive.

Limited exclusion (often in addition to full exclusion/separate laws)

3.6.27 Apart from the very wide exemption with regard to processing for the purpose of safeguarding national security,¹⁰⁶ 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” ie informing-requirements and the data subject access requirements, but the crime and taxation exception extends to the “fair processing” principle.¹⁰⁷

3.6.28 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.¹⁰⁸ This means that the courts and the information

106 See footnote 102 above.

107 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.’

108 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.¹⁰⁹

3.6.29 This was confirmed by the UK Information Commissioner, who stressed that these exceptions are restrictively applied:¹¹⁰

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”.

3.6.30 In New Zealand sec 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.

3.6.31 In the USA law enforcement agencies have immunity from almost every significant restriction in the Privacy Act.¹¹¹ 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.

South Africa

3.6.32 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.¹¹²

3.6.33 Respondents 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

109 Korff *Comparative study* at 144.

110 Korff *Comparative study* at 145.

111 Roos 1998 *THRHR* at 525.

112 The Internet Service Providers’ Association; Liberty; Neo Tsholanku, Eskom Legal Department; ENF for Nedbank; SABC; LOA; The Banking Council.

correct and even more stringently protected and that it will need to be incorporated in the legislation.¹¹³¹¹⁴

3.6.34 It was proposed that the application of such principles should apply at least until the relevant regulations are developed giving sufficient protection to information that may be contained in such data bases and it may be worth preserving their application even after such regulations have been gazetted.¹¹⁵

3.6.35 A few respondents, however, felt that critical information should be excluded.¹¹⁶ 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.¹¹⁷

3.6.36 This idea was further elaborated on by the SAFPS who wants to be excluded from the Act.¹¹⁸ 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.

113 Vodacom; SABC; ENF for Nedbank.

114 ISPA.stated that in light of sec 54 of the ECT authorising the Minister to declare a database as a critical database, the data protection principles should apply.

115 The Internet Service Providers' Association.

116 Soc of Adv Natal; SAFPS; SAPS.

117 Soc of Adv 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.

118 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.

3.6.37 After duly considering the abovementioned arguments, the Commission's preliminary view is that the specific laws dealing with national security, defence and police work should be excluded from the privacy legislation. Additional provision should furthermore be made for exemptions to be granted to responsible parties in specific circumstances.¹¹⁹ This seems to be what the majority of commentators have suggested and is also in accordance with international practice.

3.6.38 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:¹²⁰

- * Section 104 of the *Defence Act* 42 of 2002 deals with the improper disclosure of information;
- * Sec 11A of the *Armaments Development and Production Act* 57 of 1968 deals with the prohibition of disclosure of certain information;
- * Sec 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 2000¹²¹ deals with the national security ground of refusal to access to information.¹²²
- * Sec 56 of the *ECT Act* 2002 deals with the restrictions on the disclosure of information.
- * Sec 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.

119 See para 4.4 in Chapter 4 dealing with exemptions from privacy principles.

120 Other Acts that need to be considered are: Nuclear Energy Act 1982; National Supplies Procurement Act 1970; Petroleum Products Act 1977; South African Police Services Act 1995; State of Emergency Act 1997; National Archives Act 43 of 1996; Electronic Communications Security Pty (COMSEC) Act 68 of 2002.

121 See also discussion below.

122 Important to note that PAIA does not repeal pre-existing government secrecy and confidentiality laws.

- 3.6.39 The Commission therefore proposes that -**
- a) a definition of “critical information”¹²³ be developed to be used consistently in all the legislation dealing with this issue;**
 - b) various Acts dealing with the protection of critical information be consolidated or harmonised in accordance with the accepted privacy principles.**

Once this has been accomplished it will then be possible to provide specific exemptions in the privacy legislation of the information dealt with in these Acts. See sec 4 of the proposed Act at 96 below.

3.7 Sensitive information (special personal information)

3.7.1 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).¹²⁴

3.7.2 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).

3.7.3 In the document ‘Privacy Online: A Report to Congress (June 1998)’, the U.S. Federal Trade Commission 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 sensitive information. In principle, such information should not be

123 Or whatever term is decided on to be used in all the relevant legislation.

124 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.

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 sensitive information but then only in respect of the purpose for which consent has been given; and
- *the processing of sensitive 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.

3.7.4 It was further stated that where it is impossible for the data subject to consent (e.g. blood test of an unconscious victim of a road accident), processing of such sensitive information must be carried out reasonably and in the data subject's best interests and only to the extent necessary.

3.7.5 In principle the processing of sensitive 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.¹²⁵

125 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 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

3.7.6 The Commission therefore proposes that special provision be made for the protection of sensitive information. See the discussion in Chapter 4 below (Principles) and the proposed Bill sec 24 and further.

3.8 Household activity

3.8.1 In the Issue Paper 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.

3.8.2 Mixed reaction was received on this question. Some respondents agreed with the Commission's preliminary view.¹²⁶ 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.¹²⁷

3.8.3 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 society, even the number of socks a person has, their colours, sizes, and so on, also is potentially of enormous economic value.¹²⁸

3.8.4 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.¹²⁹

general application may be processed.

126 LOA.

127 Financial Services Board.

128 LOA.

129 Roos 1998 *THTHR* at 523.

3.8.5 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,¹³⁰ but that will be a factual question.

3.8.6 In principle it is therefore the Commission's view that the Act should not cover personal information kept and used by a person in the course of a purely personal or household activity. See sec 4 at 96 below.

3.9 Anonymised/de-identified information

3.9.1 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 are kept to a minimum by business.¹³¹

3.9.2 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.

3.9.3 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:

- * The National Health Bill (latest available version, published November 2003, section 16) which makes very limited reference to circumstances under which 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
- * the definition of 'personal health information' in a recent report by the Council for Medical Schemes are so wide that it could be very difficult to de-identify information.¹³²

130 LOA.

131 IMS.

132 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

3.9.4 It was pointed out ¹³³that the proposed legislation could 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.

3.9.5 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.

3.9.6 However, the Commission was referred¹³⁴ to the work done by Sweeney and Samarati that show 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?

3.9.7 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-identifying information.¹³⁵ It was argued¹³⁶ that since “removal” may be interpreted as being interchangeable with “deletion”, a very strong case on the surface exists for the action of “de-identification” to be captured by the definition of “data processing”. This is obviously "at odds" with 'protecting'

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.

133 Medical Research Council.

134 Prof Martin Olivier.

135 Borking Consultancy, speaking at the Data Protection and Privacy Commissioners Conference in Sydney, September 2003.

136 IMS.

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 it should be able to be actively pursued by organisations that may collect personal information.

3.9.8 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). **Comment is invited on this issue.**

3.9.9 In the USA the rules made under the Health Insurance Portability and Accountability Act of 1996 (the "HIPAA") have been brought into force¹³⁷. 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.

3.9.10 The Commission recommends that anonymised/de-identified information be excluded from the proposed legislation on condition that it cannot be re-identified. See sec 4 at 96 below.

3.10 Professional information (including provider information)¹³⁸

3.10.1 A submission was received on Issue Paper 24¹³⁹ 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.

137 Notwithstanding industry opposition, the rules came into effect on April 14, 2001, although most entities have 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.

138 See also the discussion on natural v juristic persons in para 3.4 above.

139 IMS.

3.10.2 “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".

3.10.3 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.

3.10.4 The definition of “professional information” should also exclude from the ambit of the Act information that all types of businesses utilise about individuals with whom they interact in their business or professional capacity.¹⁴⁰

3.10.5 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.

3.10.6 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.¹⁴¹ It does not tell us how he goes about his activities. Indeed, a prescription

140 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.

141 A collection of all the prescriptions of a doctor may reveal that he is incompetent or favours the medicine of one upplier over the other, etc.

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.¹⁴²

3.10.7 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.

3.10.8 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 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.¹⁴³

3.10.9 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

3.10.10 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.

3.10.11 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

142 See Jones C, Rankin TM, Q.C. 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.

143 A document outlining these benefits is included as "Benefit of IMS data Canada.pdf" in "Issue Paper Ancillary Docs.zip".

medical history (that is, personal health information) of any person, should be the most widely used source of information for these purposes.

3.10.12 The Commission has already proposed that de-identified information be excluded from the ambit of the Act.¹⁴⁴ This exemption will most probably provide the necessary relief sought in so far as provider information is concerned. It is, however, the Commission's preliminary opinion 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.

3.11 Conclusion

3.11.1 The Commission's provisional proposal is therefore that the scope of the protection of personal information legislation should include:

- a) information kept by both the public and the private sector;
- b) information pertaining to both natural and juristic persons;
- c) automatic and manual records;
- d) sound and image information;
- e) professional information;
- f) sensitive information; and
- g) critical information to the extent indicated.

3.11.2 Personal information kept in the course of a purely personal or household activity and de-identified information will be excluded.

3.11.3 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.

3.11.4 The Commission therefore recommends the legislative enactment to read as follows:

CHAPTER 2

GENERAL APPLICATION PROVISIONS

Application of this Act

3. This Act applies to-

- (a) the fully or partly automated processing¹⁴⁵ of personal information,¹⁴⁶ and the non-automated processing of personal information entered in a record¹⁴⁷ or intended to be entered therein;

144 See para 3.9 above.

145 **"processing"** means any operation or any set of operations concerning personal information, including in any case the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of information;

146 **"personal information"** means information about an identifiable, natural person, and in so far as it is applicable, an identifiable, 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, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
- (c) any identifying number, symbol or other particular assigned to the person;
- (d) the address, fingerprints or blood type of the person;
- (e) the personal opinions, views or preferences of the person, 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 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;
- (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, 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 person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
- (j) but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years;

To be noted that the definition of "personal information" in this Bill corresponds to the definition of "personal information" in the Promotion of Access to Information Act 2 of 2002. Since the two pieces of legislation are so closely related and the Commission has furthermore proposed that one supervisory authority be appointed to oversee both Acts it is important to ensure consistency in the terminology used. The Commission would, however, like to propose the following changes to this definition, which, if approved, would then be effected in the definition in both Acts:

- * the word "financial" included before the word "criminal" in subparagraph (b)
- * subpara (d) to read as follows: "(d) the address, blood type or any other biometric information of the person;
- * a semi-colon to be inserted after the words "the person" in para (e) and the rest of the sentence to be deleted.
- * Paragraphs (g) and (h) to be deleted.

The definition also provides for information about an identifiable juristic person in so far as it is applicable. (See also the definition of "personal information" in the ECT Act.)
Comment is invited in all instances.

- (b) the processing of personal information carried out in the context of the activities of a responsible party¹⁴⁸ established in the Republic of South Africa;
- (c) the processing of personal information by or for responsible parties who are not established in South Africa, whereby use is made of automated or non-automated means situated in South Africa, unless these means are used only for forwarding personal information.¹⁴⁹

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) that has been exempted from the application of the information principles in terms of sec 33.¹⁵⁰

Saving

-
- 147 "record" means any recorded information -
- (a) regardless of form or medium; and includes any -
 - (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 public or private body, respectively;
 - (c) whether or not it was created by a public or private body, respectively; and
 - (d) regardless of when it came into existence;
- 148 "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.
- 149 The responsible parties referred to are prohibited from processing personal information, unless they designate a person or body in South Africa to act on their behalf in accordance with the provisions of this Act. For the purposes of application of this Act and the provisions based upon it, the said person or body shall be deemed to be the responsible party.
- 150 Once the harmonisation of the legislation has taken place as recommended above in para 3.6.39 of the Discussion Paper, section 4 may read as follows:
- 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 intelligence or security services referred to in theAct;*
 - (d) *for the purposes of implementing the police tasks defined in the Act;*
 - (e) *by the armed forces in terms of theAct with a view to deploying or making available the armed forces to maintain or promote the international legal order.*

5. This Act will not affect the operation of any enactment that makes provision with respect to the processing of personal information and is capable of operating concurrently with this Act.

This Act binds the State

6. This Act binds the State.

Comment is invited in all instances.

3.11.5 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.¹⁵¹

3.11.6 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.

151 The Victorian Law Commission in Australia has recently 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 for storing data (known as a data bank),¹ 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 Public concerns have risen in tandem with the proliferation of personal 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 adoption of the Internet at exponential rates over the last decade. The ease of electronic communication that it has facilitated has spawned novel social and business practises which have necessitated even those countries who had previously established privacy and information protection legislation to reconsider and revise these laws.

4.1.2 In response to these developments, countries started to develop information protection laws in

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." Van der Merwe at 97, 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 SA LRC dated 26/8/2002 (hereafter referred to as "Tilley submission") at 3.

4 Piller *Macworld* at 2.

5 Victorian Law Reform Commission *Information Paper* 2001 at 5.

order to regulate these practices. The first law was 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).⁶

4.1.3 Since it was soon 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 Data⁷ (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.⁸

4.1.4 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.

4.1.5 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.

4.1.6 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.⁹

b) Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention)

6 See analysis of these laws in Flaherty D *Protecting Privacy in Surveillance Societies* University of North Carolina Press 1989.

7 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981.

8 OECD Guidelines.

9 Bennett Foundation Paper at 10.

4.1.7 The Convention is so far the sole international treaty to deal specifically with data protection. It entered into force on 1 October 1985.¹⁰ The Convention is potentially open for ratification by States that are not members of the CoE;¹¹ 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.¹²

4.1.8 The Convention is not intended to be self-executing. Art 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.¹³

4.1.9 The Basic Principles for Data Protection as set out in Chapter II of the Convention deals with:

- a) duties of the parties;¹⁴
- b) quality of the data;¹⁵
- c) special categories of data;¹⁶

10 As of 23 May 2002, it had been ratified by 27 CoE Member states.

11 Art 23.

12 Bygrave *Data Protection* at 32.

13 Bygrave *Data Protection* at 34.

14 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.

15 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.

16 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.

- d) data security;¹⁷
- e) safeguards for the data subject;¹⁸
- f) sanctions and remedies;¹⁹ and
- g) extended protection.²⁰

4.1.10 An additional Protocol to the Convention was adopted on 23 May 2001²¹ 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 (OECD Guidelines)

4.1.11 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

17 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.

18 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.

19 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.

20 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.

21 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.

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.

4.1.12 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 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 1996.²²

4.1.13 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.²³

4.1.14 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.²⁴

22 Bygrave *Data Protection* at 33 and references therein.

23 Victorian Law Reform Commission *Information Paper* 2001 at 23.

24 As referred to in Strathclyde LLM "Notes for Information Security Theme Two: Data protection" at 4. See para 8.2.14 in Ch 8 below for the developments in the APEC countries.

4.1.15 The OECD Guidelines are set out in the following principles:

- Collection Limitation Principle²⁵
- Data Quality Principle²⁶
- Purpose Specification Principle²⁷
- Use Limitation Principle²⁸
- Security Safeguards Principle²⁹
- Openness Principle³⁰
- Individual Participation Principle³¹

- Accountability Principle³²

-
- 25 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.
- 26 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.
- 27 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.
- 28 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.
- 29 Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- 30 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.
- 31 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.
- 32 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) European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (EU Directive)³³

4.1.16 In 1995 the European Union enacted the EU Directive in order to harmonise member states' laws in providing consistent levels of protections for citizens and ensuring the free flow of personal data within the European Union. Formally adopted in 1995, the Directive arose from the sense that European citizens were losing control over their personal information and that they had a fundamental right to privacy.³⁴

4.1.17 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.³⁵ Criticism came from both ends of the data protection spectrum.³⁶

4.1.18 The EU 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 adhere to.

4.1.19 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.³⁷ The Directive provides only a basic framework which will require to be developed in national laws.³⁸

33 EU Directive.

34 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. Such data retention schemes are already in place in Belgium, France, Spain and the United Kingdom and have been proposed in the Netherlands.

35 As referred to in Strathclyde LLM at 5.

36 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 United 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.

37 Art 3 of the EU Directive.

38 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.

4.1.20 The principles of the protection of the rights and freedoms of individuals which are contained in the Directive, notably the right to privacy, give substance to and amplify those contained in the CoE Convention.³⁹

4.1.21 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.

4.1.22 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.

4.1.23 The basic principles established by the EU Directive are as follows:⁴⁰

- 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

39 Recital 11 of the EU Directive.

40 Fisher R Excerpt from ***Privacy of Personal Information and the National Information Infrastructure***. See especially paras (a) –(e) of Art 6 of the EU Directive.

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.
- 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;
 - the right of recourse in the event of unlawful processing of data; and
 - the right to withhold permission to use their data in certain circumstances.
- 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.⁴¹
-

4.1.24 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.⁴²

4.1.25 Another possible way to protect the privacy of information transferred to countries that do not

41 Article 25 of the EU Directive.

42 See the discussion on crossborder transfers in Ch 8.

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.⁴³

4.1.26 In 1997 the European Union supplemented the 1995 directive by introducing the Telecommunications Privacy Directive.⁴⁴ This directive established specific protections covering telephone, digital television, mobile networks and other telecommunications systems.⁴⁵

4.1.27 On June 25, 2002 the European Union Council adopted the new Electronic Communications Privacy Directive as voted in the Parliament.⁴⁶ Under the terms of the new Directive member states may now pass laws mandating the retention of the traffic and location data of all communications taking place over mobile phones, SMS, landline telephones, faxes, e-mails, chatrooms, the Internet, or any other electronic communication device. Such requirements can be implemented for purposes varying from national security to the prevention, investigation and prosecution of criminal offences. This Directive allows the European Union member states to enact laws requiring Internet Service

43 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.

44 EU Directive.

45 European Union member countries were required to enact implementing legislation by October 1998. As of the summer 2002, however, several are still pending.

46 2439th Council meeting, Luxembourg, June 25, 2002. The original proposal was introduced in July 2000. The European Commission issued a proposal for a new directive on privacy in the electronic communications sector. The proposal was introduced as a part of a larger package of telecommunications directives aimed at strengthening competition within the European electronic communications markets. As originally proposed, the new directive would have strengthened privacy rights for individuals by extending the protections that were already in place for telecommunications to a broader, more technology-neutral category of “electronic communications.”

During the process, however, the Council of Ministers began to push for the inclusion of data retention provisions, requiring Internet Service Providers and telecommunications operators to store logs of all telephone calls, e-mails, faxes, and Internet activity for law enforcement purposes. These proposals were strongly opposed by most members of the Parliament. However, following the events of September 11, the political climate changed and a deal was reached between parties to vote in favour of the Council’s position.

Providers, and other telecommunications operators, to retain the traffic and location data of all people using mobile phones, text messaging, land-line telephones, faxes, e-mails, chat rooms, the Internet, or any other electronic communication devices to communicate.⁴⁷

4.1.28 It adds new definitions and protections for “calls,” “communications,” “traffic data” and “location data” in order to enhance the consumer’s right to privacy and control in all kinds of information processing. These new provisions ensure the protection of all information (“traffic”) transmitted across the Internet, prohibit unsolicited commercial marketing by e-mail (spam) without consent, and protect mobile phone users from precise location tracking and surveillance. The directive also gives subscribers to all electronic communications services (such as GSM and e-mail) the right to choose whether or not they are listed in a public directory.

e) United Nations Guidelines

4.1.29 Some account should also be taken of the UN Guidelines. The United Nations’ (UN) Guidelines Concerning Computerised Personal Data Files (hereinafter termed UN Guidelines) were adopted by the UN General Assembly on 14 December 1990.⁴⁸ 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.⁴⁹

f) Commonwealth Guidelines

47 EPIC and Privacy International *Privacy and Human Rights Report 2002* at (iii).

48 Doc E/CN.4/1990/72, 20.2.1990.

49 Bygrave *Data Protection* at 33.

4.1.30 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.

4.1.31 The intent of the proposed model legislation is to ensure that governments 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 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.

4.1.32 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.

4.1.33 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.

4.1.34 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.

4.1.35 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.

4.1.36 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.

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. 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.⁵⁰ 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.⁵¹

4.2.2 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.

50 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.

51 Bygrave **Data Protection** at 3.

4.2.3 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.

4.2.4 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.

4.2.5 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.⁵² 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 the private sector.⁵³

4.2.6 The introduction to Paragraph 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

52 New Zealand Discussion Paper at 1.

53 See discussion in Ch 7 below.

4.2.7 What follows is a discussion on 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,⁵⁴ and have accordingly been implemented to find the principles to be embodied in a South African act.

4.2.8 The information protection principles that will be discussed are the following:

- Principle 1: Processing Limitation (fair and lawful processing)
- Principle 2: Purpose Specification
- Principle 3: Further Processing Limitation
- Principle 4: Information Quality
- Principle 5: Openness
- Principle 6: Security Safeguards
- Principle 7: Individual participation
- Principle 8: Accountability

It is to be noted that additional principles are set out for sensitive information. See discussion below.

4.2.9 Respondents to the Issue Paper were in general supportive of the incorporation of these principles in legislation⁵⁵ and indicated that the principles should apply to all personal information kept by a responsible party, who should be obliged to comply with them.⁵⁶

54 Bygrave *Data Protection* at 57.

55 Eg. Vodacom; The Banking Council; Gerhard Loedoff Eskom; ENF for Nedbank; ISPA.

56 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. To elaborate further the principles would place the following obligations on credit grantors' 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;
- 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

4.2.10 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.⁵⁷

4.2.11 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.⁵⁸

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.⁵⁹

4.2.12 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

-
- c) the data may be put to and to whom it will be disclosed. Provision will then be made for "opt-out" consent; and
 - d) the credit grantor will have to obtain the credit applicant's consent to access the applicant's credit report; the credit grantor 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;
 - e) the credit grantor will have to give notice to a data subject prior to transferring default (adverse) information on the data subject to a credit bureaux, 28 days notice in writing is recommended;
 - f) the credit grantor will have to ensure that there is only one listing in respect of a failure to pay a debt.

The Credit Bureau industry will then have the following obligations:

- 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; and
- d) Ensuring that the data is erased once the data retention period has lapsed
- e) Credit Bureaux will have to provide a statement of their functions and activities for inspection by the data protection authority, because of competition and legitimate business this information cannot be made public knowledge.
- f) Credit Bureaux will have to report to the data protection authority on the results of the independent audit of its data processing and data security systems.

57 The Internet Service Providers Association.

58 LOA; Liberty.

59 LOA.

collection.⁶⁰

4.2.13 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 7: individual participation and principle 5: 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.⁶¹

4.2.14 The idea was therefore supported that the legislation would need to create a framework for information protection based on the principles of information protection as set out in the Issue Paper.

62

(i) Principle 1: Processing Limitation (Fair⁶³ and lawful processing)

4.2.15 It is sometimes argued that the primary principle of information protection laws is that the personal information must be processed fairly and lawfully.⁶⁴ This principle is primary because it

60 Medical Research Council.

61 SAPS.; See Chapter 3 above dealing with the scope of the legislation and specifically "critical data".

62 LOA.

63 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.

64 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

embraces and generates the other core principles of information protection laws presented below. 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 information⁶⁵ or not specifically mentioned at all.⁶⁶

4.2.16 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).⁶⁷ The determination what is fair may be a more difficult task.⁶⁸

4.2.17 At a general level the notion of fairness⁶⁹ 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.⁷⁰

4.2.18 Fairness/reasonableness implies that the processing of information be transparent to the data subject.⁷¹ 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 5 below. Another requirement that may flow from this argument is that information should be collected from the

ethnic origin, political opinions, religious or philosophical beliefs etc, only in specific cases.

65 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.

66 Bygrave *Data Protection* at 58 and the reference therein to the Norwegian PDA.

67 Sec 4 of Canada’s federal Privacy Act; IPP1(a) of Australia’s federal Privacy Act; Data Protection Principle 1 of the UK Data Protection Act, 1998.

68 Strathclyde LLM at 16.

69 “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*.

70 Bygrave *Data Protection* at 58.

71 Bainbridge D *Data Protection* CLT Professional Publishing Welwyn Garden City 2000 (hereafter referred to as “Bainbridge *Data Protection*”) at 59.

data subject, not from third parties.⁷² This requirement is expressly laid down in some, but not the majority of information protection instruments.⁷³

4.2.19 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.⁷⁴ 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.⁷⁵ 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.⁷⁶ See Principle 3 below.

4.2.20 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 principle.⁷⁷

4.2.21 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.⁷⁸

72 Principle 2 and 4 of New Zealand Privacy Act. See below.

73 Bygrave *Data Protection* at 59 and the references made therein.

74 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"). Sec 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.

75 Bygrave *Data Protection* at 59.

76 Bainbridge *Data Protection* at 58; Commonwealth Secretariat *Model Law 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 Act dealing with the collection, use, disclosure and retention of personal information by public agencies.

77 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.

78 Information Commissioner *Data Protection Principles* at 18.

4.2.22 Where personal information contain 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.

4.2.23 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.⁷⁹ The principle is prominent in all the main international information protection instruments as well as in national legislation.⁸¹ See Principle 2 below.

4.2.24 Article 6(1)(c) of the EU Directive 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;⁸²

4.2.25 The minimality principle is also manifested in Arts 7 and 8 of the Directive⁸³ which deal with

79 Roos 1998 *THRHR* at 499 and the references made therein. See discussion below on Principle 2.

80 Pretexting is the practice of collecting information about a person using false pretenses. Typically investigators pretext by calling family members or coworkers 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.

81 Sec 5(3) of Canada's Personal Information Protection and Electronic Documents Act 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 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 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 of those purposes.

82 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; See Principle 4 below.

83 Article 7 of the EU *Directive*

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

this question extensively, by setting out circumstances which will be reasonable, and what is not reasonable processing. 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 these 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).⁸⁴

4.2.26 Of crucial importance for the extent to which information processing may occur, is the

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
 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.

However there are a range of exceptions dealing with where

2(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.....

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.

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.

4.2.27 The necessity criterion should probably be construed as embracing two overlapping requirements:⁸⁵

- k) that the processing corresponds to a pressing (and legitimate) social, political or commercial need;⁸⁶
- l) 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.⁸⁷

4.2.28 The amount of personal information collected should be limited to what is necessary to achieve the purpose for which the information is gathered.⁸⁸ 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”.⁸⁹

4.2.29 In determining whether processing is fair/reasonable, regard is furthermore to be had to the method by which the information was obtained.⁹⁰ 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

85 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 6(1)(c) of the Directive.

86 The processing of data by credit bureaux, for instance, corresponds to a legitimate commercial and social need, and in contradiction to the minimality principle it is necessary that the information collected be comprehensive so as to facilitate correct lending decisions.

87 Bygrave *Data Protection* at 343.

88 Sec 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.

89 The term “proportionality” is used by the CoE in several of its data protection instruments. See also s 3a of Germany’s Federal Data Protection Act for the term “frugality”.

90 Bainbridge *Data protection* at 58.

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.”⁹¹

4.2.30 In order to give effect to the principle, two sets of rules can be identified:

- a) rules requiring responsible parties to collect information directly from data subjects in certain circumstances;
- b) rules prohibiting the processing of personal information without the consent of the data subject.

4.2.31 Rules requiring that information may only be collected from the subject directly, are found only in a minority of information protection instruments,⁹² 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.⁹³

4.2.32 Some privacy instruments have grappled with the consent issue. The EU Directive provides

91 Bygrave *Data Protection* at 59.

92 Sec 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.

93 **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.

that personal information may only be processed if the individual concerned "has unambiguously given his consent".⁹⁴

4.2.33 Other instruments make no mention of a consent requirement⁹⁵ while yet others often stipulate consent in fairly narrow contexts eg as a precondition for disclosure of information to third parties.⁹⁶

4.2.34 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.⁹⁷ The alternative prerequisites are often formulated broadly, thereby reducing significantly the extent to which responsible parties are hostage to the consent requirement in practice.⁹⁸ 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.⁹⁹ ¹⁰⁰

94 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 in section 14 that:

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.

95 For eg the CoE Convention.

96 Para 10 of the OECD Guidelines.

97 Art 7, see above.

98 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.

99 Bygrave *Data Protection* at 66.

100 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.

4.2.35 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 processing of sensitive information which refers to “explicit consent.”¹⁰¹

4.2.36 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.¹⁰²

4.2.37 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”).¹⁰³

4.2.38 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.

4.2.39 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

-
- 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.

101 Douwe Korff *EC Study* at 74.

102 Ibid.

103 Ibid.

principles. Such a broad consent will probably also be unreasonable (unfair and contra bonos mores).¹⁰⁴

4.2.40 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.¹⁰⁵

4.2.41 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 volonté 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.¹⁰⁶

4.2.42 In South Africa, sec 51 (1) of the Electronic Communications and Transactions Act¹⁰⁷ 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.

4.2.43 In Issue Paper 24 the question was posed whether the opt-out approach would constitute valid consent. Responses were varied.

104 **Neethling's Law of Personality** 251.

105 The LOA argued that clients should be afforded the right to consent, or not, to the collection of information. It must be pointed out, however, that 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 Data Privacy legislation should accommodate the various types of consents.

106 Douwe Korff **EC Study** at 76.

107 **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.

4.2.44 It was argued that the "opt-out" approach implies implicit consent;¹⁰⁸ and would constitute valid consent, provided it meets all the criteria of implied consent required by the common law and set out in the privacy instruments.¹⁰⁹

4.2.45 It was suggested that the following requirements be met by responsible parties when the "opt-out" approach is being used:-¹¹⁰

- 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.¹¹¹

4.2.46 The banking industry explained that it has adopted the opt-out approach¹¹² since there is no

108 SABC.

109 Vodacom.

110 SABC.

111 This requirement (informed consent) re-iterated by the Banking Council.

112 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:

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.¹¹³

4.2.47 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 Banking Practice.¹¹⁴

-
- 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 our services and products is conditional upon your consent”.

113 The Banking Council.

114 **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 depend 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:

4.2.48 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.¹¹⁵ 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.¹¹⁶

4.2.49 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 USA's recent federal legislation about spam¹¹⁷ (H.R.2515 Anti-Spam Act of 2003).¹¹⁸

4.2.50 One of the clearest arguments against allowing opt-out in this context has been written by David Harris. 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

-
- 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;"

115 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.

116 Sanlam Life; Legal Service.

117 See discussion on direct marketing below.

118 Prof Martin Olivier.

recipient can be effectively overwhelmed by the number of received e-mails.^{119,120}

4.2.51 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:¹²¹

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.

4.2.52 In conclusion it should be noted that the proposed legislation will make provision for a consent requirement as set out below. However, the way in which the consent provision is to be implemented will have to be set out in the codes of conduct of the different sectors as approved by the Information Commissioner, or in relevant regulations. See also the definition of “consent” in sec 2.¹²²

4.2.53 Comment is invited on the following clauses:

PRINCIPLE 1 ***Processing limitation***

119 Prof Martin Olivier.

120 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. I suggest 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.

121 Douwe Korff *EC Study* at 77.

122 ‘consent’ means any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal information relating to them;

Lawfulness of processing¹²³

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.*

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.* ¹²⁴

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.*

¹²³ OECD par 7; CoE art 5; EU Cir art 6(1)(a); New Zealand (NZ) Principle 4; The Netherlands(NL) art 76; Roos thesis fnnt 51 at 482 and 483.

¹²⁴ Sec 8 (embodying the minimality principle, see paras 4.2.23-4..2.28 above) can also be included under Principle 2: Purpose specification and Principle 4:Data quality. Comment is invited.

- (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 93¹²⁵ below.*

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.*

125

This section furthermore to be read with the other information principles; See also ss 10, 11 and 12 of the UK DPA; arts 14 and 15 of the EU Directive; See also sec 45 of the ECT Act for the opt-out option regarding unsolicited commercial communications.

(ii) Principle 2: Purpose specification/ Collection limitation

4.2.54 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.

4.2.55 This principle is furthermore set out in Article 6(1)(b) of the EU Directive.¹²⁶ 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.¹²⁷

Purpose specified at time of collection

4.2.56 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.

4.2.57 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?

4.2.58 Another issue raised is that 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

¹²⁶ Article 6(1)(b) of the EU Directive stipulate respectively 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.

¹²⁷ See discussion in Roos thesis at 483.

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?¹²⁸

4.2.59 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.¹²⁹ They are therefore not permitted to use the information for an unregistered purpose.¹³⁰ (It is proposed that the South African legislation will make provision for a process of notification. See discussion in Chapter 5 below.)

4.2.60 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.

4.2.61 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 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.

4.2.62 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.¹³¹

128 New Zealand Discussion Paper at 3.

129 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.

130 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.

131 New Zealand Discussion Paper at 2.

4.2.63 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.¹³²

4.2.64 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.¹³³

4.2.65 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.¹³⁴

4.2.66 Respondents to Issue Paper 24 agreed with this principle.¹³⁵ Responsible parties should be obliged to identify the minimum amount of information that is required in order properly to fulfil their purpose 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.¹³⁶

Retention of records

132 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 .

133 Douwe Korff *EC Study* at 63.

134 Douwe Korff *EC Study* at 64.

135 ENF for Nedbank; LOA; Credit Bureau Association.

136 ENF for Nedbank; LOA.

4.2.67 Article 6(1)(e) of the EU Directive stipulate 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.

4.2.68 See also art 5(e) of the CoE Convention.¹³⁷ The Commonwealth Model Law for private sector sets out the finality of records in art 20 (2) and (3).¹³⁸

4.2.69 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,¹³⁹ national laws make specific provision for the erasure etc of personal information once the data are no longer required.¹⁴⁰

4.2.70 For example in national laws see Data Protection Principle 5 in the UK Data Protection Act¹⁴¹ and Principle 9 of the New Zealand Privacy Act.¹⁴² Similar provisions are found in several

137 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.

138 Article 20 Retention of records
(1).....
(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).

139 US federal Privacy Act 1974 being an example.

140 Bygrave *Data Protection* at 60.

141 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.

142 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.

other jurisdictions. See for example, principle 2(2) of the Hong Kong Personal Data (Privacy) Ordinance¹⁴³ and the 1993 Quebec Act respecting the Protection of Personal Information in the Private Sector (section 12).¹⁴⁴

4.2.71 The principle will however be subject to the requirements of other enactments. There are, for example, laws requiring taxpayers to retain taxation records and health agencies to retain medical records. In the public sector the national archives¹⁴⁵ and national¹⁴⁶ and local¹⁴⁷ government require the retention of certain archives.¹⁴⁸

4.2.72 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.

4.2.73 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);

143 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 or are to be used.

144 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.

145 National Archives of South Africa Act 43 of 1996.

146 Electoral Act 73 of 1998.

147 Eg. the Local Government Municipal Electoral Act 27 of 2000 and the Local Government Municipal Property Act 6 of 2004.

148 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 and

*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.

- * 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).

4.2.74 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.¹⁴⁹

4.2.75 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.¹⁵⁰

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.¹⁵¹

4.2.76 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.

4.2.77 In the Commonwealth Model Bill for the public sector this principle is set out in art 14.¹⁵² In

149 The Banking Council.

150 LOA.

151 SAFPS.

152 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

the Model Law for the private sector it is set out in art 20.¹⁵³

4.2.78 Comment is invited on the following clauses:

PRINCIPLE 2

Purpose specification¹⁵⁴

Collection for specific purpose

11. *Personal information must be collected for a specific, explicitly defined and legitimate purpose.*

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

of personal information held by a public authority.

153 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 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).

154 NL art 7; NZ Principle 3.

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 proceedings that 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.*

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).

(iii) Principle 3: Further Processing Limitation

4.2.79 The principles of collection limitation, purpose specification and use limitation are closely related and require that, once personal information are collected, there are limits to the internal uses to which a collecting body may put them, or to the external disclosure that may be made.¹⁵⁵ The notion of “relevance” underlies all these principles, since the information may be processed only for purposes specified at the time of collection.¹⁵⁶ Information gathered to determine income tax liability, for example, may not be used to evaluate eligibility for social assistance. If information is disclosed

¹⁵⁵ See discussion in Roos thesis at 496.

¹⁵⁶ See purpose principle above.

for other purposes, the consent of the individual must first be obtained.¹⁵⁷

4.2.80 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.¹⁵⁸

4.2.81 In New Zealand this principle is set out in Principle 10: Limits on use of personal information¹⁵⁹ and in the UK it is set out in Principle 2.¹⁶⁰

4.2.82 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.¹⁶¹

4.2.83 The Commonwealth Model Law for the Public sector makes provision for this principle in section 9.¹⁶² The Commonwealth Model Law for the private sector also makes provision for this

157 Roos 1998 *THRHR* at 505.

158 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").

159 New Zealand Discussion Paper at 7.

160 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.

161 The principle itself is straightforward and runs only to a single sentence. However, the detail is to be found in the list of exceptions.

162 9 Limits on use of personal information
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
(b) 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 –

principle in sections 12, 14 and 15.¹⁶³

-
- (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.

163 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]*

4.2.84 Two questions must be distinguished. First of all, what should be regarded as the specified purpose,¹⁶⁴ and secondly, how is the incompatibility of any secondary processing with the primary purpose to be determined.¹⁶⁵

4.2.85 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.¹⁶⁶

4.2.86 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 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

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.

¹⁶⁴ Dealt with in Principle 2.

¹⁶⁵ 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.

¹⁶⁶ Douwe Korff *EC Study* at 64.

to see how this test will be applied to the private sector in practice.¹⁶⁷

4.2.87 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.).¹⁶⁸

4.2.88 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.

4.2.89 In other words, under the Dutch Law too 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 unambiguously consented to this beforehand).¹⁶⁹

4.2.90 An issue has arisen overseas as to whether "browsing" constitutes a "use" under such a principle. An English case suggests that simply reading personal information, but not employing that

167 Douwe Korff *EC Study* at 64.

168 Douwe Korff *EC Study* at 65.

169 Douwe Korff *EC Study* at 65.

information for a purpose, may not constitute "use." In that case it could be shown that a police officer had checked a confidential police informationbase 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.

4.2.91 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.

4.2.92 As will be clear from the above, Art. 6(1)(b) of the Directive 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 Art. 8(4), also quoted above, i.e. the Member States may only allow this (even with suitable safeguards) with regard to research which serves a substantial public interest.¹⁷⁰

4.2.93 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.¹⁷¹

170 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, in that 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 some in other laws or regulations.

171 Credit Bureau Association.

4.2.94 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.

4.2.95 The OECD Guidelines incorporate the principle of disclosure limitation within a broader principle termed the “Use Limitation Principle”,¹⁷² while the UN Guidelines specifically address the issue of disclosure under the principle of purpose specification.¹⁷³

4.2.96 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.¹⁷⁴

4.2.97 In New Zealand this principle is set out in Principle 11¹⁷⁵: Limits on disclosure of personal

172 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.

173 Bygrave *Data Protection* at 67.

174 Bygrave *Data Protection* at 67.

175 **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

information¹⁷⁶ The Commonwealth Model Law for the Public sector makes provision for this principle in sections 11 and 12¹⁷⁷ and in the Model Law for the private sector in sections 13 and 16.¹⁷⁸

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.

176 New Zealand Discussion Paper at 7.

177 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.

178 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

4.2.98 In Issue Paper 24 the question was posed whether institutions should be allowed to share information and, if so, under what circumstances. Respondents generally felt that information should be shared (disclosed), but subject to specific conditions. Although there has been a growth in information sharing,¹⁷⁹ there is currently legal uncertainty as to the legality of such practices as well as the proper ways of handling the information.¹⁸⁰

4.2.99 Submissions were received from the following sectors: insurance,¹⁸¹ banking,¹⁸² credit

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.

(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.

179 SALRC *Issue Paper 24* at 122.

180 MFSA.

181 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 continues, or long-term insurers will not be able to properly assess the risks involved.

182 Nedbank indicated that an area which will need to be carefully considered is that of the use of information within a

bureaux,¹⁸³ the fraud prevention service,¹⁸⁴ archives¹⁸⁵ and telecommunications.¹⁸⁶

4.2.100 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

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. 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.

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.

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. 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 e.g. 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.

- 183 Data sharing within the context of the South African credit information system prevents over-commitment, bad debt, fraud , money laundering and promotes responsible lending , and accordingly should be allowed. 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 the 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 to, again the onus would be on the subscribers or clients of the credit bureaux .
- 184 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. It is, however, proposed that there should be a provision similar to sec 29 of the UK Data Protection Act in any future legislation and that for the purposes of this exemption. 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 in term 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.
- 185 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. 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
- 186 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.

must know that the information will be shared in certain circumstances).¹⁸⁷

4.2.101 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.¹⁸⁸ Another view was that the consent requirements should constitute an 'opt out' option as discussed.

4.2.102 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.¹⁸⁹

4.2.103 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 informationbase maintained by the LOA¹⁹⁰.

187 Vodacom.

188 Strata.

189 Credit Bureau Association.

190 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 information which ABC deems necessary, and

a) 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

4.2.104 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.¹⁹¹

4.2.105 In April 2003 the Performance and Innovation Unit (PIU) in the UK, one of Whitehall's most influential bodies, produced a report,¹⁹² 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.¹⁹³

4.2.106 It has been argued that the PIU report effectively marginalised information protection to enable information sharing to take place.¹⁹⁴ 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.

4.2.107 As to who should be responsible for the accuracy and maintenance of the information, where it is shared by different entities, different views were expressed. Some commentators held that

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)"

191 SAPS.

192 Performance and Innovation Unit *Privacy and Data Sharing, the Way Forward for Public Services* (hereafter referred to as PIU report) April 2002 available at <http://www.number-10.gov.uk/su/privacy/index.htm>.

193 Whilst the PIU Report focuses on government bodies, the principles apply equally to companies and other "private bodies"

194 Sarah Williams "Writing in Computers and Law" available at <http://www.scl.org/Services/default.asp?p=154&c=-999&ctID=12&clD=1140000634>.

the data processor should be responsible.¹⁹⁵ ¹⁹⁶ 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). ¹⁹⁷ ¹⁹⁸ 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.¹⁹⁹ See discussion on Principle 8 (accountability) below.

195 SAFPS.

196 Liberty indicated that, as regards a 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 his 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.

197 The Banking Industry.

198 ENF for Nedbank.

199 Credit Bureau Association.

4.2.108 Comment is invited on the following clauses:

PRINCIPLE 3²⁰⁰

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.

(iv) Principle 4: Information Quality

4.2.109 Principle 2 of the OECD Guidelines reads as follows:²⁰¹

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.

4.2.110 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.²⁰²

4.2.111 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

201 CDT's Guide.

202 See discussion in Roos thesis at 490.

information that was originally adequate becomes inadequate,²⁰³ and use thereof unreasonable.

4.2.112 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 terms to describe the stipulated information quality. Art 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.²⁰⁴ Other laws refer to “accuracy or correctness” or “completeness” (OECD Guidelines).²⁰⁵

203 Information Commissioner *Data Protection Principles* at 18.

204 Fourth Principle
Personal data shall be accurate and, where necessary, kept up to date.

205 Bygrave *Data Protection* at 62.

4.2.113 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).²⁰⁶ 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.²⁰⁷

4.2.114 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.²⁰⁸

4.2.115 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 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.²⁰⁹

4.2.116 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.²¹⁰ 4.2.117 In the Commonwealth

206 Bygrave *Data Protection* at 63.

207 Information Commissioner *Data Protection Principles* at 19.

208 Douwe Korff *EC Report* at 62.

209 Douwe Korff *EC Report* at 62.

210 Bygrave *Data Protection* at 13.

Model Law for the public sector the quality data principle is manifested in art 9.²¹¹ In the Model Law for the private sector it can be found in art 17.²¹²

4.2.118 In New Zealand the principle manifests itself in Principle 8 stipulating that the accuracy etc of personal information has to be checked before use.²¹³

4.2.119 Even though the finality principle has been included in Principle 2 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.²¹⁴

4.2.120 A privacy risk exists where such personal information is retained since:²¹⁵

- 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.

211 **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.

212 **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 collected the information;

(b) the individual consents to the updating; or

(c) this Act or another law permits the updating.

213 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.

214 Art 5 of the CoE Convention.

215 Bygrave *Data Protection* at 60.

4.2.121 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.²¹⁶ See Principle 2 (Purpose specification) above.

4.2.122 Factors, which make the quality of information retention difficult are that information may be saved in a different format and in different mediums.²¹⁷ For instance, 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.²¹⁸

4.2.123 There may be a substantial cost implication for business, but the vision is a principle of good record information management, which is an excellent principle to work towards. Perhaps a phased implementation period would be advisable.

4.2.124 Comment is invited on the following clause:

PRINCIPLE 4

Information quality²¹⁹

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.

²¹⁶ Information Commissioner **Data Protection Principles** at 20.

²¹⁷ The Banking Council.

²¹⁸ LOA.

²¹⁹ OECD par 8; CoE art 5; EU Dir art 6(1) (c); Roos thesis at 492.

(v) Principle 5: Openness

4.2.125 The principle of openness flows from the notion of fairness and transparency set out above.²²⁰ 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 knowledge of the fact that personal information about him or her is being kept by a specific body.²²¹

4.2.126 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).²²² Obviously allowance must be made for exceptions to this principle, for example where personal information is processed for the purposes of national security.²²³

4.2.127 The most important of these rules are those which require responsible parties to orient data subjects directly about their information-processing operations. Secondly, 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.²²⁴

4.2.128 Principle 6 of the OECD Guidelines²²⁵ stipulates that there should be a general policy of

220 See discussion in Roos thesis at 505.

221 Roos 1998 *THRHR* at 499.

222 *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).

223 See in general on exceptions Neethling *Huldigingsbundel WA Joubert* at 125-128.

224 Bygrave *Data Protection* at 63.

225 Para 9 Part II Basic Principles of National Application of OECD Guidelines; Roos 1998 *THRHR* at 503.

openness about developments, practices and policies with respect to personal information.²²⁶ 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.

4.2.129 Articles 10-11 of the EU Directive²²⁷ 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.²²⁸

226 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.

227 Article 10 of the EU Directive
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.

228 At 98.

4.2.130 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 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.²²⁹

4.2.131 Art 10-11 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)).

4.2.132 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".

4.2.133 This means that the following facts should be publicly known:²³⁰

- b) the existence of record-keeping systems, registers and data banks that contain personal data;
- c) nature of the data being processed;
- d) a description of the main purpose and uses of the data; and
- e) identity and usual residence of the data controller.

4.2.134 An example of the principle in national legislation is that of Principle 3 of the New Zealand Privacy Act.²³¹ Underlying the principle are the idea of openness: that collection of personal

229 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 be always 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).

230 CDT's Guide.

231 **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 -

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.²³²

4.2.135 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 records must be kept.²³³ A similar provision is found in section 51 which applies to private bodies. PAIA does not, however, specifically deal with the collection of information.

4.2.136 It was clear from the response to the Issue Paper that there is in general support for this principle.²³⁴

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.

4.2.137 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-justified. The ultimate question should be how much information must be provided so that any consent is properly informed.

235

-
- (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 sec 1.

232 New Zealand Discussion Paper at 3.

233 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.

234 The Banking Council; SAFPS.

235 LOA.

4.2.138 In addition to the right of access to his information record, a data subject must also have the right to require from the responsible party information as to the identity of all persons who have had access to his information record. This will enable him 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.²³⁶ See Principle 7 below.

4.2.139 Comment is invited on the following clauses:

PRINCIPLE 5
Openness²³⁷

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

236 Ibid.

237 NZ Principle 3; Three elements: notification to DPC; register by DPC; information to subject.

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.

(vi) Principle 6: Security safeguards

4.2.140 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.²³⁸ 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.

4.2.141 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.²³⁹ However, in many instances appropriate business and legal safeguards have yet to be developed.

4.2.142 The advent of information technology has increased interest in the right to privacy. Computers now support critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information.²⁴⁰ 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. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially and has become more difficult to protect.^{241 242 243}

4.2.143 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

238 CDT’s Guide to Online Privacy; See Bygrave **Data Protection** at 67; Roos thesis at 515.

239 Cameron O Information and Systems Management **Balancing Security and Privacy** Discussion Document for the Department of Justice to Establish Security Requirements and Frameworks (hereafter referred to as “ISM Discussion Document” at 4.

240 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.

241 OECD Security Guidelines at 7.

242 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.

243 SALC **Computer-related crime** Discussion Paper at 3; The potential danger if computers performing these functions are interfered with is very serious.

with, these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.²⁴⁴²⁴⁵

4.2.144 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 technology, the likelihood increases that information attacks will threaten vital national interests.²⁴⁶

4.2.145 In addition, the disgruntled organisation insider is a significant threat.²⁴⁷ As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use.²⁴⁸²⁴⁹

4.2.146 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

-
- 244 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.
- 245 GAO testimony at 3.
- 246 GAO testimony at 4.
- 247 A 32 year old Johannesburg man bearing a grudge against the company, was recently found guilty of loading a virus on the computer of Edgars, 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.
- 248 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")at 10.
- 249 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. lafrica.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 thta, 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.
 - * 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.

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.²⁵⁰

4.2.147 Security specialists have found it useful to place potential security violations in three categories:²⁵¹

- 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.

4.2.148 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.²⁵²

.2.149 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

250 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.

251 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, or
- They could not make informed judgments as to whether they were spending too little or too much of their resources on security.

252 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.

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 those supporting national defence and emergency services, could be disrupted.²⁵³

4.2.150 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.²⁵⁴ 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.²⁵⁵ 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.²⁵⁶

4.2.151 Problems regarding the security of information have been acknowledged and addressed worldwide since the early eighties. Both the EU Directive and the OECD Guidelines make provision for security issues.²⁵⁷

4.2.152 The principle manifests itself in Principle 5 of The OECD Guidelines.²⁵⁸ 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

253 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.

254 CCIPS United States Department of Justice "Electronic Frontier" at 10.

255 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.

256 VeriSign Internet Security Intelligence Brief June 2005.

257 CDT's Guide; See Bygrave *Data Protection* at 67.

258 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.

data. A representative provision is also found in Art 7 of the CoE Convention.²⁵⁹

4.2.153 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 (art 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 (Art 17(2)). The latter requirements are supplemented in Art 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".²⁶⁰ Further, the measures taken pursuant to Art 17(1) and (3) shall be documented. (Art 17(4)).

4.2.154 In the Commonwealth Model Law for the public sector the security principle is set out in art 13²⁶¹ and in the Model Law for the private sector in art 18.²⁶²

259 Art 7 of the CoE Convention:
"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."

260 Bygrave *Data Protection* at 68.

261 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.

262 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) Upon request, the organisation shall make available to any person a general description of the safeguards that it uses

4.2.155 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 now drawn up new guidelines entitled “Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security”²⁶³ to deal specifically with cyber terrorism, computer viruses, hacking and other threats.²⁶⁴ The Security Guidelines should be read in conjunction with the abovementioned Guidelines.

4.2.156 The Guidelines suggest the need for a greater awareness and understanding of security issues and the need to develop a “culture of security”.²⁶⁵

4.2.157 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.²⁶⁶ This 2002 guideline built on the security safeguards principle in the earlier 1992 OECD guidelines.

to protect personal information and to fulfil its obligations under subsection (1).

263 See fn 240 above.

264 Organisation for Economic Co-operation and Development (OECD) “OECD Governments Launch Drive to Improve Security of Online Networks” News release dated August 7, 2002 (hereafter referred to as “OECD news release”) at 1.

265 OECD Security Guidelines at 7.

266 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.

4.2.158 The nine principles are complementary and should be read as a whole.²⁶⁷ The Principles are as follows:

- a) Awareness:²⁶⁸ Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.²⁶⁹
- (b) Responsibility:²⁷⁰ All participants are responsible for the security of information systems and networks.²⁷¹
- (c) Response:²⁷² Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.²⁷³
- d) Ethics:²⁷⁴ Participants should respect the legitimate interests of others.²⁷⁵
- e) Democracy:²⁷⁶ The security of information systems and networks should be compatible with

267 OECD Security Guidelines at 9.

268 OECD Security Guidelines at 10.

269 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.

270 OECD Security Guidelines at 10.

271 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.

272 OECD Security Guidelines at 10.

273 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.

274 OECD Security Guidelines at 11.

275 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.

276 OECD Security Guidelines at 11.

essential values of a democratic society.²⁷⁷

- f) Risk assessment:²⁷⁸ Participants should conduct risk assessments.²⁷⁹
- g) Security design and implementation:²⁸⁰ Participants should incorporate security as an essential element of information systems and networks.²⁸¹
- h) Security management:²⁸² Participants should adopt a comprehensive approach to security management.²⁸³
- i) Reassessment:²⁸⁴ Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.²⁸⁵

4.2.159 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

277 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.

278 OECD Security Guidelines at 11.

279 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.

280 OECD Security Guidelines at 12.

281 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.

282 OECD Security Guidelines at 12.

283 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. 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.

284 OECD Security Guidelines at 12.

285 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.

promoting a culture of security as set out in the Guidelines.²⁸⁶

4.2.160 An example of national legislation incorporating the security principle is Data Protection Principle 7 of the UK Data Protection Act²⁸⁷ and Principle 5 of the New Zealand Act, which is closely modeled on a principle in the Australian Privacy Act.²⁸⁸

4.2.161 In practice six major areas of security design and management have been identified.²⁸⁹ 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.

4.2.162 The security mechanisms of traditional paper-based communications media - envelopes and locked filing cabinets - are therefore being replaced by technological and organisational

286 OECD Security Guidelines at 15.

287 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.

288 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.

289 GAO testimony at 10.

measures.

4.2.163 Some examples of security technologies²⁹⁰ 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.

4.2.164 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.²⁹¹ Many technologies can be used in many different ways. It is therefore crucial to recognise the context in which any given technology is used.²⁹²

4.2.165 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.

4.2.166 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.

4.2.167 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

290 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.

291 OECD Hall Report at 16 and 23.

292 OECD Hall Report Introduction at 4.

which information protection should focus have been identified²⁹³ and a series of Data-protection-friendly Technologies were recommended with reference to the principles of information minimisation and as-soon-as possible anonymisation.²⁹⁴

4.2.168 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.²⁹⁵

4.2.169 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 compatibility 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).²⁹⁶

4.2.170 In South Africa certain offences were created in sections 85 to 89²⁹⁷ of the Electronic

293 Douwe Korff **EC Study** at 160; They are authority (the basis for providing access, e.g. 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).

294 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.

295 Douwe Korff **EC Study** at 161.

296 Douwe Korff **EC Study** at 161.

297 As set out in Chapter XIII (Cyber crime).

Communications and Transactions Act²⁹⁸ 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.²⁹⁹ 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.

4.2.171 The question therefore 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. See question 15 in Issue Paper 24.

4.2.172 Respondents were divided in their answer to this question. Most commentators felt that security issues should form part of the new privacy legislation.³⁰⁰ Some commentators were of the opinion that security issues have been adequately addressed in other legislation.^{301 302}

4.2.173 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.³⁰³ (See also the discussion on critical data in Chapter 3).³⁰⁴

298 Act 25 of 2002.

299 The ECT Act only deals with electronic data and transactions.

300 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.

301 Vodacom.

302 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 (that still needs to be put into operation) 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.

303 * 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 (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

4.2.174 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 policies³⁰⁵ 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 drafting regulations which may ameliorate the situation. The regulations, which will revise the MISS, are to be published shortly.

4.2.175 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 Act should provide for information security being commensurate with the risk attendant on the compromise of the information.³⁰⁶

4.2.176 The Commission was, however, cautioned that the Privacy Act will not be able to deal with the practical aspects of security issues.³⁰⁷ For instance, identity theft has become a 'hot topic' as far as financial institutions are concerned. This was highlighted in recent reported cases of unauthorised electronic transactions.³⁰⁸

4.2.177 Identity theft happens within a 'paper' environment (over the counter

-
- * 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.
 - * The Department of Arts, Culture, Science and Technology which has been charged with developing the technology foresight study of ICT in South Africa.
 - * Auditor General which has been charged to ensure compliance and certification of these policies and framework.

304 ISM Discussion Document at 2.

305 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.

306 Nedbank.

307 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.

308 The Banking Council.

transactions/applications etc.) and within an electronic environment (internet banking).³⁰⁹ 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.³¹⁰³¹¹

4.2.178 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. 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.³¹²

4.2.179 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)³¹³ that is perpetuated technologically and should therefore be dealt with according to the criminal laws of the

309 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.

310 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."

311 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.

312 SAFPS.

313 *Neethling's Law of Personality* 258.

country.³¹⁴

4.2.180 Reference was furthermore made in one submission to the question whether in the absence of an undertaking or intention, a negligent disclosure of private information³¹⁵ would give rise to liability.³¹⁶ The conclusion was that the general delictual remedies do not apply³¹⁷ and it was argued that the case exists for development of the common law or a constitutional claim for damages action.³¹⁸

4.2.181 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.

4.2.182 The following trends have been noted:³¹⁹

- (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

314 Liberty; LOA.

315 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' By 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 Vecchiato, ITWeb, 25 March 2003, <http://www.itweb.co.za/sections/internet/2003/0303251258.asp?O=FTP> "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.

316 Andrew Rens Wits Law School.

317 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>.

318 Andrew Rens Wits Law School.

319 Smedinghoff T "Trends In The Law of Information Security" **B.N.A. International World Data Protection Report** August 2004.

- (c) a new emphasis on a duty to disclose breaches of information security

4.2.183 Thus, rather than telling companies what specific security measures they must implement, developing law 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 specific risk assessment.³²⁰

4.2.184 Perhaps the most significant legal obligation raised by the recent series of security breaches, however, is the duty to notify persons who may be affected by the breach (eg. persons whose personal information has been disclosed). This approach 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.

4.2.185 Comment is invited on the following clauses:

PRINCIPLE 6 ³²¹

Security safeguards

320 It is significant that the King Commission’s “Code of Corporate Practices and Conduct” specifically addresses the issue of risk management. 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 review 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.”

321 OECD par 11; EU Dir A 17; NL 10, 12, 13 & 14; NZ Principle 5.

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 required in terms of specific industry or professional rules and regulations.*

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).*

Notification of security compromises

Option 1:³²²

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.*

322 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 sec 20 of this Act.

- (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.*

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.

(vii) Principle 7: Individual Participation (Data subject participation and control)

4.2.186 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.³²³ 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.³²⁴

4.2.187 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)

4.2.188 There are furthermore rules which grant persons the right to gain access to personal information relating to them and kept by other persons and organisations. 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 Art 12 of the EU Directive.³²⁵ Principle 7 of the OECD Guidelines³²⁶ also deals with individual participation.

323 See discussion in Roos thesis at 497.

324 Roos 1998 *THRHR* at 504 and references made therein.

325 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

4.2.189 The right in Art 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 Convention³²⁷ and Principle 4 of the UN Guidelines. Only the UN Guidelines, specifically mentions the right to be informed of the recipients of data.

4.2.190 In New Zealand this principle is set out in Principle 6.³²⁸ This right to access is subject to many exemptions, but this is not unusual when one compares it to legislation in other jurisdictions. It

-
- (c) provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; 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.

326 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;

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.

327 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.

328 **PRINCIPLE 6**

remains to be seen whether in practice these exemptions will result in the right of access being unduly curtailed.³²⁹

4.2.191 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.

4.2.192 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.³³⁰

4.2.193 In the Commonwealth Model Law for the public sector the principle manifested in section 15³³¹ and in New Zealand this principle is set out in Principle 7³³²

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.

329 Roos 1998 *THRHR* at 504.

330 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 *Huldigungsbandel WA Joubert* at 124 fn 128).

331 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
(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

4.2.194 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.

4.2.195 In South Africa the right of access to information held by the State and private bodies is specifically provided for in the Constitution.³³³ This includes information that is specifically about someone and, more generally, the information the state uses to make decisions affecting someone.³³⁴

4.2.196 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

(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.

332 **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.

333 Sec 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 the administrative and financial burden on the state.

334 De Waal et al *Bill of Rights Handbook* at 526.

information other than personal information (general information) or to the right to access of personal information of a third person.

4.2.197 The Promotion of Access to Information Act (PAIA) which was enacted to give effect to sec 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 access³³⁵ is necessary for effective and equitable control of information,³³⁶ 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.³³⁷ Of course, there may be exceptions to the right of access to information in particular circumstances.³³⁸

4.2.198 Detailed provision was furthermore made for the correction of information in clauses 51, 52 and 53 of the original Open Democracy Bill, but only section 88 of PAIA survived.³³⁹ 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.³⁴⁰

335 See sec 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).

336 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.

337 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 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 sec 88.

338 *Neethling's Law of Personality* at 279 and the references made therein.

339 **Correction of personal information**

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. (Secs 11 and 50)

340 CDT's Guide.

4.2.199 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.³⁴¹ At this level the right of access to information and the right to privacy is therefore not in conflict.³⁴²

4.2.200 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.³⁴³ 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.

4.2.201 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.

4.2.202 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.

4.2.203 The Freedom of Information Act 2000³⁴⁴ 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.

341 Reference to Eiselen in Roos thesis at 659.

342 This particular section of the privacy legislation can in fact be seen as giving effect to sec 32(2) of the Constitution.

343 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..³ 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.

344 The Freedom of Information Act came into operation on January 1, 2005.

4.2.204 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.³⁴⁵ Such requests automatically become subject access requests under the Data Protection Act and must be treated as such.³⁴⁶ That means that despite the exception under the FOIA, the applicant has a right to his or her information under the Data Protection Act.

4.2.205 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.

4.2.206 Both acts are administered by the Information Commissioner.

4.2.207 It is proposed that a similar provision should be made in South Africa.³⁴⁷ The Commission’s proposal in this regard is that privacy legislation should deal with the access to the personal information of the requester and that PAIA should deal with the right to access to all other information.³⁴⁸ A single authority will furthermore administer both Acts. See discussion in Chapter 5. Should this proposal be accepted, provision will be made in this Act (under a separate chapter entitled “data subject’s rights”) for the procedures to be followed by data subjects to access their own information and PAIA will be amended accordingly.

345 Section 40 of the Freedom of Information Act 2000.

346 Information Commissioner **Freedom of Information Act Awareness Guidance** No 1.

347 Specific comment is invited on this principle as well as on the practical implementation of the principle (proper procedures etc as currently dealt with in PAIA and the PAIA regulations).

348 Amendments to PAIA to be effected by consequential amendments.

4.2.208 Submissions from commentators supported the introduction of the individual participation principles in the privacy legislation.^{349 350} 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 does not take place in response to a request.^{351 352}
- * 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.^{353 354}

4.2.209 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.³⁵⁵

4.2.210 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

349 The Banking Council.

350 ENF for Nedbank.

351 Section 88 'Correction of personal information.
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.

352 Andrew Rens.

353 SAHA.

354 Andrew Rens.

355 SAHA.

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.³⁵⁶

4.2.211 Comment is invited on the following proposed clauses:

PRINCIPLE 7³⁵⁷

Individual participation ³⁵⁸

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.

356 Credit Bureau Association.

357 NZ Principle 6 & 7; Roos 1998 *THRHR* at 503.

358 The Commission's proposal in this regard is that this Act will deal with the access to the personal information of the requester and that the Promotion of Access to Information Act 2 of 2002 will deal with the right of access to all other information. See discussion in Chapter 4 of the Discussion paper, para 4.2.186 and further, especially para 4.2.207. A single authority will furthermore administer both Acts. If this proposal is accepted provision will be made in this act for the procedures to be followed in this regard and PAIA will be amended accordingly.

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.

(viii) Principle 8: Accountability

4.2.212 Principle 8 of the OECD Guidelines reads as follows:³⁵⁹

Accountability Principle

³⁵⁹ CDT's Guide; See discussion in Roos thesis at 519.

A data controller should be accountable for complying with measures which give effect to the principles stated above.

4.2.213 Article 6 (2) of the EU Directive states:

It shall be for the controller to ensure that paragraph 1 is complied with.

4.2.214 The UK Data Protection Act is an example of national legislation in this regard.³⁶⁰

4.2.215 Respondents to the Issue paper were in favour of the principle.³⁶¹ 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.

4.2.216 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”.

4.2.217 However, according to the OECD Guidelines Explanatory Memorandum,³⁶² 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.³⁶³

360 Sec 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.

361 The Banking Council. The OECD guidelines are subscribed to by the Banking Council in this respect; LOA; Credit Bureau Association.

362 OECD Guidelines Explanatory Memorandum at 32.

363 Roos thesis at 519.

4.2.218 For a discussion of remedies, liabilities and sanctions see Chapter 6 below.³⁶⁴

4.2.219 Comment is invited on the following clauses:

PRINCIPLE 8

Accountability³⁶⁵

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.*

4.3 Processing of special personal information (sensitive information)³⁶⁶

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).³⁶⁷ These conditions therefore primarily manifests 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 Art 8(1) of the EU Directive:³⁶⁸ it embraces information on a person’s “racial or ethnic origin”, “political opinions”,

364 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.

365 NL A15 (A 49&50 : sanctions).

366 See discussion on sensitive information in chapter 3 above.

367 Para 3.7.1 at 85 above.

368 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.

“religious or philosophical beliefs”, “trade union membership”³⁶⁹, “health” and “sexual life”. Further, Art 8(5) makes special provision for data on criminal records and the like.³⁷⁰

4.3.3 Similar lists are found in numerous other data protection instruments at both international and national level,³⁷¹ though these vary somewhat in scope. For instance, the list in Art 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).

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.³⁷² Information on credit worthiness or debts is sometimes subject to special restrictions.³⁷³ 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.³⁷⁴

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.³⁷⁵

369 This has caused some problems in EU countries about the publishing of membership lists of such bodies for which consent is now required.

370 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.

371 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 **explicit** consent to processing.

372 The Netherlands.

373 The Netherlands, Portugal, Denmark etc.

374 Korff *Comparative Study* at 85.

375 Korff *Comparative Study* at 85; The Information Commissioner accepted that it was a traditional feature of data protection law, but did not agree.

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.³⁷⁶

4.3.7 Another question that arises is whether information that indirectly reveal certain sensitive matters is covered. Thus the fact that someone regularly buys kosher or hala'l meat or subscribes to certain magazines, or visit 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 sensitive information. The French law expressly stipulates that information which "indirectly" reveal sensitive matters is also subject to the in-principle prohibition.³⁷⁷

4.3.8 Most national laws provide for express consent for the processing of sensitive 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).³⁷⁸ 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 authorisations as envisaged in Art 8(4), but only the UK has in fact issued them.³⁷⁹ A special Order has been issued on the processing of sensitive data.³⁸⁰

376 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.

377 Korff *Comparative Study* at 84.

378 Korff *Comparative Study* at 90.

379 Sec 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.

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

4.3.10 In response to Issue Paper 24 it was submitted that certain medical information may be particularly sensitive. It is for this reason that the LOA has Codes of Conduct relating, amongst others, to medical information. It may be necessary for information to be disclosed to a doctor nominated by the assured, rather than the assured directly.³⁸¹

4.3.11 On the other hand the SAFPS stated that it cannot support Article 8(5) of the EU Directive. 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 detriment of business, consumers and the South African economy.³⁸²

4.3.12 Comment is requested on the following relevant clauses:

Part B

Processing of special personal information³⁸³

Prohibition on processing of special personal information

24. *It is prohibited to process personal information concerning³⁸⁴ 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.*

Exemption to the prohibition on processing of personal information concerning a person's religion or philosophy of life

381 LOA.

382 SAFPS.

383 See NZ Act sections 6-11; Netherlands sections 6 – 24; Commonwealth sections 7-15(16).

384 Sometimes the words “revealing” or “on” are used and the words “directly or indirectly” are included.

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.

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.*

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.

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;*

(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 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;*
- (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).*

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.

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.*

4.4 Exemptions and exceptions

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.³⁸⁵

4.4.3 The difference between exclusions, exemptions and exceptions can be explained as follows:³⁸⁶

- 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 1, 2, 3 and 5 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 excluded completely from the coverage of the law. These have been dealt with in Chapter 2 of the Act dealing with the scope or application of the legislation.

4.4.4 Broadly speaking, the exceptions and exemptions cover two situations: firstly where the risks to the privacy or identity of the data subject are relatively small³⁸⁷ and secondly, where other interests override the data subject's rights to privacy and identity.³⁸⁸ In general, these exceptions and exemptions appear to be justified.³⁸⁹

385 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 2004/06/15 (hereafter referred to as "Stewart **Exemptions and Exceptions**") at 7.

386 Stewart **Exemptions and Exceptions** at 2 and further.

387 Eg. Processing of information for activities exclusively intended for personal or home use.

388 Eg, public interest, interests of other parties or those of the data subject himself or herself.

389 Roos thesis at 522.

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.³⁹⁰

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:³⁹¹

- 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.

- a) Freedom of expression

4.4.8 The laws in different countries in this respect are widely divergent and 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. This divergence may raise problems regarding cross-border journalism.

4.4.9 The EU Directive states as follows in Art 9:

Member States shall provide for exemptions and derogations from the provisions of this Chapter, Chapter IV and Chapter V 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.

4.4.10 It should be noted that the right to freedom of expression is guaranteed in Art 10 ECHR and Art 11 of the Charter of Fundamental Rights to everyone, not just to journalists, artists and writers. It therefore seems as though the journalistic exemption in the Directive should be read broadly so as to

390 See Chapter 3 at 56 and further.

391 Korff *Comparative Study* at 130 and further.

encompass all cases in which the responsible party exercises his right to freedom of expression. Such considerations will be of particular importance to human rights organisations who collect sensitive information for purposes which are not solely “journalistic” in the narrow sense.³⁹²

4.4.11 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.³⁹³

4.4.12 The law in the Netherlands exempts processing for exclusively journalistic, artistic or literary purposes from a limited range of provisions.³⁹⁴ 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.

4.4.13 The UK law also contains a highly qualified exemption for processing for journalistic, artistic and literary purposes.³⁹⁵ Subject to certain complex substantive and procedural conditions, personal

392 Korff *Comparative Study* at 130.

393 Korff *Comparative Study* at 137.

394 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.)

395 **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,

information which are 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” are exempt from the information protection principles and from the exercise of data subject rights. The conditions are difficult to understand, 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.³⁹⁶

b) Freedom of information

4.4.14 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.³⁹⁷

4.4.15 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.³⁹⁸

(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.

(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.

396 Korff *Comparative Study* at 136.

397 Section 32 of the Constitution.

398 Korff *Comparative Study* at 128.

4.4.16 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 7: Individual Participation in Chapter 4 below.³⁹⁹

c) Major public interests

4.4.17 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.⁴⁰⁰

4.4.18 Laws dealing with this category refer to national security, defence, the investigation and prosecution of offences, financial interests of the state, public health, social protection, scientific research and government statistics.

4.4.19 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 further or made subject to additional formal requirements. The exemptions for these kinds of interests often cross-refer to other laws.⁴⁰¹ It is important to remember, though, that such other laws must also be applied in accordance with the Directive.⁴⁰² See the discussion on critical information in Chapter 3 above.⁴⁰³

4.4.20 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 para 3.9 in Chapter 3 dealing with anonymised or de-identified information.⁴⁰⁴

399 At 184.

400 Roos thesis at 523.

401 Douwe Korff *EC Study* at 128.

402 Douwe Korff *EC Study* at 128.

403 At 73.

404 At 88 above.

d) The protection of data subjects and others

4.4.21 Art 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.

4.4.22 Most of the EU member states have adopted a general exception clause on the lines suggested above.⁴⁰⁵ However, they apply different tests in this regard. In the Netherlands the same wording is used as in the Directive,⁴⁰⁶ but the explanatory memorandum to the law stresses that the “necessity” test should be applied strictly and only to avoid “absurd” consequences from the application of the normal rules.⁴⁰⁷ 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.⁴⁰⁸

4.4.23 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.⁴⁰⁹

4.4.24 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

405 Not including Belgium, France, Luxembourg and Portugal.

406 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).....
(e) protecting the data subject or the rights and freedoms of other persons.

407 Korff *Comparative Study* at 146.

408 Sections 27- 39 of the UK Data Protection Act 1998.

409 Roos thesis at 523.

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.⁴¹⁰

4.4.25 In conclusion the Commission's preliminary proposals can be summarised as follows:

- a) Provision is made in Chapter 2 of the proposed Act for the restriction of the scope of the Act. In terms of this chapter, personal information kept in the course of a purely personal or household activity as well as de-identified information are excluded. It is envisaged that certain specified pieces of legislation dealing with the armed forces, the police and the security services may also be excluded from the Act eventually.⁴¹¹ At the moment these government sectors are dealt with, together with private bodies, in the general exemption clause in Chapter 4.
- b) Freedom of information is dealt with in Principle 7 of the Act as well as in the Promotion of Access to Information Act 2 of 2000.
- c) Provision has been made for exceptions found within the principles themselves.
- d) Wide provision is also made for responsible parties⁴¹² 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.
- e) No specific provision has been made for exemptions regarding processing of personal information for journalistic, artistic or literary expression.

Comment is invited on all these aspects.

4.4.26 The Commission therefore proposes that the legislative enactment reads as follows:

410 Roos thesis at 523.

411 See Chapter 3 of the discussion paper and Chapter 2 of the Bill.

412 Including both public and private bodies.

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.

Comment is invited in all instances.

CHAPTER 5: MONITORING AND SUPERVISION

5.1 Introduction

5.1.1 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

5.1.2 It has been argued² 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.

5.1.3 The rules found in information protection laws furthermore usually belong to two main categories:³

- b) rules concerned directly with regulating the processing of personal information (so-called Information Protection Principles)⁴; and
- c) 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.

5.1.4 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.

5.1.5 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).

5.1.6 Four models, embodying the abovementioned rules for privacy protection, were identified in Issue Paper 24:⁶

- c) 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

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* 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.

protection of privacy that are enforced by the industry and overseen by the privacy oversight agency.⁸

d) 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 for 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. 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

e) 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, especially 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

f) Technologies of privacy

With the recent development of commercially available technology-based systems,

⁸ EPIC and Privacy International *Privacy and Human Rights Report* 2002 at 4.

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.

privacy protection has also moved into the hands of individual users. Users of the Internet and of 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 on Data Protection and Privacy Commissioners held in Cardiff on 9-11 Sept 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 make 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 the 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 implemented without also addressing human behaviour and establishing processes within which the technologies would be used, would work.

5.1.7 It was noted in the Issue Paper 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

5.1.8 This fact was confirmed in collating the responses to Issue Paper 24. 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 enforcement 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.

5.2 Enforcement systems

5.2.1 As indicated above, respondents were divided in their comments regarding the system to be chosen. Each option will therefore be discussed in this section (para 5.2) with the comments it elicited in each case discussed in para 5.3 below.

a) Regulatory system (eg. UK, New Zealand, the Netherlands, Canada)

Comprehensive law

5.2.2 A regulatory system makes provision for a comprehensive Act setting out the Principles

¹⁷ Bennett **Government Foundation Paper** 2001 at 28; Bennett CJ "The Data Protection Authority: Regulator, Ombudsman, Regulator or Campaigner?" Presentation delivered at 24th International Conference of Data Protection 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 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.

of Information Protection¹⁹ as well as provisions dealing with the monitoring and enforcement of these principles.

Sectoral laws

5.2.3 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

5.2.4 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

5.2.5 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 - 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.

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 countries in OECD countries with Data Protection Supervisory Authorities: Office of the Federal Privacy Commissioner, Australia; Büro 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 für den Datenschutz, Germany; Hellenic Data Protection Authority, Greece; Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary; Personuvern, Iceland; Data Protection Commissioner, Ireland; Garante per la Protezione dei dati Personali, Italy; Commission à la Protection des Données Nominatives, Luxembourg; College Bescherming Persoonsgegevens, Netherlands; Privacy Commissioner, New Zealand; Datatilsynet, Norway; Bureau of the Inspector General for the Protection of Personal Data, Poland; Comissão Nacional de Protecção de Dados, Portugal; Commissioner for the Protection of Personal Data, Slovak Republic; Agencia de Protección de Datos, Spain; Data Inspection Board, Sweden; Federal Data Protection Commissioner, Switzerland; Information Commissioner, United Kingdom. OECD countries without supervisory authorities are Japan, Korea, Mexico, Turkey and the United States.

5.2.6 The most detailed treatment of the competence and functions of information protection authorities is found in the EU Directive. Art 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

5.2.7 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 2001²⁴ by the CoE Committee of Ministers replicating in Art 1 the basic thrust of Art 28 of the Directive.²⁵

5.2.8 The UN Guidelines specifically address the need to establish national data protection authorities that are “impartial”, “independent” and “technically competent”.²⁶

5.2.9 The Commonwealth guidelines make provision for the establishment of an independent 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

²³ Bygrave **Data Protection** at 71; Art 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.

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

Codes of conduct

5.2.10 Some Commissioners have explicit responsibilities to negotiate privacy codes of

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.

conduct. Some countries' laws make specific provision for industries, professions, etc to draw up sectoral 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

5.2.11 Codes of conduct are primarily instruments of self-regulation and will also be discussed below in para (b) and (c), 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

5.2.12 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 law. Indeed, this is all that is expected by the EU

²⁹ See eg Parts VI-VII of the New Zealand Act; s 51(3)-(4) of the United Kingdom Act; Part IIIA of the Australian Act; and Art 25 of the Netherlands' Act.

³⁰ Bygrave *Data Protection* at 74 referring to Art 27; See discussion on codes of conduct below in para 5.6 below..

³¹ Bennett and Raab *The Governance of Privacy* at 113.

³² See Part VI of the New Zealand Privacy Act.

Directive.³³

5.2.13 Where a formal ratification process is laid out, as in New Zealand and the Netherlands, this can bureaucratised 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

5.2.14 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

5.2.15 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

5.2.16 The EU Directive requires that oversight authorities must act with complete

³³ Bennett and Raab *The Governance of Privacy* at 113.

³⁴ Ibid.

³⁵ Bygrave *Data Protection* at 73.

³⁶ Bygrave *Data Protection* at 74.

independence 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 Art 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

5.2.17 This criterion of independence boils down to the capacity for a 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

5.2.18 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

5.2.19 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 not to a government minister, and is generally regarded as well insulated from direct political interference.⁴³

³⁷ Art 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 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.

⁴³ Bennett and Raab *The Governance of Privacy* at 175 and 176.

5.2.20 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 Art 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

5.2.21 At the 23rd International Conference of Data Protection Commissioners⁴⁶ 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, 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

5.2.22 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

⁴⁴ See Art 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.

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.

⁴⁹ Bygrave *Data Protection* at 75.

⁵⁰ See eg sec 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 Art 19(1) of the EU Directive stipulates the types of information to be notified to include "at least" :

- a) the identity of the data controller and his/her representative;
- b) the purposes of the data processing;
- c) the categories of data subject and data held on the latter;
the categories of recipients of the data;
- d) 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 Act of 1984.

⁵⁴ Bygrave *Data Protection* at 75.

- 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 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

5.2.23 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

⁵⁵ Bygrave *Data Protection* at 76.

⁵⁶ See Art 28(2) and (5) of the EU Directive.

⁵⁷ Lopez JMF "The Data Protection Authority: The Spanish Model" Presentation at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, Sept 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

to access 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 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.

5.2.24 The contemporary role of the Information Protection Authority is therefore that of ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer and international ambassador.⁶²

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.

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 Irish and UK Commissioners have opted for a systemic solution to the problem in that the mechanism for enforcing the provision of their access regime and their data protection regime is one and the same – a Commissioner who regulates both.

⁶² Bennett Conference Paper 2002.

5.2.25 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 out problems.

5.2.26 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 Act⁶³ 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 PIPEDA⁶⁴ are very similar to those under the Privacy Act.

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, n.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/02_04_09_e.asp#000.htm>. The Commissioner's office completed and issued findings and recommendations on 27 complaints.

- 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 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 UK⁶⁷ 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. Para 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;

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 217 and 143.

- 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.

5.2.27 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 pertaining to notification, enforcement, prosecution of offenders and powers of entry and inspection all set out in the relevant sections of the act.

5.2.28 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.

5.2.29 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 (Annual Report 1996 at 32).

Problems

5.2.30 Problems experienced by **agencies** in giving effect to information legislation are as

⁶⁸ Korff *Comparative Study* at 206.

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.⁶⁹
- 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”.⁷⁰

5.2.31 On the other hand, the enactment of comprehensive legislation may have the following negative implications for **responsible parties**:

⁶⁹

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 details 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, 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 Ch 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.

⁷⁰

Korff ***Comparative Study*** at 207.

- a) The informationbase owners may face additional costs in having to comply with whatever legislation is passed;⁷¹
- 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.⁷²

*Sanctions and remedies*⁷³

5.2.32 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.

5.2.33 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 works by persuasion, is enforced by shame and punished by blame.⁷⁴

5.2.34 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.⁷⁵ It also stipulates that decisions

⁷¹ The USA is currently debating the merits of privacy legislation and a major part of the debate concerns the costs to business.

⁷² 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.

⁷³ See discussion in Chapter 6 below.

⁷⁴ Bygrave *Data Protection* at 79 and references therein.

⁷⁵ Art 22.

by a data protection authority which give rise to complaints “may be appealed against through the courts”.⁷⁶

(b) Self-regulatory system (eg USA)

5.2.35 The United States is a good example of the second category of enforcement systems namely the self-regulatory system. 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.⁷⁷

5.2.36 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.⁷⁸

5.2.37 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.⁷⁹

5.2.38 For instance, in the USA, Congress has created specific statutory rights to privacy for oral and electronic communications;⁸⁰ financial, educational and credit information;⁸¹ criminal

⁷⁶ Art 28(3).

⁷⁷ Reidenberg presentation 2001 at 2.

⁷⁸ Ibid.

⁷⁹ US Department of Commerce *Privacy and the NII: Safeguarding Telecommunications-related Personal Information* October 1995 (US Department of Commerce *Privacy Report*) at 11.

⁸⁰ Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510 et seq (1995).

⁸¹ 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).

history,⁸² and even video rental records.⁸³ All of these laws were passed following collaboration among civil liberties-, consumer-, and industry groups.⁸⁴

5.2.39 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.⁸⁵ 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.⁸⁶

5.2.40 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.⁸⁷

5.2.41 Since there are no comprehensive privacy legislation, there is also no oversight agency. As a result, individuals with complaints about privacy must pursue expensive lawsuits, or they may have no recourse at all. Also, foreign governments have nowhere to bring concerns about disparate privacy regulation.⁸⁸

5.2.42 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

⁸² Privacy Act of 1974, 5 U.S.C. 552a (1974); Freedom of Information Act, 5 U.S.C. 552 (1966).

⁸³ The Video Privacy Protection Act 1988, 18 U.S.C. 2710.

⁸⁴ Goldman **Brandeis Lecture** at 2 and references therein to the abovementioned legislation.

⁸⁵ 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 Schwartz PM and Reidenberg JR *A Study of United States Data Protection* Charlottesville, VA Michie 1996.

⁸⁶ Reidenberg presentation 2001at 2.

⁸⁷ Reidenberg presentation 2001at 5.

⁸⁸ Gellman book review supra.

corrected otherwise than by legislative intervention. Industries have therefore been encouraged to self-regulate.⁸⁹

5.2.43 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.⁹⁰

5.2.44 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.⁹¹

5.2.45 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.⁹²

5.2.46 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.⁹³

⁸⁹ Froomkin *Stanford Law Review* 2000 at 1525.

⁹⁰ Hustinx PJ "Co-regulation or self-regulation by public and private bodies - the case of data protection" Published in *Freudendesgabe für Alfred Bullesbach 2002 Umbruch von Regelungssystemen in der Informationsgesellschaft* (hereafter referred to as "Hustinx") at 2.

⁹¹ Bennett *Government Foundation Paper* 2001 at 23; Raab C D "Privacy Protection: The Varieties of Self-regulation" Paper delivered at the International Conference of Data Protection and Privacy Commissioners held in Cardiff on 9-11 Sept 2002 (hereafter referred to as "Raab presentation 2002").

⁹² Froomkin 2000 *Stanford Law Review* at 1525.

⁹³ Hustinx at 2.

5.2.47 In order for institutions to regulate themselves four interrelated policy instruments may play a role⁹⁴ namely privacy statements, privacy codes, privacy standards and privacy seals.

iii) Privacy commitments/ statements

5.2.48 Privacy commitments perform no other function than to indicate to clients, consumers and regulators that the organisation has considered privacy protection at some level, and believed 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.⁹⁵ 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 brief, open and "user friendly" manner.⁹⁶

ii) Codes of conduct

5.2.49 Codes offer a flexibility and can be adapted to the specific economic, technological and regulatory contexts of different sectors. With or without legislation, codes will continue to be significant instruments by which organisational responsibilities are defined, employee obligations are communicated and citizen rights are established.⁹⁷

5.2.50 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

⁹⁴ Raab presentation 2002 at 1.

⁹⁵ Bennett *Government Foundation Paper* 2001 at 17.

⁹⁶ Bennett presentation 2002 at 18.

⁹⁷ 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.

thorough understanding of existing practices, as well as a commitment to improve.⁹⁸

5.2.51 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.

5.2.52 Many codes are developed in the absence of a regulatory framework in order to avoid or anticipate further regulatory intervention.⁹⁹ 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.¹⁰⁰

5.2.53 Five kinds of privacy code can be identified¹⁰¹ according to their scope of application: organisational code¹⁰², the sectoral code,¹⁰³ the functional code¹⁰⁴, the professional code¹⁰⁵ and the technological code¹⁰⁶.

⁹⁸ Bennett Evaluation of Privacy Codes 1997 at 16.

⁹⁹ In contrast to codes that are developed to implement or supplement legislation as is the case within the framework of statutory data regimes.

¹⁰⁰ Bennett Evaluation of Privacy Codes 1997 at 21.

¹⁰¹ Raab presentation 2002 at 9-11. See also Bennett and Raab *The Governance of Privacy* at 123-126.

¹⁰² This applies to one agency that is bound by a clear organisational structure.

¹⁰³ 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.

¹⁰⁴ 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.

¹⁰⁵ Codes developed for those directly involved in information processing activities eg market researchers, and health professionals.

¹⁰⁶ As new potentially intrusive technologies have entered society, codes have developed to deal with their specific application.

iii) Privacy standards

5.2.54 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 for instance and a standard specification for security management systems, which includes a risk analysis for the different categories of information stored by the organisation.¹⁰⁷

5.2.55 The idea of a more general privacy standard¹⁰⁸ that could incorporate the entire range of privacy protection principles was negotiated in Canada.¹⁰⁹ 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.¹¹⁰

5.2.56 The Centre Europeenne 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 to comply with relevant information protection legislation, a series of sector specific initiatives in key areas such as health information and human resource

¹⁰⁷ Bennett presentation 2002 at 22. See in this regard the British Standard, BS7799.

¹⁰⁸ Bennett presentation 2002 at 23.

¹⁰⁹ 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.

¹¹⁰ 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.

management and task specific initiatives mainly related to the online environment.¹¹¹

iv) Privacy seals

5.2.57 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.

5.2.58 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.¹¹²

5.2.59 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.¹¹³

5.2.60 Current seal programmes have not, however, inspired great confidence.¹¹⁴ 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

¹¹¹ Bennett presentation 2002 at 24.

¹¹² Bennett presentation 2002 and references therein.

¹¹³ Bennett presentation 2002 at 25.

¹¹⁴ 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 decided they are better off without the trustmark and the attendant hassle.

which privacy protective practices can be claimed and assured.¹¹⁵

5.2.61 Ideally these four instruments (commitments, codes, standards and seals) should be cumulative. The self-regulatory process should involve:¹¹⁶

- a) an agreement and statement of organisational policy;
- b) a codification of that policy throughout the organisation 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”.

5.2.62 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.¹¹⁷

5.2.63 A more generic problem with self-regulatory schemes is that they regulate only those motivated or principled enough to take part in them.¹¹⁸

5.2.64 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.¹¹⁹ 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.

¹¹⁵ Bennett presentation 2002 at 26.

¹¹⁶ Bennett presentation 2002 at 26.

¹¹⁷ Bennett presentation 2002 at 26.

¹¹⁸ Froomkin 2000 *Stanford Law Review* at 1528.

¹¹⁹ National Telecommunications and Information Administration, Department of Commerce USA *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.

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.

5.2.65 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, 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.

c) Co-regulatory system (eg Australia)

5.2.66 The third system identified is the co-regulatory system. This concept refers to self-regulation by an industrial association with governmental oversight and ratification.¹²⁰ 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

¹²⁰

Bennett and Raab *The Governance of Privacy* at 184 notes that a distinction should be made between co-regulation and enforced self-regulation.

rights, obligations and enforceable bottom line of legislative guarantees.¹²¹

5.2.67 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.

5.2.68 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.

5.2.69 In this co-regulatory system industry codes play a far more central role than in other countries.¹²² It can be seen as a form of voluntary regulation within the confines of broader legislative provisions.

5.2.70 In Australia an organisation or industry registering a Privacy Code under the Australian Privacy Act, must prove and be legally accountable for the Code providing at least the same level of protection that the ten National Privacy Principles of the Australian Privacy Act require – preferably more.¹²³ Where a code is not established, the Privacy Principles set out in the Act automatically apply.

5.2.71 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

¹²¹ 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.

¹²² Bennett and Raab *The Governance of Privacy* at 129.

¹²³ 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 transfer once local ratification is complete.

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.¹²⁴

5.2.72 Caution should be exercised where a code of conduct exists in that the code should not create a lesser standard than those 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.¹²⁵ The cost of compliance with these standards may, furthermore, out-weigh the cost of compliance with formal legislation.¹²⁶

5.2.73 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.

5.3 Submissions received: Evaluation of options identified

5.3.1 In their submissions, the following specific comments were made by respondents regarding the systems identified above:

a) Regulatory system

(i) Comprehensive law¹²⁷

5.3.2 Respondents in favour of the regulatory approach stated that a new privacy law is now urgently required.¹²⁸ 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

¹²⁴ See for example Part IIIA of the Australian Privacy Act 1988 as amended.

¹²⁵ Senate Committee at 6.

¹²⁶ Bennett and Raab *The Governance of Privacy* at 129.

¹²⁷ USA Department of Commerce only the respondent not in favour of a comprehensive law. See discussion on self-regulation in Para 5.3.43 below.

¹²⁸ Financial Services Board; ENF for Nedbank.

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.¹²⁹

5.3.3 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.¹³⁰

5.3.4 It was argued that consolidated national information protection legislation will:

- * Provide a consistent approach to privacy and information protection across all sectors of the economy based on the founding principles¹³¹ listed in Chapter 4.
¹³²
- * Go a long way in providing guidance and clarity in the regulatory and legislative environments pertaining to privacy and information protection.¹³³ 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.¹³⁴
- * Create an overall stable and investment-friendly regulatory and legislative framework, benefitting the South African economy and its people.¹³⁵

¹²⁹ ENF for Nedbank.

¹³⁰ Nedbank; See discussion in Ch 7 below regarding the adequacy requirement.

¹³¹ Fair and lawful processing, Openness; Collection limitation; Use/Purpose specification; Disclosure limitation; individual participation; Data quality; Finality; Security safeguards; Accountability and Sensitivity.

¹³² Vodacom.

¹³³ Vodacom.

¹³⁴ Financial Services Board, Banking Council.

¹³⁵ Vodacom.

- * 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).¹³⁶
- * Ensure that South African organisations are able to compete in the international information-technology based services market through cross-border transactions.¹³⁷

5.3.5 The objectives of a information protection system should essentially be:¹³⁸

- * 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 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.

(ii) Regulatory agency for South Africa?

5.3.6 An important question in the privacy debate in South Africa is whether an Information

¹³⁶ 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.

¹³⁷ ENF for Nedbank.

¹³⁸ ENF for Nedbank.

Privacy Act should make provision for an information protection agency. In parallel 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),¹³⁹ the following interesting viewpoints were held:

- (a) The **Human Rights Commission (HRC)**¹⁴⁰ 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.¹⁴¹ 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 implications of clogging up the court system even further.¹⁴²

¹³⁹ 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.

¹⁴⁰ Submission to the Open Democracy Bill.

¹⁴¹ PAIA eventually made provision for Magistrates' Courts and magistrates to be specifically designated by the Minister of Justice in terms of sec 1 and 91A of the Act as a forum for relief. To date, this has not happened yet.

¹⁴² 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 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.

- (b) The **Open Democracy Lobby Group**¹⁴³ 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.¹⁴⁴

5.3.7 One of the South African Law Reform Commission's preliminary proposals set out in its Issue Paper¹⁴⁵ 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.

5.3.8 The Commission received a mixed reaction from respondents. Many of the comments received were in favour of a statutory agency,¹⁴⁶ but some differed as to the powers to be

¹⁴³ 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).

¹⁴⁴ 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 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.

¹⁴⁵ SALRC Issue Paper 24.

¹⁴⁶ Eg MFSA; SAHA; ENF for Nedbank; ISPA; IMS.

afforded to such an institution.¹⁴⁷ Some respondents expressed their opposition to the creation of an oversight agency.¹⁴⁸

Respondents in favour of the creation of an agency argued as follows:

5.3.9 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. 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.¹⁴⁹

5.3.10 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.¹⁵⁰ 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.¹⁵¹

¹⁴⁷ SAFPS; FSB.

¹⁴⁸ Eg. Vodacom; SABC; LOA.

¹⁴⁹ ENF for Nedbank.

¹⁵⁰ IMS.

¹⁵¹ SAHA.

5.3.11 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 the benefits of e-commerce, economic and telecommunication infrastructure growth, privacy-enhancing technologies and control over their personal information in this progressive environment.¹⁵²

5.3.12 It should, however, 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 with the maximum respect for the right as a whole.¹⁵³

152 IMS.

153 ISPA.

5.3.13 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 the PAIA.¹⁵⁴ There is not currently sufficient championing of the right to access to information at higher levels of government.¹⁵⁵ 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/gatherer violating such codes.¹⁵⁶ 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.¹⁵⁷

5.3.14 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.¹⁵⁸ A separate regulatory authority to oversee compliance within South Africa should have sufficient ability to ensure effective enforcement of contraventions of such legislation.

5.3.15 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.¹⁵⁹

¹⁵⁴ ISPA.

¹⁵⁵ SAHA.

¹⁵⁶ 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 and they believe that similar provisions should bind other entities.

¹⁵⁷ IMS.

¹⁵⁸ Nedbank.

¹⁵⁹ SAHA.

5.3.16 Even in Canada it has been suggested the Federal Information Commissioner should be better resourced and given the power to make binding orders.¹⁶⁰ 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.¹⁶¹

5.3.17 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.¹⁶²

5.3.18 In addition, 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.¹⁶³

5.3.19 Furthermore, the reliance on outdated court processes to ensure compliance with these protections undermines their benefits.¹⁶⁴ 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.¹⁶⁵

¹⁶⁰ See Roberts A "New Strategies for Enforcement of the Access to Information Act" (2002) 27 *Queens Law Journal* 647-682.

¹⁶¹ SAHA.

¹⁶² Nedbank.

¹⁶³ ISPA.

¹⁶⁴ Internet Service Providers Association.

¹⁶⁵ SAHA.

5.3.20 In a submission to the Commission received from the Human Rights Commission¹⁶⁶ 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 Unit shares the COSATU position on this issue. It is furthermore necessary, when looking into the 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.

5.3.21 In April 2003, SAHA 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.¹⁶⁷

5.3.22 In this regard, an adequately resourced oversight body/person is important to ensure that individuals and companies can have recourse to the law without the need for an expensive process.¹⁶⁸

5.3.23 With regard to the anticipated costs of implementation of the requirements of a 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 is allowed for local businesses to convert existing data and databases and to implement processes and procedures in order to comply with the legislative requirements.¹⁶⁹ The Law 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 is wholly supported as well as the development of legislation to facilitate the development of that culture, one would wish to avoid a "double

¹⁶⁶ PAIA Unit South African Human Rights Commission "Comments on the DATA Protection Document" 1 June 2004.

¹⁶⁷ SAHA.

¹⁶⁸ ISPA.

¹⁶⁹ Nedbank.

taxation” for members who have to absorb the costs of enabling surveillance and at the same time protect privacy.¹⁷⁰

5.3.24 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.¹⁷¹ It is imperative that an oversight authority should have adequate funding (now and in the future) as well as resources to adequately conduct oversight and enforcement.¹⁷² Whether the entity is a single person, or has regional officers/offices, government has to be lobbied to ensure that this ‘regulator’ is adequately resourced to carry out its mandate.¹⁷³

5.3.25 Moreover, such a body must be independent, that is, able to criticise any privacy invasive proposals.¹⁷⁴ This also requires sufficient insulation and protection from other arms of government. It was even suggested that such a person/office be afforded Chapter 9 protection as envisaged by the Constitution. Finally, this office should be coordinated and streamlined with other sector regulators to ensure effective regulation of the sector.¹⁷⁵

5.3.26 The question as to where a statutory authority should be situated produced different views:

- * Some respondents 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 Human Rights Commission¹⁷⁶ or the Department of

¹⁷⁰ 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.

¹⁷¹ SAHA.

¹⁷² EPIC and Privacy International *Privacy and Human Rights* 2002 at 13 and 14; MFSA.

¹⁷³ The Internet Service Providers’ Association.

¹⁷⁴ EPIC and privacy International *Privacy and Human Rights* 2002 at 13 and 14; MFSA.

¹⁷⁵ The Internet Service Providers’ Association.

¹⁷⁶ Society of Advocates, KwaZulu Natal; 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).

Communication.¹⁷⁷

- * Others specifically indicated that they did not support the view that the authority should reside within or be related to the existing Human Rights Commission.¹⁷⁸
- * The Public Protector was furthermore not deemed to be the appropriate body to perform the function of dispute-resolution under PAIA and privacy legislation for the following reasons:¹⁷⁹
 - 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.

5.3.27 Another related question was whether the rights to access to information and privacy should be dealt with by separate agencies or whether one agency for both would be possible. 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 to access to information.¹⁸⁰

5.3.28 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 may be better to have one officer combine both roles in South Africa. 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.¹⁸¹

¹⁷⁷ ENF for Nedbank; See also the discussion on sector-specific regulators below.

¹⁷⁸ Eg The Banking Council.

¹⁷⁹ SAHA.

¹⁸⁰ SAHA.

¹⁸¹ National Archives.

5.3.29 It was argued that there seems no reason why an oversight body should not be given authority to investigate complaints in terms of both the Promotion of Access to Information Act 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 of ensuring compliance. It is worth noting that since the enactment of the 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.¹⁸²

5.3.30 In its report to the Human Rights Commission on its role with respect to PAIA, SAHA argued that sec 8 of the Human Rights Act 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 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, it was recommended as follows:¹⁸³

- * 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.¹⁸⁴

182 SAFPS.

183 SAHA.

184 SAHA also argued that the Human Rights Commission is currently inadequately resourced to perform this role, even before considering its role regarding dispute-resolution. The need for adequate resourcing should therefore also be considered with respect to promotional and related functions under privacy legislation.

5.3.31 In conclusion the following recommendations were made:¹⁸⁵

- * That a statutory regulatory authority be responsible for privacy and information protection and that such an authority be:
 - responsible for access to information as well as privacy and information protection;
 - either the Human Rights Commission or a new independent Information and Privacy Commissioner;
 - responsible for both promotion, publicity, education, advice, assistance, monitoring, and reporting to Parliament and for enforcement of rights and dispute-resolution;
 - specifically empowered to resolve disputes under provisions of both PAIA and privacy legislation - this would involve amendments to PAIA;
 - accessible as a dispute-resolution mechanism intermediate between internal appeal against decisions of public or private bodies and recourse to the courts; and
 - empowered to make binding orders to resolve disputes.
- . That *consideration* be given to assigning particular commissioners to issuing 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
- . That the following steps in the dispute-resolution process under privacy legislation and PAIA 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.

Respondents who were against the creation of a new independent oversight agency submitted the following arguments:

5.3.32 The idea was supported that self-regulation should be developed by sector players,

¹⁸⁵

SAHA.

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.¹⁸⁶

5.3.33 It was furthermore argued that where recommendations are made for the establishment 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.¹⁸⁷ 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.¹⁸⁸

5.3.34 Furthermore, the legislation will need to indicate clearly how co-operation with sector-specific regulatory authorities will occur, especially in dealing with customer complaints.¹⁸⁹

5.3.35 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.¹⁹⁰ If this second approach is followed, it is important that sector authorities are sufficiently funded, skilled and resourced to

¹⁸⁶ Vodacom.

¹⁸⁷ 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.

¹⁸⁸ Vodacom. In analogy, the current concurrent jurisdiction of ICASA and the Competition Commission can be considered.

¹⁸⁹ Vodacom.

¹⁹⁰ See also the discussion above in para 5.3.27.

perform this additional role.¹⁹¹

5.3.36 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 is a need for specific privacy laws which apply specifically to state owned entities.¹⁹² The existing regulatory bodies, which oversee the various industries, have adequate systems and insight to properly ensure compliance and makes the need for an independent regulatory agency or authority unnecessary.¹⁹³

5.3.37 An example provided of a sector with an existing regulatory body is the long-term insurance industry. The FSB 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.¹⁹⁴ It has insight into the industry and already has systems in place and is actively involved in monitoring compliance, which would minimise costs.¹⁹⁵ 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.¹⁹⁶ 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 one will quickly see that there is no room for a statutory regulatory agent. Moreover, one must also consider that such an

¹⁹¹ Vodacom.

¹⁹² SABC.

¹⁹³ LOA submission.

¹⁹⁴ LOA.

¹⁹⁵ LOA.

¹⁹⁶ LOA.

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.¹⁹⁷

5.3.38 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 the 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.¹⁹⁸

5.3.39 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.¹⁹⁹

There were 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:

5.3.40 The appointment of an information commissioner should be avoided, but an ombudsperson with legislative power should be considered.²⁰⁰ The ombudsperson would be responsible for responding to complaints from consumers and other aggrieved persons who believe that their right of privacy have been infringed. 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

¹⁹⁷ LOA.

¹⁹⁸ Liberty.

¹⁹⁹ SAPS.

²⁰⁰ 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.

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.²⁰¹

5.3.41 The appointment of a Commissioner to act as a policeman in ensuring compliance with information privacy legislation is, however, not supported. Any proposed legislation should, if 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 is 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.²⁰²

5.3.42 An oversight body is, however, 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.²⁰³

(b) Self-regulatory system

5.3.43 One submission was received in which self-regulation (only sectoral legislation/codes of conduct and then only when and if necessary, no oversight agency) as a way of privacy protection 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:²⁰⁴

- * 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

²⁰¹ SAFPS.

²⁰² SAFPS.

²⁰³ MFSA.

²⁰⁴ United States Department of Commerce.

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.

- * 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.²⁰⁵

* 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;²⁰⁶
- b) Privacy Policy Generator Tools;²⁰⁷

205

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.

206

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.

207

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 Online Marketing.

- c) Privacy “Seal” Programs/Verification Services;²⁰⁸
- d) Alternative Dispute Resolution Providers;²⁰⁹ and
- e) Privacy Protection Training/Awareness.²¹⁰

208

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. BBBOnLine's mission is to promote trust and confidence on the Internet through the BBBOnLine Reliability and Privacy Seal Programs. BBBOnLine'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 BBBOnLine 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.cpawebtrust.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/isp/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.

209

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 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.

210

GetNetWise (<http://www.getnetwise.org>)

5.3.44 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. Possible costs to be noted resulting from implementing privacy legislation, which may be highly resource intensive for government and private sector.

5.3.45 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.

5.3.46 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.

5.3.47 Another respondent, however, raised a cautionary note²¹¹ in indicating that the absence of a contractual remedy in the South African law for damages to personality interests²¹² 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

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.

211 Andrew Rens.

212 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.

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.²¹³

(c) Co-regulatory system

5.3.48 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.²¹⁴

5.3.49 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 should, furthermore, be taken of voluntary ombud which exist outside legislation but could be an important part of any framework.²¹⁵

5.3.50 One respondent²¹⁶ 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

²¹³ Andrew Rens.

²¹⁴ Credit Bureau Association.

²¹⁵ Credit Bureau Association.

²¹⁶ SABC.

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.²¹⁷

5.3.51 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.²¹⁸

5.3.52 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.²¹⁹
- * 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.²²⁰

²¹⁷ SABC.

²¹⁸ 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.

²¹⁹ 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.

²²⁰ LOA.

- * 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.²²¹
- * 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).²²²

5.3.53 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.²²³

5.3.54 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 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.²²⁴ Many of the principles espoused in the Issue Paper are already present in the LOA Code.²²⁵

221 Michalsons for IMS.

222 Michalsons for IMS.

223 Sanlam Life: Law Service.

224 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.”

225 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.

5.4 The proposed information protection system for South Africa

5.4.1 In comparing different information protection laws, cross-national regulatory trends²²⁶ can be identified.²²⁷ 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.

5.4.2 A highly efficient information protection system would therefore comprise:²²⁸

- * 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-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;

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."

²²⁶ 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.

²²⁷ Bygrave *Data Protection* at 88.

²²⁸ Bennett and Raab *The Governance of Privacy* at 207.

- * 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; all are necessary conditions for high quality information protection. None is a sufficient condition.

5.4.3 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/ instruments need to be channelled in the same direction so that the rules support each other rather than frustrate each other.²²⁹ PET's (privacy enhancing tools) is furthermore to be regarded as a useful complement to existing regulatory and self-regulatory approaches.²³⁰

5.4.4 In evaluating the different systems discussed above, the following points should be noted:

- * The Commission does not regard the self-regulatory system to be a suitable system for South Africa. 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, resulting in a confusing patchwork of provisions that reveals large gaps resulting in information protection that becomes "fragmented, incomplete, and discontinuous".²³¹ Under these circumstances, individuals' rights are difficult and costly to pursue.²³²
- * Over time it has also become clear that the existence of vigorous supervisory authorities are a sine qua non of good privacy protection inasmuch as laws are not self-implementing and the culture of privacy cannot securely establish itself

229 Reidenberg presentation 2001at 3.

230 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, sec 18 of the proposed Act which refers to technical and organisational measures to be implemented by the responsible parties to secure information.

231 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.

232 Bennett and Raab *The Governance of Privacy* at 105.

without an authoritative champion.²³³

- * The regulatory and co-regulatory system both make provision for a comprehensive act and a supervisory authority. The interaction between a supervisory authority, industry specific regulators and self-regulating adjudicators should be established clearly. It should, however, be noted that in co-regulating systems many sectors (especially small to medium industries) do not necessarily have adjudicators or regulators. Even if the co-regulatory system is adopted in a country, provision will therefore still have to be made for those industries without sector-specific adjudicators through a general supervisory authority.²³⁴ 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.
- * It is envisaged that a single statutory regulatory authority will administer both the information privacy legislation and the access to information legislation.

5.4.5 The Commission's preliminary proposal is therefore that a comprehensive act should be instituted with or without sectoral legislation and codes of conduct, to be implemented within a regulatory system, implemented by a statutory regulatory authority working in conjunction with individual sectors.

5.4.6 The Commission therefore proposes that the information protection enforcement system be set out as follows:

²³³ Bennett and Raab *The Governance of Privacy* at 107.

²³⁴ 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.

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 (Proclamation 103 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 Commission²³⁵

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*

²³⁵

The current proposal of the Law Commission is that the Information Commission will be responsible for the supervision of both the Promotion of Access to Information Act and the Protection of Personal Information Act. See Chapter 5 and para 4.2.207 in Chapter 4 of the discussion paper. Should this proposal be approved, the powers and duties of the Commission will be extended and PAIA amended accordingly.

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;*²³⁶

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*

²³⁶

This section will only apply if the Act provides for the appointment of self-regulating adjudicators.

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 sec 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

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 Officer²³⁷

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*

²³⁷

See sec 1 of PAIA for the definition of "information officer" and sec 17 regarding the designation of deputy information officers. It is envisaged that one officer should be designated in an organisation to deal with both privacy and information matters. It should be noted that PAIA does not currently make provision for the appointment of officers in private bodies. Comment is invited.

them has registered them with the Commission.

Comment is invited.

5.5 Notification, registration and licensing schemes

a) Introduction

5.5.1 A primary condition for effective information protection is that of transparency.²³⁸ Worldwide, responsible parties are enjoined to be open about their processing activities.²³⁹ This obligation may include the requirement to inform (and to receive authorisation from) the supervisory authority of their processing activities.²⁴⁰

5.5.2 We have seen above that there are three main categories to the rules monitoring the activities of responsible parties.²⁴¹ In some countries mere notification is necessary before processing may start. Others require registration and a third group insists on licensing as a precondition. A further requirement may be for the oversight authority to keep a register of the processing activities of which it has been informed.

5.5.3 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.²⁴²

5.5.4 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

²³⁸ See Principle 5: Openness as discussed in Chapter 4 para 4.2.125 above as well as the proposed clause 17(1).

²³⁹ See in this regard Principle 6 of the OECD Guidelines set out in fn 227 in Chapter 4 above; See also Principle 3 of the UN Guidelines.

²⁴⁰ Bennett and Raab *The Governance of Privacy* at 99.

²⁴¹ Para 5.2.22.

²⁴² Bygrave *Data Protection* at 75.

authority with basic details of its intended processing operations.²⁴³

5.5.5 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.²⁴⁴

5.5.6 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).²⁴⁵ In countries with new legislation, lighter notification responsibilities have been established from the start. Registration has never been seriously considered in information protection regimes in North America or Australasia.²⁴⁶

5.5.7 Compliance with notification everywhere also remains very low indeed.²⁴⁷ 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.

5.5.8 Many of the authorities would prefer to spend their resources on other measures which could contribute more effectively to compliance by responsible parties.²⁴⁸ It was argued²⁴⁹ that

²⁴³ Bygrave *Data Protection* at 75.

²⁴⁴ 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).

²⁴⁵ 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.

²⁴⁶ Bennett and Raab *The Governance of Privacy* at 99.

²⁴⁷ 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.

²⁴⁸ Korff *Comparative Study* at 170.

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 contained²⁵⁰ and that the supervisory authority should concentrate its activities both on giving advice and spreading awareness about information protection and supervising compliance.²⁵¹

5.5.9 It would therefore seem as though 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.

5.5.10 Notification appears to serve three main purposes.²⁵²

- * 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 of processing operations (or of notifications);
- * it is helpful for responsible parties as it helps 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.²⁵³

5.5.11 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

249 EU 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.

250 Roos thesies 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’”.

251 See discussion below.

252 **WP 106 on Notification** at 6.

253 Register provides information for educational purposes.

Directive).²⁵⁴

b) Processing operations which must be notified

5.5.12 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.^{255 256}

5.5.13 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 (Art 18(1)).²⁵⁷ Some countries extend 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.²⁵⁸

5.5.14 It should be noted that even where processing is not required to be notified, 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 though not formally notified.

5.5.15 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

²⁵⁴ See discussion below.

²⁵⁵ Whereas some relied heavily on notification and the keeping of registers, others sought to minimise these obligations or did have alternative systems in place.

²⁵⁶ **WP 106 on Notification** at 4.

²⁵⁷ Art 18 (1) 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.

²⁵⁸ Korff **Comparative Study** at 168.

register.²⁵⁹

5.5.16 The legal framework for the exemptions to the duty of notification is mainly provided for in paragraphs 2 to 5 of Article 18²⁶⁰ of the Directive. There is no Member State where at least some partial exemptions from notification obligations have not been implemented.²⁶¹

5.5.17 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.²⁶²

5.5.18 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.²⁶³

²⁵⁹ Bainbridge *Data Protection* at 69.

²⁶⁰ Art 18(2) -(5) 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.

²⁶¹ 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.

²⁶² **WP 106 on Notification** at 8; see, however, the discussion on exemptions in Chapter 4 above.

²⁶³ 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.

5.5.19 The Art 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 report²⁶⁴ it confirmed the importance of having notification as a general requirement but identified best practices as regards the duty of notification to be followed.²⁶⁵

5.5.20 As a general rule failure to notify is regarded as a criminal offence of strict liability.²⁶⁶

c) Notifiable particulars and publication of particulars

5.5.21 With some exceptions the types of information to be notified 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(Art 19).²⁶⁷

²⁶⁴ **WP 106 on Notification.**

²⁶⁵ **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.

²⁶⁶ Bainbridge **Data Protection** at 67 for UK example.

²⁶⁷ 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.

5.5.22 To the extent that they require notification, the states list (at least) all the matters mentioned in Art. 19(1)(a) – (f) of the Directive, quoted above; and they all of course also stipulate that if such aspects of a processing operation change, the change too must be reported. However, they differ considerably in their specification of additional notifiable particulars.²⁶⁸

5.5.23 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 contents of these registers will vary because of the differences in the notifiable particulars.²⁶⁹

5.5.24 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.²⁷⁰ 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 agency's web site.²⁷¹

d) Prior checking

5.5.25 “Prior checks” or requirements that responsible parties obtain the “prior authorisation” of

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 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 of a legitimate interest.

²⁶⁸ Korff *Comparative Study* at 173.

²⁶⁹ Ibid.

²⁷⁰ Roos thesis at 725.

²⁷¹ Bainbridge *Data Protection* at 74 for UK example.

their national information protection authority, are the strictest form of control over processing operations.

5.5.26 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 (Art 20(1)).²⁷²

5.5.27 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”.²⁷³

5.5.28 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”.

5.5.29 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.²⁷⁴ However, no processing have to date been made subject to a “prior check” in the UK (even though the 1998 law does provide for the possibility).²⁷⁵

5.5.30 There are substantial differences between the EU member states as concerns the kinds of operations for which they stipulate such prior formalities. Examples are the processing of

²⁷²

Art 20(1) 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.

²⁷³

WP 106 on Notification at 3.

²⁷⁴

Bainbridge **Data Protection** at 78.

²⁷⁵

Korff **Comparative Study** at 173.

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.²⁷⁶

5.5.31 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 informed of this; and for the processing of information on criminal-legal matters etc., other than by licenced detective agencies.²⁷⁷

5.5.32 It would appear from Art 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”.²⁷⁸

5.5.33 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 exception do not conform with the Directive.²⁷⁹

5.5.34 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

²⁷⁶ Korff *Comparative Study* at 174.

²⁷⁷ Ibid.

²⁷⁸ *WP 106 on Notification* at 3.

²⁷⁹ *WP 106 on Notification* at 4.

responsible parties.²⁸⁰

e) In-house officials

5.5.35 Article 18 (2) of the Directive²⁸¹ allows Member States to exempt responsible parties from notification duties where “the responsible party, in compliance with the national law which governs him, 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;
- * For keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2) (...).²⁸²

5.5.36 The main task of the in-house official is to ensure compliance with the Law 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 (e.g., 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

²⁸⁰ Korff *Comparative Study* at 175.

²⁸¹ Art 18(2) 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.

²⁸² This alternative to notification provided by the Directive is currently implemented in Germany, the Netherlands, Sweden, Luxembourg and France.

cases of doubt” contact the relevant supervisory authority. However (except in the special context of a “prior check”), this is not obligatory.²⁸³

5.5.37 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 an own database and/ or intranet of the organisation.²⁸⁴

5.5.38 It is the Commission’s preliminary recommendation that a system of light notification (subject to exemptions) and prior investigation be implemented. However, since the Information officer contemplated in Chapter 5 above is appointed by the responsible party and not by the Commission and is not subject to independence requirements, an exemption in this regard has been excluded. It will be an offence to process personal information without notification unless the processing is exempt from notification and liability will be strict. Comment is invited on all of these proposals. The proposed legislative enactment will read as follows:

²⁸³ Korff *Comparative Study* at 176.

²⁸⁴ 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.

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 47.²⁸⁵

(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(1)(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

²⁸⁵

It is envisaged that the exemptions granted to certain categories of bodies from the provisions set out in Chapter 2 (publication and availability of certain records) of PAIA will also be applicable in so far as the notification requirements in terms of this Act are concerned.

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;²⁸⁶*
- (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.*

- (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.*

²⁸⁶

Exemptions.

(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 sec 83 of this Act.*

5.6 Codes of conduct

5.6.1 As noted above, codes of conduct are found in all the privacy systems discussed above.²⁸⁷ Since the Commission has, however, already indicated its preference for a regulatory system, the discussion in this section will be restricted to codes of conduct as found within this system. Five kinds of privacy code can be identified²⁸⁸ according to the scope of application: organisational code²⁸⁹, the sectoral code,²⁹⁰ the functional code²⁹¹, the professional code²⁹² and the technological code²⁹³.

²⁸⁷ See para 5.2.10-5.2.13 (regulatory system), paras 5.2.49 - 5.2.53 (self-regulatory system) and para 5.2.69-5.2.73 (co-regulatory system). 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 IIIA of the Australian Privacy Act, 1988 and Article 25 of the Dutch Personal Data Protection Act.

²⁸⁸ Raab presentation 2002 at 9-11. See also Bennett and Raab *The Governance of Privacy* at 123-126.

²⁸⁹ This applies to one agency that is bound by a clear organisational structure.

²⁹⁰ 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.

²⁹¹ 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.

²⁹² Codes developed for those directly involved in information processing activities eg market researchers, and health professionals.

²⁹³ As new potentially intrusive technologies have entered society, codes have developed to deal with their specific application.

5.6.2 The EU Directive clearly provides for the use of codes of conduct.²⁹⁴ To contribute to the proper implementation of the Directive at the national level, Article 27 of the Directive²⁹⁵ 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 furthermore 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.²⁹⁶

5.6.3 The OECD Guidelines, furthermore, provide that member countries should encourage and support self-regulation, whether in the form of codes of conduct, or otherwise.²⁹⁷

5.6.4 Codes of conduct are, therefore, seen as a useful means to clarify the application of information protection law in a particular sector, and can also be used as an alternative to sectoral regulation.²⁹⁸ 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.²⁹⁹ It furthermore has the advantage that, once negotiated, the codes

²⁹⁴ The Directive does not, however, provide any indication of the exact legal status to be provided to such codes.

²⁹⁵ 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.

²⁹⁶ 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 (hereafter referred to as Wugmeister et al *Codes of Conduct*).

²⁹⁷ 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.

²⁹⁸ 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.

²⁹⁹ Korff *Comparative Study* at 196.

can be adapted to changing economic and technological developments.³⁰⁰

5.6.5 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.³⁰¹

5.6.6 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, credit information). The Information Commissioner may also initiate codes of practice.³⁰²

5.6.7 While it is preferable for codes to emanate from the representative associations themselves, the Commission 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.³⁰³

5.6.8 The Commission 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 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 (e.g. 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.³⁰⁴

5.6.9 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,

³⁰⁰ Bennett and Raab *The Governance of Privacy* at 113.

³⁰¹ Office of the New Zealand Privacy Commissioner **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.

³⁰² NZ *Codes of Practice Guidance note* at 2.

³⁰³ Korff *Comparative Study* at 197 with reference to the Irish Commissioner in his 2001 Annual Report.

³⁰⁴ Ibid.

or indeed requires, the assessment and/or approval of “voluntary” codes, while State regulation may involve the drawing up of rules in consultation with (or even by) sectoral organisations.³⁰⁵

5.6.10 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.³⁰⁶ 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.”³⁰⁷

5.6.11 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 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.³⁰⁸

³⁰⁵ Korff *Comparative Study* at 196.

³⁰⁶ 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.

³⁰⁷ 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.

³⁰⁸ 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

- 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.³⁰⁹

5.6.12 In Europe the stipulations in the Directive confirm a trend towards what one may call *quasiself-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 compatibility 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.³¹⁰

5.6.13 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 approval of Community Codes).³¹¹

5.6.14 It has been argued that where a formal ratification process is laid out, as in New Zealand and the Netherlands, this can bureaucratise 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”.³¹²

processing of personal data. These codes are used to promote compliance with sector specific data protection requirements.

309 Bennett and Raab *The Governance of Privacy* at 113.

310 Ibid.

311 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.

312 Bennett and Raab *The Governance of Privacy* at 113.

5.6.15 The following guidance have been given on the matters that should be addressed in particular in acceptable codes of conduct.³¹³

- * 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.

5.6.16 A code of conduct will furthermore include provisions for:³¹⁴

- * 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.

5.6.17 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).³¹⁵

5.6.18 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 complaint handling body adding substantially to the resource requirements.³¹⁶

³¹³ Korff *Comparative Study* at 198.

³¹⁴ NZ *Codes of Practice Guidance Note* at 4.

³¹⁵ Korff *Comparative Study* at 198.

³¹⁶ Office of the Federal Privacy Commissioner Australia *Guidelines on Privacy Code Development* September 2001 (hereafter referred to as "Australian *Privacy Code Guidelines*") at 20.

5.6.19 An exciting new development to be noted³¹⁷ is that a code of conduct approach is developing to cross-border information transfers.³¹⁸ 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.³¹⁹

5.6.20 It is the Commission's preliminary recommendation 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. 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. Comment is invited. The legislative enactment of this provision will read as follows:

³¹⁷ Especially in so far as South Africa's trade with the rest of Africa is concerned.

³¹⁸ Wugmeister *Codes of Conduct* et al at 1.

³¹⁹ See further discussion on cross-border data transfers at Chapter 7 below.

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 the 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.*
- (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.*

5.7 Information matching (profiling)

5.7.1 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.

5.7.2 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. 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.³²⁰

5.7.3 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 the subject on account of this accumulated information, which may, or may not, be correct.³²¹

5.7.4 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.³²²

5.7.5 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.³²³

5.7.6 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.³²⁴

5.7.7 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

³²⁰ Andrew Rens.

³²¹ Tilley at 3.

³²² Bygrave Data Protection 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.

³²³ Bygrave **Computer Law and Security Report** 2001 at 2.

³²⁴ Bygrave **Computer Law and Security Report** 2001 at 2.

any identifiable individual from such profiling.³²⁵ Profiling is a valuable marketing tool and freely allowed as long as it is not making individualised personal information available. This view was also confirmed in the response to a question posed in the Issue Paper 24 as to the acceptability of profiling.

5.7.8 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.³²⁶

5.7.9 However, in so far as information which can identify a person is concerned, different opinions were expressed. 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.³²⁷

5.7.10 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.³²⁸

³²⁵ 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'. 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.

³²⁶ The Banking Council.

³²⁷ Andrew Rens.

³²⁸ Internet Service Providers Association.

- b) Written consent is necessary for non public information.³²⁹ Consent should be obtained from the data subject involved prior to information profiling taking place.³³⁰ 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 individual's consent should be provided with adequate remedies to enable them to take action against the responsible party in breach.³³¹
- c) If personal information is being used for this purpose without the consent of the data subject it should constitute an unacceptable infringement on his privacy.³³² The consent requirement should, however, not apply with regard to the prevention and detection of fraud.³³³
- d) Where consent must be provided for, "implied" consent may particularly be feasible, but the new law should then clearly set out for information of the whole of the public, when and how it will operate in practice.³³⁴

5.7.11 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.³³⁵

³²⁹ Strata.

³³⁰ Eskom Legal Department.

³³¹ SABC.

³³² ENF for Nedbank.

³³³ SAFPS.

³³⁴ Financial Services Board.

³³⁵ Credit Bureau Association.

- 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.³³⁶ 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 further 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.³³⁷
- 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 be possible.³³⁸
- 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. Any law prohibiting this practice will constitute an enormous blow to the South Africa economy.³³⁹

5.7.12 The EU Directive only deals with profiling as such in article 15(1) which provides for automated decisionmaking.³⁴⁰ Article 15(1) states that EU member states shall grant the right

³³⁶ The Banking Council.

³³⁷ SAPS.

³³⁸ LOA.

³³⁹ LOA.

³⁴⁰ **Article 15 Automated individual decisions**

- (i) 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

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, creditworthiness, reliability, conduct, etc.”

5.7.13 As an information protection provision, Art. 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, Art. 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 Art. 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.³⁴¹

5.7.14 Article 15 derives from several concerns. The central concern is rooted in the perceived growth of automatisisation of organisational decisions about individual persons. The drafters of the Directive appear to have viewed as particularly problematic the potential for such automatisisation to diminish the role played by persons in shaping important decision-making processes.³⁴² 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’.³⁴³

5.7.15 A second expressed fear is that the increasing automatisisation of decision-making processes engenders automatic acceptance of the validity of the decisions reached and a

relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

- (ii) 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.

³⁴¹ Bygrave *Computer Law and Security Report* 2001 at 2.

³⁴² Bygrave *Data Protection* at 3.

³⁴³ Bygrave *Computer Law and Security Report* 2001 at 5.

concomitant reduction in the investigatory and decisional responsibilities of humans. 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. 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. An important rationale for the right in Art 15(1) is, therefore, protection of human integrity and dignity in the face of an increasingly automated and inhumane world.³⁴⁴

5.7.16 Marketing profiles are, however, not regarded as necessarily detrimental to the data subject. On the latter point, the EU Commission seems to have been of the opinion that simply sending a commercial brochure to a list of persons selected by computer does not significantly affect the persons for the purposes of Art. 15(1). Also, other commentators view advertising (or at least certain forms of advertising) as too trivial to be significant.³⁴⁵

5.7.17 The prohibition against automated decision making is set out 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, most of the other European countries. However, no similar provision has been made in the Australian³⁴⁶ and Canadian³⁴⁷ legislation.

5.7.18 The Commission's preliminary views regarding profiling can be summarised as follows:

a) There is no objection to the compiling of statistical information and profiles

³⁴⁴ Bygrave Computer Law and Security Report 2001 at 8.

³⁴⁵ 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" (e.g. 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).

³⁴⁶ Privacy Amendment (Private Sector) Bill 2000.

³⁴⁷ Personal Information Protection and Electronic Documents Act 2000 (Bill C-6).

of personal information, provided it is not possible to trace the information to an identifiable data subject.

- b) The legitimate interests of business should be appropriately accommodated. In ordinary circumstances marketing profiles should not be regarded as detrimental to a data subject. Marketing practices are currently being dealt with in the ECT Act³⁴⁸ as well as in the National Credit Bill.³⁴⁹
- 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 39 (1) (k) and section 40 (3) of the proposed Bill furthermore already makes provision for the supervision of information matching legislation.
- e) 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.

5.7.19 The conclusion of the Commission is therefore that a section should be included in the proposed Act to provide for the prohibition of unreasonable automated decision making since its exclusion will deprive data subjects of a significant counterweight to the ongoing expansion, intensification and refinement of automated profiling practices. Comment is invited as to whether a specific section similar to sec 45 of the ECT Act should be included in the information protection legislation.

³⁴⁸

Section 45 of the Electronic Communications and Transactions Act, 25 of 2002 reads as follows:

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).

³⁴⁹

See in this regard Part C Credit Marketing Practices (clauses 73-77) of the NCB.

5.7.20 The legislative enactment of this provision will read as follows:

**CHAPTER 10
MISCELLANEOUS**

Automated decision making

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.*

Comment is invited.

CHAPTER 6: ENFORCEMENT

6.1 Introduction

6.1.1 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

6.1.2 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.³

6.1.3 It is therefore clear that the existence and ready availability of effective remedies 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.⁴

¹ EU 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 5 entitled "Supervision".

³ **WP101 on enforcement** at 3.

⁴ Korff **Comparative Study** at 179.

6.1.4 We have already established⁵ that the most notable difference between the self-regulatory system on the one hand and the regulatory or co-regulatory systems on the other hand, is the manner in which the information protection principles are enforced.⁶ 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.⁷ 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.

⁵ See Chapter 5 above.

⁶ See also Roos thesis at 533.

⁷ Roos thesis at 534.

6.1.5 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.⁸ Art 28(4) provides that the authority shall consider complaints.⁹ Art 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.¹⁰ Art 28(3) also stipulates that decisions by an information protection authority which give rise to complaints “may be appealed against through the courts”.¹¹ Finally, art 28(6) stipulates that the supervisory authorities must cooperate with one another.¹²

6.1.6 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

Art 28(3) 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 Art 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.

9

Art 28(4) 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.

10

Article 22 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 him by the national law applicable to the processing in question.

11

Art 28(3).

12

Art 28 (6) 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.

6.1.7 All information protection Acts stipulate a variety of sanctions and remedies for breach of their provisions.¹³ Provision is usually made for a combination of penalties (fines and imprisonment), compensatory damages and where applicable, revocation of licences and deregistration.

6.1.8 In the final analysis, the central question concerns the exact powers that a Commission has to order compliance with the information protection principles. Here there is a clear difference between those authorities whose powers are limited to those of investigation and recommendation, and those that can mandate changes in behaviour.¹⁴

6.2 Investigating complaints

6.2.1 All the 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.¹⁵

6.2.2 The oversight function of information protection authorities typically encompasses the handling and resolution of complaints by citizens pertaining to the processing of personal information.¹⁶ 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.¹⁷

6.2.3. In most countries the national authorities are vested with extensive powers of access to

¹³ 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.

¹⁴ Bennett and Raab *The Governance of Privacy* at 117.

¹⁵ Korff *Comparative Study* at 206.

¹⁶ Bygrave *Data Protection* at 70.

¹⁷ 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.

files and filing systems used to process personal information, and the authorities can therefore usually demand full access to all relevant sites and materials.¹⁸

6.2.4 Commissioners are sometimes given astonishingly wide and strong powers of search and entry, often exercisable without a judicial warrant.¹⁹

6.2.5 After a complaint has been received the authority usually gets in touch with the responsible party concerned, “advices” 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.²⁰

6.2.6 Examples of the work done by Privacy Commissioners in other countries are set out in Chapter 5 above.²¹

6.2.7 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”.²²

6.3 Assessment/Audit

¹⁸ Korff *Comparative Study* at 206.

¹⁹ Korff *Comparative Study* at 200; See eg sec 34(1)(d) of the Canadian Privacy Act; sec 12(1)(d) of the Canadian PIPEDA.

²⁰ Korff *Comparative Study* at 208.

²¹ See specifically para 5.2.26 and further.

²² Greenleaf presentation 2002 at 24.

6.3.1 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 Act. Such an assessment may also be conducted on the initiative of the Commission itself (especially where new technology is being used for the first time).²³

6.3.2 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.

6.3.3 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.²⁴ 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.

6.3.4 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 sec 42 have been received with regard to processing for special purposes (journalism, literary and artistic purposes).

6.3.5 As is the case with enforcement notices discussed above, the latter notices are also subject to an appeal procedure set out in terms of sec 48 of the Act. Under sec 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.

²³ See eg section 42 of the UK Data Protection Act, 1998; section 13(1) (b) of the New Zealand Act; Sec 60 of the WBP in the Netherlands; sec 18 of the Canadian PIPEDA (private bodies); sec 37 of the Canadian Privacy Act (public bodies).

²⁴ Bainbridge *Data Protection* at 146.

6.3.6 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.²⁵

6.3.7 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.²⁶ In the last five years privacy specialists have developed an assessment model for the application of new technology or the introduction of a new service, which has good potential for raising privacy alarms at an early stage in an organisation's planning process in either the public or the private sectors.

6.3.8 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.

6.4 Advisory approach

6.4.1 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,²⁷ or they have not had it in relation to certain sectors.²⁸

6.4.2 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

²⁵ 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 .

²⁶ 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.

²⁷ Eg Germany's Federal Data Protection Commissioner see the Federal Data Protection Act ss 24-26.

²⁸ Bygrave *Data Protection* at 71.

adverse publicity for poor privacy protection can be an effective sanction.²⁹ The implementation of the Directive does not appear to have changed the generally advisory and conciliatory approach of the national information protection authorities.³⁰

6.4.3 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.³¹ In many jurisdictions, the enforcement of information protection laws seems rarely to involve meting out penalties in the form of fines or imprisonment.

6.4.4 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.³² However, the outcomes may be more in line with compromises than a solution imposed on the basis of a purely legal ruling.³³ It would appear that if the authority has a “stick behind the door” it can be more forceful in such attempts at “conciliation”.³⁴

6.4.5 The benefits of giving advice are 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 claim of pre-judgment, or

²⁹ Bennett and Raab *The Governance of Privacy* at 117.

³⁰ Korff *Comparative Study* at 200.

³¹ Korff *Comparative Study* at 207.

³² Bygrave *Data Protection* at 79 and references therein.

³³ Korff *Comparative Study* at 207.

³⁴ 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 “proposed” by the authority.

bias, where a complaint is later made about the matter.³⁵

6.5 Enforcement powers

6.5.1 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.³⁶

6.5.2 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 also does not specifically address whether or not these authorities must be given competence to issue legally binding orders.³⁷

6.5.3 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.³⁸

6.5.4. 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.³⁹

6.5.5 Examples of different enforcement procedures are as follows:

³⁵ 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.

³⁶ In the UK fines may be levied on controllers (responsible parties) convicted of an offence.

³⁷ 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".

³⁸ Korff *Comparative Study* at 208.

³⁹ Ibid.

- a) In France, the 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.⁴⁰
- 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.⁴¹
- 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 52⁴² 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)⁴³
- 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:

- a) the enforcement notice;
- b) the information notice; and
- c) 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) to take or refrain from taking specified steps within a specified time and to refrain from

⁴⁰ Ibid.

⁴¹ Greenleaf presentation 2002 at 9.

⁴² See section 52 (4) of the federal Privacy Act.

⁴³ Greenleaf presentation 2002 at 11.

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 regard processing for the special purposes (journalism, literary and artistic purposes as set out in the Act).⁴⁴

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.

6.5.6 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 available to all interested parties.⁴⁵

6.6 Courts/judicial remedies

6.6.1 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.⁴⁶ Recital 55 of the EU Directive makes provision for judicial remedies.⁴⁷ Art 22 of the EU Directive⁴⁸ provides for

⁴⁴ For a discussion of information notices, see para 5.5 above.

⁴⁵ Korff *Comparative Study* at 201.

⁴⁶ Bennett and Raab *The Governance of Privacy* at 117.

⁴⁷ 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

judicial remedies for data subjects.

6.6.2 In the EU Directive Article 24⁴⁹ permits sanctions to be imposed in case of infringement of the provisions adopted pursuant to the Directive.

6.6.3 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,⁵⁰ 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.⁵¹

6.6.4 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 policemen who obtain access to criminal records or other confidential information on behalf of

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 or public law, who fails to comply with the national measures taken under this Directive.

48 See footnote 10 above.

49 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.

50 Sections 40 an 48 of the UK Data Protection Act.

51 Korff *Comparative Study* at 181.

unauthorised third parties).⁵²

6.6.5 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, the last few years, begun to enforce the law more strictly, by imposing very substantial fines of up to Euro 60,000.⁵³

6.6.6 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.⁵⁴ 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 1977.⁵⁵

6.7 Compensation

6.7.1 Article 23⁵⁶ of the EU Directive provides for compensation to the data subjects who have suffered damage.

6.7.2 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

⁵² Korff *Comparative Study* at 209.

⁵³ Ibid.

⁵⁴ Bennett and Raab *The Governance of Privacy* at 118.

⁵⁵ Sec 82 of the New Zealand Privacy Act.

⁵⁶ 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.

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 provision specified by the Directive.⁵⁷

6.7.3 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.⁵⁸

6.7.4 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 - 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.⁵⁹

6.8 Conclusion

6.8.1 It is clear that the best way of providing external supervision is through an independent oversight authority,⁶⁰ as well as by providing information subjects with legal remedies which they can enforce in a court of law.⁶¹ The oversight body 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

⁵⁷ Korff *Comparative Study* at 180.

⁵⁸ Ibid.

⁵⁹ Korff *Comparative Study* at 180.

⁶⁰ See Chapter 5 above.

⁶¹ See discussion in Chapter 5 above; Roos thesis at 723 referring to Data Protection Working Party Transfers of personal data to third countries 4-5.

compensation by either the responsible parties or the data processors.⁶² Finally, in accordance with most other jurisdictions, the legislation should also provide for a number of criminal offences under the Act. Comment is invited.

6.8.2 The proposed legislation reads as follows:

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;⁶³ 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.*

⁶² Summary in Roos thesis at 538.

⁶³ The New Zealand definition includes subparagraph (b) set out below. Comment is invited.

1.(1) For the purposes of this Part of this 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 principle; 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.

(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 conduct 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 sec 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 sec 73; and*
- (f) otherwise carry out in those premises any inquiries that the Commission sees fit in terms of sec 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 record, other material or equipment 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

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 **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 sec 63, must make an assessment, subject to subparagraph (2), as to whether it is likely or unlikely that the processing being conducted 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.

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 an independent auditor's report indicating that the processing is occurring in compliance with the principles of the Act, or 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 must 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.

(12) A report made by the Commission under section 81(10) is deemed to be the equivalent to an enforcement order served in terms of sec 83 of this Act.

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.

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 Commission,*

that it ought to have exercised its discretion differently, the court must allow the appeal or substitute such other notice or decision as could have been served or made by the Commission; 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.

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.

(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.

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 sec 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.

CHAPTER 7: CROSS-BORDER INFORMATION TRANSFERS

7.1 As was indicated in Issue Paper 24, the ease with which electronic data flows across borders leads 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.

7.2 It is for this reason that Article 25 of the European Directive 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.¹

¹

See Bygrave *Data Protection* at 81; Broadly similar, but less complicated, principles on transborder data flows are set down in paras 17-18 of the OECD Guidelines and in 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 data flows between a broader range of countries

7.3 The European Union and all its trading partners have been required to have adequate information protection regimes, conforming to the European Data Protection Directives, with effect from 24 October 1998.² This means that 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 selfregulation covering the information protection principles outlined in Chapter 4 of the Discussion Paper.³

7.4 The following points should be noted:⁴

- a) Article 25 requires an “adequate level” of protection, not “comparable level” or similar level”.
- b) Under Article 25, the determination of “adequate level” can be made by the transmitting country, by another EU member nation, or by the EU staff in Brussels.
- c) Article 25(2) provides that an adequate level of privacy protection is assessed in light of all circumstances surrounding the information transfer operation, including:
 - the nature of the information;

2

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.

3

See also DMA Submission on Open Democracy Bill.

4

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”).

- the purpose and duration of the information processing and transmission operation;
- the rules of law in force; and
- the professional rules and security measures established for the information.

7.5 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 this provision of Article 25 in Article 26. In terms of these exemptions adequacy is determined in each individual case or with regard to individual bodies.

7.6 Article 26⁵ identifies the circumstances under which an EU member nation can authorise transfer in the absence of an adequate level of information protection, including:

- a) 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).

⁵

Art 26 provides as follows:

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 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.

b) the company receiving the information establishes privacy rights through appropriate contractual clauses.⁶

7.7 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 containing standard information protection clauses. This kind of contract would bind the 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.⁷

7.8 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.⁸

7.9 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.

7.10 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.⁹

7.11 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

⁶ 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.

⁷ EPIC and Privacy International *Privacy and Human Rights Report 2002* at 16.

⁸ 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.

⁹ 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.

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.¹⁰

10

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>.

7.12 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 26, 2000, the Commission approved the agreement.¹¹ Over 200 companies have joined the Safe Harbor.¹²

7.13 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.

7.14 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

¹¹ 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, available at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf.

¹² Safe Harbor List <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+lis>.

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 for United States signatory companies to implement the principles.

7.15 In February 2002 the European Commission issued a report on the practical operation of the European Union-United States Safe Harbor Agreement.¹³ 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.

7.16 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.

7.17 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.

7.18 Respondents to Issue Paper 24 were in general in favour of the principle that care should be taken to ensure that the South African model will be regarded as adequate in terms of sec 25. There was, however, a difference of opinion regarding the question whether adequacy necessarily implied a strong, regulatory information protection system.

13

European Commission Staff Working Paper, February 2002, available at http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf.

7.19 Respondents who were in favour of ensuring adequate protection of information through a comprehensive general statute argued as follows:

- * 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. 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.¹⁴
- * It will definitely affect South African international trade negatively if we do not meet the requirements of article 25 of the EU directive.¹⁵

¹⁴ The Internet Service Providers Association.

¹⁵ The Banking Council; Gerhard Loedolff; Nedbank; Eskom Legal Department.

- * 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. ¹⁶Therefore, 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.). ¹⁷The 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 that such legislation

¹⁶ Nedbank.

¹⁷ Nedbank.

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 operations¹⁸.

7.20 On the opposite side, the following arguments were posed:

- * 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."¹⁹ There is therefore a case for satisfying the adequacy provision through selfregulation and the courts.²⁰

18 Nedbank.

19 Sanlam Life; Legal Service.

20 Sagie Nadasen Legal Adviser : Sanlam Life Law Service.

- * Du Motier and Goemans (*Data Privacy and Standardizaion* 2000) 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:²¹
- (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.²²

- * Possibilities exist for *ad hoc measures* where there are inadequate levels of

²¹ Ibid.

²² Ibid.

protection. Thus, a contract between the information provider in the EU and the recipient in the third country can be concluded whereby additional safeguards for the data subject are provided due to the absence of an enforceable set of information protection rules.²³

- * Carey (*Data Protection Act 1998* (1998)) notes 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.²⁴
- * 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 ”²⁵.
- * 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

²³ Ibid.

²⁴ Ibid.

²⁵ Ibid.

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 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.²⁶

7.21 A new initiative being explored by multi-national corporations to overcome the difficulties when transferring information on a global basis is the development of global codes of conduct that would govern all their practices worldwide at the same time.²⁷

7.22 Given the growing number of cross-border information transfers, the idea of relying on global rules for all cross-border information transfers is attractive. The code of conduct concept is a simple one. Related companies doing business in multiple countries would apply just one set of rules to govern their information transfers from within the European Union to outside the EU rather than having to comply with the specific requirements of each of the countries in which they operate. Companies could also draft these codes so that they comply with the privacy laws in non-EU countries.

7.23 The Directive makes provision for and encourages members to make use of codes of conduct. The primary obstacle to using codes of conduct for cross-border transfers is that there is no streamlined mechanism for approving enterprise-wide codes. Mutual recognition by different states or co-operation mechanisms between the regulatory authorities of the different states could, however, facilitate the needs of multinational companies with establishments in several jurisdictions.²⁸

²⁶ SAFPS; Credit Bureau Association.

²⁷ Wugmeister et al **Codes of Conduct** at 3.

²⁸ Wugmeister et al **Codes of Conduct** at 1; See also Art 29 Working Party Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Directive to Binding Corporate Rules for International Data Transfers June 2003.

7.24 In summary the following points should be noted:

a) 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. 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, 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.

b) 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, in so far as its trade with African countries are concerned, should it comply with sec 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.

7.25 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. The Bill will furthermore stipulate that information will not be transferred to another country if proper safeguards for the protection of the information has not been made.

7.26 The legislative enactment will read 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 Principles set out in Chapter 3 of this Act; or*
- (b) the data subject consents to the transfer; or*
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject's request; or*
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or*
- (e) all of the following apply:*
 - (i) the transfer is for the benefit of the individual;*
 - (ii) it is reasonably impracticable to obtain the consent of the data subject to that transfer;*
 - (iii) if it were reasonably practicable to obtain such consent, the individual would be likely to give it.*

Comment is invited

CHAPTER 8: COMPARATIVE LAW ¹

8.1 Introduction

8.1.1 It is important to learn from the experiences of other countries. 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:²

- the legal framework and the protection afforded to data privacy;³
- cultural attitudes to openness and privacy and the role of the government;⁴
- historical events, which may have left an indelible impression on public attitudes to privacy;⁵ and
- population size, which has an impact on the ease with which projects can be implemented.⁶

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: An International Survey of Privacy Laws and Developments*** and the references therein. This annual report published in the USA by EPIC and Privacy International, reviews the state of privacy in over sixty countries around the world. It outlines legal protections for privacy, new challenges, and summarises important issues and events relating to privacy and surveillance. Electronic versions of the report is available at <http://www.epic.org/>. See also

² A Performance and Innovation Unit of the UK Cabinet Office ***Privacy and Data-Sharing: The Way Forward for Public Services*** Ann B, International Comparisons April 2002 (hereafter referred to as “***PIU Privacy and Data Sharing Report***”) at 18.

³ 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.

⁴ 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.

⁵ 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.

⁶ 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.

8.1.2 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.

8.2 International Directives⁷

8.2.1 The first data protection laws in the world were enacted in the seventies.⁸ There are now well over thirty countries which have enacted data protection statutes at national or federal level and the number of such countries is steadily growing.⁹

8.2.2 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 Data¹⁰ and the 1981 Organisation for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.¹¹

8.2.3 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.

8.2.4 The Convention is the hereto sole international treaty dealing specifically with data

⁷ See discussion with regard to international instruments in paras 1.2.12 and 4.1 above.

⁸ An analysis of these laws is found in Flaherty D *Protecting Privacy in Surveillance Societies* University of North Carolina Press 1989.

⁹ Bygrave *Data Protection* at 30.

¹⁰ Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 1981.

¹¹ OECD Guidelines.

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

8.2.5 The Convention is not intended to be self-executing. Art 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.¹⁵

8.2.6 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.

8.2.7 In 1995, the European Union enacted the Data Protection Directive¹⁶ 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.

8.2.8 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).¹⁷

8.2.9 The Directive sets a baseline common level of privacy that not only reinforces current data

12 EPIC and Privacy International *Privacy and Human Rights Report 2003* at 9. It has been ratified by 30 CoE Member states.

13 Art 23.

14 Bygrave *Data Protection* at 32.

15 Bygrave *Data Protection* at 34.

16 EU Directive.

17 For further discussion see Ch 7 above.

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.¹⁸ It provides only a basic framework which will require to be developed in national laws.¹⁹

8.2.10 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.

8.2.11 Some account should also be taken of the UN Guidelines.²⁰ 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.²¹

8.2.12 The Commonwealth Law Ministers have furthermore proposed for consideration by Senior Officials at their meeting in November 2001 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.

8.2.13 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, in accordance with general practice in member countries only to deal with information privacy which

¹⁸ See Ch 1 above.

¹⁹ 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.

²⁰ UN Guidelines.

²¹ Bygrave *Data Protection* at 33.

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.²²

8.2.14 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.²³ In March 2004, version 9 of the APEC Privacy Principles was released as a public consultation draft. Implementation mechanisms, including mechanisms to deal with transborder data flows are also still under consideration. A high APEC standard could be a means of resolving international data export issues, but low standards could result in a privacy confrontation between Europe and the Asia-Pacific.²⁴

8.2.15 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.

²² 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. They asked the Commonwealth Secretariat to prepare an amended draft which would be considered at the next planning meeting of Secretariat officials.

²³ A Privacy Sub Group was set up comprising Australia, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States.

²⁴ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

8.3 United States of America²⁵

8.3.1 The United States Constitution does not explicitly mention a right to privacy. 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”²⁶ and also in so far as marriage, procreation, contraception, family relationships, child rearing and education are concerned.²⁷

8.3.2 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.²⁸

8.3.3 The Privacy Act of 1974 regulates the information practices of federal agencies.²⁹ It requires agencies to apply basic fair information procedures.³⁰ The efficiency of the Act is, however, hampered by a weak remedial scheme and the lack of a proper information protection

²⁵ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 522 and the references made therein. See also the discussion regarding the self-regulatory system of the USA in para 5.3.43-46 in Ch 5 above.

²⁶ *Katz v United States* 386 U.S. 954 (1967).

²⁷ 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).

²⁸ Roos thesis at 38 and the references made therein.

²⁹ See also the Family Educational Rights and Privacy Act (FERPA) Pub L 93-380, 88Stat 571 (1974); Right to Financial Privacy (RFPA) 1978 Pub L 95-630; Privacy Protection Act (PPA) Pub L 96-440 codified at 42 USC s2000aa; Health Insurance Portability and Accountability Act (HIPAA) Pub L 104-191 codified at 42 USCA s 1320.; etc.

³⁰ Privacy Act, Pub. L. No. 93-579 (1974), codified at 5 USC § 552a,.

authority. It has furthermore been argued³¹ that its effectiveness is significantly weakened by administrative interpretations of a provision allowing for disclosure of personal information for a “routine use” compatible with the purpose for which the information was originally collected. Limits on the use of the Social Security Number have also been undercut in recent years because Congress has approved new purposes for the identifier and because the private sector employs the identifier for many purposes with virtually no safeguards for the individual.

8.3.4 In the 2003 term, the Supreme Court considered the Privacy Act, a privacy exemption to the Freedom of Information Act, and the issue of whether police could compel an individual to identify himself in public. In *Doe v. Chao*,³² the Court ruled that a plaintiff in a Privacy Act suit must demonstrate actual damages to qualify for the Act's minimum statutory award of USD 1,000.³³

8.3.5 In March 2003, the Department of Justice announced that it would exempt the National Crime Information Center (NCIC) from data quality standards in the Privacy Act. The NCIC contains 39 million criminal records, and is used by over 80,000 law enforcement agencies. The change was strongly opposed by a broad coalition of organizations and individuals across the United States.³⁴

8.3.6 The United States has no comprehensive privacy protection law for the private sector. 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

³¹ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 524.

³² 124 S.Ct 1204 (2004).

³³ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

³⁴ Ibid.

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).

activities,³⁹ educational records,⁴⁰ motor vehicle registrations,⁴¹ and telemarketing.⁴²

8.3.7 There is no independent information protection agency 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:

- The Office of Management and Budget⁴³ plays a limited role in setting policy for federal agencies under the Privacy Act, but it has not been particularly active or effective.
- In 1999 a Chief Counselor for Privacy was appointed within the Office of Management and Budget to coordinate federal stances towards privacy. The Counselor had only a limited advisory capacity. The Bush Administration has eliminated this position.
- The Federal Trade Commission has oversight and enforcement powers for the laws protecting children's online privacy, consumer credit information and fair trading practices but has no general authority to enforce privacy rights. The FTC has received thousands of complaints but has issued opinions in only a few cases. It has also organised a series of workshops and surveys, which have found that industry protection of privacy on the Internet is poor, but the FTC had long said that the industry should have more time to make self-regulation work. In a shift from this position, in June 2000, the FTC recommended in a report to the United States Congress that legislation is necessary to protect consumer privacy on the Internet due to the dismal findings in a survey of online privacy policies.⁴⁴ Since issuing that report, the new Chairman of the Commission appointed by President Bush has recommended that more study is necessary before legislation is passed to protect

³⁹ See 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.

⁴³ Part of the executive office of the President.

⁴⁴ ***Privacy Online: Fair Information Practices in the Electronic Marketplace:*** A Federal Trade Commission Report to Congress May 2000.

Internet Privacy.⁴⁵ Instead, FTC has focused on enforcing existing law in the areas of telemarketing, spam, pretexting, and children's privacy.⁴⁶ 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.⁴⁷ Enrolment began in June 2003, and now approximately 60 million numbers have been added to the list.⁴⁸

8.3.8 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.⁴⁹

8.3.9 Developments since 1999 have been as follows:

- The end of 1999 brought increased scrutiny on financial privacy. In 1999, the Michigan Attorney General sued several banks for revealing that they were selling information about their customers to marketers. Other banks across the country subsequently admitted that they were also selling customer records. The Gramm-Leach-Bliley Act, 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 effective date of the privacy provisions were pushed back from November 2000 until July 2001.

⁴⁵ Protecting Consumers' Privacy: 2002 and Beyond, Remarks of FTC Chairman Timothy J. Muris, October 2001.

⁴⁶ See FTC Privacy Initiatives.

⁴⁷ The Proposed National "DO NOT CALL" Registry, Amendment to the Telemarketing Sales Rule, January 2002.

⁴⁸ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

⁴⁹ See discussion in Ch 7 above.

- In 2000 the sole federal law governing information use online went into effect. The Children's Online Privacy Protection Act (COPPA), passed by Congress in 1998 and requiring parental consent before information is collected from children under the age of 13, went into effect in April 2000.⁵⁰

- 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.⁵¹ In April 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.⁵² 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.⁵³

- In 2003, Congress passed legislation significantly amending the Fair Credit Reporting Act (FRCA) and the nation's first spam regulation.⁵⁴

⁵⁰ FTC Privacy Pages .

⁵¹ Office of the Secretary ***Standards for Privacy of Individually Identifiable Health Information***; Proposed Rule 45 CFR Parts 160 and 164, §164.501 March 27, 2002.

⁵² EPIC and Privacy International ***Privacy and Human Rights Report 2004*** and the references made therein.

⁵³ 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/>.

⁵⁴ EPIC Fair Credit Reporting Act page available at <http://www.epic.org/privacy/frca/>.

8.3.10 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.⁵⁵ A number of court cases have dealt with the protection of the right to privacy and data.⁵⁶

8.3.11 There has been significant debate in the United States in recent years about the development of privacy laws covering the private sector:⁵⁷

- 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.⁵⁸
- c) There is also **substantial activity in the states**. In recent years, Massachusetts and Hawaii have considered comprehensive privacy bills for the private sector.

⁵⁵ See *Lake v WalMart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998), for a review of state adoption of common law privacy torts.

⁵⁶ 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.¹⁹⁶⁰ 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.¹⁹⁶¹ *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.¹⁹⁶² Also, in March 2001, the Supreme Court held that a state 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 Bible, 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 Drayton*, 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 *Earls*, 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.^{Bd. of Educ. v Earls, 122 S. Ct. 2559 (2002). In *Falvo*, 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 *Gonzaga*, 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).}

⁵⁷ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 529 and the references as indicated below.

⁵⁸ See EPIC Bill Track.

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.⁵⁹ Minnesota enacted a Bill that requires ISPs to give notice and obtain user authorisation before using personal information for secondary purposes.⁶⁰ In a statewide referendum, North Dakota residents established opt-in protections for financial information.⁶¹ Additionally, Georgia enacted a privacy law that prohibits private businesses from discarding documents or computer components that contain personal information⁶².

- 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.⁶³ A series of companies, including Intel and Microsoft, were discovered to have released products that secretly track the activities of Internet users.⁶⁴ 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**⁶⁵ has been created and private-sector corporations are collaborating to use commercial marketing data for terrorism profiling.⁶⁶
- f) Recent years have seen a new trend towards the increased use of **video**

59 California Senate Bill 168.

60 Minnesota S.F. 2908.

61 Friery T "Privacy Alert: North Dakota Votes for 'Opt-In' Financial Privacy," Privacy Rights Clearinghouse, June 21, 2002.

62 Georgia Senate Bill 475.

63 Hoofnagle CJ **Consumer Privacy In the E-Commerce Marketplace 2002** Third Annual Institute on Privacy Law Practicing Law Institute G0-00W2 (June 2002).

64 See Big Brother Inside Campaign .

65 H.R. 5005, Homeland Security Act of 2002.

66 See Letter from the Center for Information Policy Leadership to Interested Parties, 2002.

- surveillance** cameras linked with facial recognition software in public places.^{67 68}
- g) There have been a number of proposals to create a **National ID**⁶⁹ in the wake of the September terrorist attacks.⁷⁰ Most of these efforts have sought the creation of a national identification system through the standardisation of state driver's licenses.^{71 72}
- h) Several other programmes have been initiated in the past few years, such as the

⁶⁷ 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.

⁶⁸ 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", *Wired News*, February 16, 2002;. Tests on the face recognition systems in operation at Palm Beach Airport in Florida, American Civil Liberties Union Press Release, "Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws," May 14, 2002;. and Boston Logan Airport have also shown the technology to be ineffective and error-ridden. Hiawatha Bray, "'Face Testing' at Logan is Found Lacking," *Boston Globe*, July 17, 2002.

⁶⁹ See also the recommendations of the National Commission on Terror Attacks Upon the United States (911 Commission) regarding the need for secure identification in the US.

⁷⁰ 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.

⁷¹ *Your Papers Please: From A State Driver's License to a System of National Identification*, EPIC Report, February 2002.

⁷² 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, the Driver's License Modernization Act of 2002. There are also more limited attempts to create national identification systems through "enhanced visa" documents and "trusted traveler" programs.

US-VISIT,⁷³ SEVIS,⁷⁴ CAPPSII,⁷⁵ MATRIX⁷⁶ and TIA⁷⁷(discontinued).⁷⁸

8.4 United Kingdom of Great Britain and Northern Ireland⁷⁹

8.4.1 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.⁸⁰ 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.

8.4.2 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 1998.⁸¹ The legislation, which came into force on March 1, 2000, replaced the 1984 Data Protection Act. It implements the requirements of the European Union's Data Protection Directive.⁸² 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

⁷³ United States Visitor and Immigrant Status Indicator Technology programme which requires visitors to the USA to submit a biometric identifier to the government.

⁷⁴ 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.

⁷⁵ Computer Assisted Passenger Pre-screening System aims to conduct background risk assessments on all air travellers before they fly on commercial airliners. The intention is to link CAPSS II and US-VISIT when both programmes are fully operational.

⁷⁶ 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.

⁷⁷ 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.

⁷⁸ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

⁷⁹ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 513 and the references made therein.

⁸⁰ Human Rights Bill, CM 3782, October 1997.

⁸¹ Data Protection Act 1998c. 29.

⁸² Data Protection Act 1984 (c. 35).

that entities that maintain records register with the Information Commissioner.

8.4.3 The Information Commissioner (formerly known as the Data Protection Commissioner and the Data Protection Registrar), is an independent officer that enforces both the Data Protection and Freedom of Information Acts.⁸³ Statistics are published in the Annual Report.⁸⁴ In June 2003, the Commissioner issued a code of guidance for employer/employee relationships.

8.4.4 The Commissioner is also responsible for enforcing the Telecommunications (Data Protection and Privacy) Regulations. These regulations came into force on March 1, 2000, and implement the 1997 European Union Telecommunications Directive.⁸⁵

8.4.5 There are also a number of other laws containing privacy components, most notably those governing medical records⁸⁶ and consumer credit information.⁸⁷ 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.⁸⁸

⁸³ Home page of the Information Commissioner, <<http://www.dataprotection.gov.uk/>>.

⁸⁴ As of March 31, 2002, there were 198,519 databases registered with the Commission.
a) The agency received 12, 479 requests for assessment and inquiries in 2001-2002.
b) There were 106 cases forwarded for prosecution resulting in 66 prosecutions and 33 convictions.
c) The Commissioner has also issued a number of comprehensive reports for the public.
d) She has published a Code of Practice for the use of Closed Circuit Television (CCTV) and a study of the availability and use of personal information in public registers.

⁸⁵ Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. They replaced the Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998 which came into effect on May 1, 1999.

⁸⁶ Access to Medical Reports Act 1988, Access to Health Records Act 1990, The Health and Social Care Act 2001.

⁸⁷ Consumer Credit Act, 1974.

⁸⁸ Crime & Disorder Act 1998: Data protection implications for information-sharing.

8.4.6 It has been noted⁸⁹ that the privacy picture in the United Kingdom is mixed. There is, at some levels, a strong public recognition and defence of privacy. Proposals to establish a national identity card, for example, have routinely failed in the past to achieve broad political support. 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.⁹⁰

8.4.7 Home Secretary David Blunkett announced on July 3, 2002 a six month consultation period on “entitlement cards,” a new name for a national ID card proposal.⁹¹ The cards will be mandatory for all persons over 16 years old and would be required to obtain health care, jobs and other services.⁹² A consultation and draft Bill was released in April 2004 . It will require biometric technologies and establish a central National Identity Register.⁹³

8.4.8 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)⁹⁴ and the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁹⁵ In November 2001, the United Kingdom signed the Council of Europe Convention on Cybercrime.⁹⁶ 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.

⁸⁹ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 513 and the references made therein.

⁹⁰ See Criminal Justice and Public Order Act 1994.

⁹¹ See Privacy International ID Cards Page.

⁹² The proposal has been widely criticised by politicians and major media across the political spectrum. Blunkett first proposed the card shortly after September 11 but was forced to back away after it was also severely criticised.

⁹³ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

⁹⁴ Signed May 14, 1981; Ratified August 26, 1987; Entered into Force December 1, 1987.

⁹⁵ Signed November 11, 1950; Ratified March 8, 1951; Entered into Force September 3, 1953.

⁹⁶ Signed November 23, 2001.

8.5 Kingdom of the Netherlands⁹⁷

8.5.1 The Dutch Constitution was amended in 1983 to include art 10 which grants citizens an explicit right to privacy.⁹⁸

8.5.2 In May 2000, the government-appointed commission for “Constitutional rights in the digital age” presented proposals for changes to the Dutch constitution. The commission was set up after confusion about the legal status of e-mail under the constitutionally protected privacy of letters. The commission’s task was to investigate if existing constitutional rights should be made more technology-independent and if new rights should be introduced.⁹⁹ No changes have been effected yet.

8.5.3 The Wet Bescherming Persoonsgegevens (WBP)(Personal Data Protection Act) of 2000 was approved by the Parliament in June 2000¹⁰⁰. 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

⁹⁷ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 362 and the references made therein.

⁹⁸ 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.”

Article 12 states:
 “(1) Entry into a home against the will of the occupant shall be permitted only in the cases laid down by or pursuant to Act of Parliament, by those designated for the purpose by or pursuant to Act of Parliament.
 (2) Prior identification and notice of purpose shall be required in order to enter a home under the preceding paragraph, subject to the exceptions prescribed by Act of Parliament. A written report of the entry shall be issued to the occupant.”

Article 13 states:
 “(1) The privacy of correspondence shall not be violated except, in the cases laid down by Act of Parliament, by order of the courts.
 (2) The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.”

⁹⁹ According to this proposal, Article 10 will be expanded to the right of persons to be informed about the origin of data recorded about them and the right to correct that data. Article 13 would be made technology-independent and would give the right to confidential communications. Breaches of this right could only be authorised by a judge or a minister. The discussion about possible changes is still ongoing. Data retention requirements and changes to article 13 of the Constitution, as recommended by the Mevis Committee, have recently been officially proposed by the Government in the Telecommunications Data Requisition Bill. In its annual report for 2001, the data protection authority criticised this proposal saying that “constitutional protection should not be restricted to the content of communications, but should extend to ‘traffic data’, i.e. information about the communications.”

¹⁰⁰ Personal Data Protection Act, Staatsblad 2000 302, July 6, 2000, unofficial translation.

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.¹⁰¹ Most of the existing codes are currently under revision for adaptation to the new legislation.

8.5.4 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.¹⁰² 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.

8.5.5 A focus of the CBP recently has been on establishing privacy protections within information communication technology. It is a major participant in the European Privacy Incorporated Software Agents (PISA) project¹⁰³ which was established to develop privacy enhancing techniques to protect user information in electronic transactions.¹⁰⁴

8.5.6 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".¹⁰⁵

¹⁰¹ 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.

¹⁰² Homepage <www.cbpweb.nl>.

¹⁰³ In January 2001, it issued a report on email and Internet privacy in the workplace setting out 17 guidelines for employers. According to the Chamber the report "argues in favor of a balanced and common sense approach to e-mail and Internet checks at the workplace." It concludes that although employees retain a reasonable expectation of privacy in the workplace, employers should be entitled to monitor email and Internet usage under certain conditions.

¹⁰⁴ College Bescherming Persoonsgegevens, Annual Report for the Year 2001, July 2002.

¹⁰⁵ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

8.5.7 Two decrees have been issued under the Data Registration Act. The Decree on Sensitive Data¹⁰⁶ sets out the limited circumstances when personal data on an individual's religious beliefs, race, political persuasion, sexuality, medical, psychological and criminal history may be included in a personal data file. The Decree on Regulated Exemption¹⁰⁷ exempts certain organisations from the registration requirements of the Data Registration Act.

8.5.8 Recent developments include the compulsory identification for all persons from the age of 14 (to have started in 2005) which is intended to increase public safety and the passing, in May 2004, of the law on e-commerce (Wet elektronische handel) that implements the EU E-commerce Directive (2000/31/EC).¹⁰⁸

8.5.9 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).¹⁰⁹ 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.¹¹⁰ 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.

8.6 New Zealand¹¹¹

8.6.1 Article 21 of the New Zealand Bill of Rights Act, 1990 states "Everyone has the right to be

¹⁰⁶ Decree on Sensitive Data, March 5, 1993.

¹⁰⁷ Decree on Regulated Exemption, July 6, 1993.

¹⁰⁸ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

¹⁰⁹ Signed May 7, 1982; Ratified May 28, 1993; Entered into Force September 1, 1993.

¹¹⁰ Signed November 23, 2001.

¹¹¹ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 370 and the references made therein.

secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise." ¹¹² 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.¹¹³

8.6.2 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.

8.6.3 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.¹¹⁴

8.6.4 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 information matching programs run by government agencies, and it makes special provision for the sharing of law enforcement information among specialized agencies.

8.6.5 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

¹¹² Bill of Rights Act, 1990, Chapter 4, Section 21, available at <http://www.oefre.unibe.ch/law/icl/nz01000_.html>.

¹¹³ 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.

¹¹⁴ See Chapters 4 and 5 above dealing respectively with the privacy principles and codes of conduct.

notification authority.¹¹⁵

8.6.6 Complaints by individuals are initially filed with the Privacy Commissioner who attempts to conciliate the matter. The Commissioner regards the power to investigate and to require answers during investigations as "a vital element" in securing such a high conciliation rate. When conciliation fails, the Director of Human Rights Proceedings¹¹⁶ 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.

8.6.7 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.

8.7 Canada¹¹⁷

8.7.1 There is no explicit right to privacy in Canada's Constitution and Charter of Rights and Freedoms.¹¹⁸ 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.¹¹⁹

8.7.2 Privacy is regulated at both the federal and provincial level. At the federal level, privacy is

¹¹⁵ Homepage <<http://www.privacy.org.nz>.

¹¹⁶ The Director is an official appointed under the Human Rights Act of 1993.

¹¹⁷ EPIC and Privacy International *Privacy and Human Rights Report 2003* at 176 and the references made therein.

¹¹⁸ 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).

¹¹⁹ *Hunter v Southam*, 2 S.C.R. 145, 159-60 (1984).

protected by two acts:

- a) the 1982 federal Privacy Act; and
- b) the 2001 Personal Information and Electronic Documents Act (PIPEDA).

8.7.3 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. It provides individuals with a right to access and request correction of personal information about themselves held by those agencies, subject to some exceptions.¹²⁰ 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.¹²¹ 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.¹²²

8.7.4 The Personal Information Protection and Electronic Documents Act (PIPEDA) was approved by Parliament in April 2000.¹²³ 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.

8.7.5 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.

¹²⁰ Privacy Act, c. P-21.

¹²¹ 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.

¹²² Privacy and Data Sharing Report fn 2 at 20.

¹²³ Bill C-6, Personal Information Protection and Electronic Documents Act.

8.7.6 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.¹²⁴ 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.

8.7.7 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.¹²⁵ 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.

8.7.8 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. 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.

8.7.9 The Commissioner's powers under PIPEDA are very similar to those under the Privacy Act. Under PIPEDA the Commissioner has investigated:¹²⁶

¹²⁴ European Union Article 29 Working Party, *Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act*, January 26, 2001.

¹²⁵ Commission Decision of December 20, 2001, Official Journal of the European Communities L 2/13.

¹²⁶ Examples of investigations under the Privacy Act as referred to in EPIC and Privacy International *Privacy and Human Rights Report 2003* are as follows:

- a) Canadian Customs and Revenue Agency (CCRA) following reports that customs officials were opening mail coming into Canada and passing information relating to immigration cases to Citizenship and Immigration Canada (CIC). [Office of the Privacy Commissioner, New Release , March 19,2001]
- b) Human Resources Development Canada (HRDC) regarding the existence of a government database called the Longitudinal Labour Force File, which could contain up to 2,000 pieces of information on Canadian citizens. The records included tax returns, benefit information, immigration files from the provincial and municipal levels, training information and employment and social insurance master files. The Privacy Commissioner expressed concern about the size of the individual files, their comprehensiveness and the lack of statutory safeguards, the absence of any retention or destruction policy and, above all, the fact that the data base had been compiled

- a) Air Canada for sharing its customers' personal and financial information with its partners.
- b) a U.S.-based international marketing firm that was disclosing personal information by gathering and selling data on physicians' prescribing patterns.
- c) a Canadian bank's refusal to grant a customer's request for access to their credit score.
- d) a telecommunications company for improperly disclosing a subscriber's unlisted telephone number to a collections agency.

8.7.10 The Bank Act,¹²⁷ Insurance Companies Act,¹²⁸ and Trust and Loan Companies Act¹²⁹ 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.”¹³⁰ There are sectoral laws for pensions,¹³¹ video surveillance,¹³² immigration,¹³³ and Social Security.¹³⁴ The Young Offenders Act¹³⁵ regulates the information that can be disclosed about offenders under the

largely without the knowledge of Canadian citizens Publication of the Commissioner's report appears to have resulted in a public outcry, the upshot was an announcement by the JHRDC that it was dismantling the longitudinal file and was scrapping the software that allowed sharing with other agencies and returning the information which it had received from them. Privacy and data Sharing Report at 21.[Minister of Human Resources Development Canada, HRDC Dismantles Longitudinal Labour Force File Databank, News Release, May 29, 2000.]

- c) Department of National Defense (DND) for workplace privacy violations, which entailed accessible online employee information.[Privacy Commissioner of Canada Annual Report to Parliament 2000-2001, Part One, n 494.

¹²⁷ Bank Act, c. 46, ss. 242, 244, 459.

¹²⁸ Insurance Companies Act, s. 489, s. 607.

¹²⁹ Trust and Loan Companies Act, s. 444.

¹³⁰ “88% of Canadians Oppose Banks Target-Marketing Insurance: Compass Poll,” *Canada Newswire*, April 27, 1999.

¹³¹ Canada Pension Plan, R.S.C. 1985, c. C-8, s. 104.07.

¹³² Criminal Code, c. C-46, s. 487.01.

¹³³ Immigration Act, S.C. 1985, c. I-2, s. 110.

¹³⁴ Old Age Security Act, c. O-9, s. 33.01.

¹³⁵ Young Offenders Act, C. Y-1, s. 38.

age of 18 while the Corrections and Conditional Release Act¹³⁶ speaks to the information that can be disclosed to victims and their families.

8.7.11 In May 2002 Canada became the first national government to make privacy assessments 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).¹³⁷

8.7.12 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.

8.7.13 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.

8.7.14 Public sector legislation covering government bodies exists in almost all provinces and territories.¹³⁸ Nearly every province has some sort of oversight body, but they vary in their powers and scope of regulation.

8.7.15 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.¹³⁹

¹³⁶ Corrections and Conditional Release Act, 1992, c. 20, s. 26, 142.

¹³⁷ EPIC and Privacy International *Privacy and Human Rights Report 2004* and the references made therein.

¹³⁸ A list of state laws and commissions is <http://infoweb.magi.com/~privcan/other.html>.

¹³⁹ 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

8.8 Commonwealth of Australia¹⁴⁰

8.8.1 Neither the Australian Federal Constitution¹⁴¹ nor the Constitutions of the six States contain any express provisions relating to privacy. There is periodic debate about the value of a Bill of Rights, but no current proposals. The Constitution limits the legislative power of the Commonwealth (federal) government, with areas not expressly authorised being reserved for the States.

8.8.2 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).

8.8.3 Privacy Law in Australia comprises a number of Commonwealth (federal) statutes covering particular sectors and activities,¹⁴² 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.

8.8.4 The principal federal statute is the Privacy Act of 1988¹⁴³ 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).

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.

¹⁴⁰ EPIC and Privacy International **Privacy and Human Rights Report 2003** at 139 and the references made therein.

¹⁴¹ The Commonwealth of Australia Constitution Act.

¹⁴² 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

¹⁴³ Privacy Act 1988 (Cth).

8.8.5 The Privacy Act provides for:

- 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).

8.8.6 The origins of the Privacy Act were the protests in the mid-1980s against the Australia Card scheme – a proposal for a universal national identity card and number. This proposal was dropped, but use of the tax file number was enhanced to match income from different sources with the Privacy Act providing some safeguards. The use of the tax file number has been further extended by law to include benefits administration as well as taxation. Some controls over this matching activity were introduced in 1990.¹⁴⁴

8.8.7 The Privacy Act was extended by the Privacy Amendment (Private Sector) Act 2000 (Commonwealth) to cover private sector organisations, passed in December 2000 and which took effect in December 2001.

8.8.8 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.¹⁴⁵

¹⁴⁴ The Data-matching program (Assistance and Tax) Act 1990.

¹⁴⁵ See Roger Clarke's Homepage <<http://www.anu.edu.au/people/Roger.Clarke/>>.

8.8.9 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;
- 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);¹⁴⁶
- 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.

8.8.10 The Act does, however, include an innovative principle of anonymity. Principle 8 states that: “Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation.”

8.8.11 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

¹⁴⁶

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.

data to flow to third countries.¹⁴⁷ The group recommended the introduction of additional safeguards to address these concerns.

8.8.12 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 look at options that do not impose unnecessary burdens on business."¹⁴⁸ In April 2004 the Privacy Commissioner urged a move away from the initial strategy of cooperation with the business sector towards greater enforcement. The Privacy Amendment Act of 2004 furthermore extended data - correction rights to non-Australian citizens.¹⁴⁹

8.8.13 The Office of Privacy Commissioner,¹⁵⁰ 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.

8.8.14 The Office has a wide range of functions, including handling complaints, auditing compliance, promoting community awareness, and advising the government and others on privacy matters. The Commissioner's office, which was cut back in the late 90's, recently received additional resources in anticipation of the new private sector jurisdiction.¹⁵¹

¹⁴⁷ European Union Article 29 Working Party **Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000.**

¹⁴⁸ 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.

¹⁴⁹ EPIC and Privacy International **Privacy and Human Rights Report 2004** and the references made therein.

¹⁵⁰ Homepage <<http://www.privacy.gov.au/>>.

¹⁵¹ Work done by the Commission:
 a) In September 2001, the Privacy Commissioner issued the finalised Guidelines on the implementation of the NPPs and a revised draft of the Guidelines on the development of industry codes.
 b) In April 2002, the Privacy Commissioner approved the first private sector code, submitted by the Insurance Council of Australia (ICA). Office of the Federal Privacy Commissioner, Media Release, "Federal Privacy Commissioner Approves Australia's First Privacy Act Privacy Code," April 17, 2002, Under the new General Insurance Information Privacy Code, complaints concerning the general insurance industry will be handled by the Privacy Compliance Committee, a committee of the Insurance Enquiries and Complaints Ltd, rather than the Privacy Commissioner. The Internet Industry Association is also drafting a code that it hopes will meet the European Union requirements. Karen Dearne, Privacy Safety Net for European Union, Australia IT News,

8.8.15 The federal Privacy Commissioner is also the supervisory and complaint handling agency of Part VIIC of the Crimes Act enacted in 1989¹⁵² and the Data-matching Program (Assistance and Tax) Act 1990.¹⁵³

8.8.16 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.¹⁵⁴ The research findings were incorporated into three separate reports:

- a) Privacy and the Community;
- b) Privacy and Business; and
- c) Privacy and Government.

8.8.17 The results showed overwhelming support for privacy protection.¹⁵⁵ The Privacy Commissioner indicated that the results of the survey would be used in the future planning of the office.

8.8.18 Some Australian States and Territories also enacted separate privacy laws.

-
- c) December 11, 2001. Other industries that have already adopted self-regulatory initiatives (e.g. the direct marketing and telecommunications industries) will have to decide whether to apply to register their Codes of Practice, and their alternative dispute resolution schemes, under the Privacy Act.
In March 2002 the Commissioner signed an agreement with the Australian Competition and Consumer Commission, which enforces existing fair trading rules, to facilitate cooperation and coordination between the offices where standards overlap. Office of the Federal Privacy Commissioner, "Regulators Co-Operate to Improve Privacy Compliance," Media Release, 12 March 2002.

¹⁵² 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).

¹⁵³ That provides detailed procedural controls over the operation of a major program of information matching between federal tax and benefit agencies.

¹⁵⁴ 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.

¹⁵⁵ 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***.

CHAPTER 9: A DRAFT BILL ON THE PROTECTION OF PERSONAL INFORMATION

9.1 In this, the second document to be published by the Law Commission in its investigation into privacy and information protection, the Commission has tried to develop and expand the proposals that were set out in its previously published Issue Paper.¹

9.2 The preliminary proposals of the Commission were summarised as follows in the Issue Paper:²

- 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 agency 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 agency.

9.3 Support from written submissions received, numerous discussions with various stakeholders and further research conducted, have strengthened the Commission's original views. These principles now form the basis of the proposed draft Bill set out in **Annexure B** to this discussion paper.

9.4 The Draft Bill comprises ten Chapters. Chapter 1 contains certain general provisions including an introductory section setting out the objects 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 the regulatory authority, notification and prior investigation and codes of conduct. Enforcement,

¹ SALRC Issue Paper 24 2003.

² Para 9.8 at 269 of SALRC Issue Paper 24.

offences and sanctions are provided for in Chapters 8 and 9. Finally, the miscellaneous and transitional provisions are contained in Chapter 10.

9.5 The Act 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.

9.6 In general, commentators cautioned that consistency in terminology, definitions and concepts of privacy and information protection when used in different laws and regulations such as the Promotion of Access to Information Act and the Electronic Communications and Transactions Act is of the utmost importance.³

9.7 It was furthermore noted⁴ that in information protection legislation, itself, two approaches can be identified:

- a) The EU approach which refers to "processing" of data. "Processing" being a term that, at the very least, includes the activities of the collection, use and disclosure of personal information
- b) The North American/Australian approach which refers separately to the "collection", "use" and "disclosure" of personal information.

9.8 The Commission has opted for the use of the term "processing" in order to ensure that all relevant activities are included. Other important terms used are "responsible party" (sometimes referred to as the "data controller"), "data subject" and "personal information".

9.9 The Bill gives effect to eight core information protection principles, namely processing limitation, purpose specification, further processing limitation, information quality, openness,

³ Vodacom.

⁴ IMS.

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.

9.10 Provision has been made for an independent Information Protection Commission with a full-time Information Commissioner to direct the work of the Commission. The Commission will be responsible for the implementation of both the Protection of Personal Information Act and the Promotion of Access to Information Act. Data subjects are under an obligation to notify the Commission 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.

9.11 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 Commission 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.

9.12 Enforcement should be through the Commission 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 Commission may furthermore assist a data subject in claiming compensation from a responsible party for damage suffered. Obstruction of the Commission's work is regarded in a very serious light and constitutes a criminal offence.

9.13 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.

9.14 The proposals and Bill prepared by the Law Commission will form the subject of a further consultative process before final consideration by the Commission itself. A series of workshops will be held across the country where the draft Bill will be considered and discussed by interested parties.

9.15 Should these proposals be adopted, the protection of information privacy in South Africa will be brought into line with international requirements and developments.

SUMMARY OF PRELIMINARY RECOMMENDATIONS

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 our 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 thirty 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 as well as the initiative of the Commonwealth Law Ministers in this regard. In both 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.

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, still to be enacted, National Credit Bill [B18-2005]. All these Acts contain interim provisions regarding information protection in South Africa.

The preliminary recommendations of the Commission, as set out in the Bill accompanying this document as **Annexure B**, can be summarised as follows:¹

- a) Privacy and information protection should 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 should be developed and incorporated in the legislation. The proposed 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 [**Chapter 3, Part A, clauses 7-23**]. Exemptions are furthermore possible for specific sectors in applicable circumstances [**Chapter 4, clauses 32-33**]. Special provision has furthermore been made for the protection of special (sensitive) personal information [**Chapter 3, Part B, clauses 24-31**].
- c) A statutory regulatory agency should be established. Provision has been made for an independent Information Protection Commission with a full-time Information Commissioner to direct the work of the Commission [**Chapter 5, Part A, clauses 34-46**]. The Commission will be responsible for the implementation of both the Protection of Personal Information Act (see Annexure B) and the Promotion of Access to Information Act, 2000. Data subjects will be under an obligation to notify the Commission of any processing of personal information before they undertake such processing [**Chapter 6, Part A, clauses 47-51**] 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 52-53**].
- d) Enforcement of the Bill will be through the Commission 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 Commission may furthermore assist a data subject in claiming compensation from a responsible party for any damage suffered. Obstruction of the Commission's work is regarded in a very serious light and constitutes a criminal offence [**Chapter 8, clauses 63-87 and Chapter 9, clauses 88-92**].

¹

- 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 Commission 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 Commission 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 54-62**].

- f) 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 10, clause 94**].

The preliminary recommendations and draft legislation need to be debated thoroughly. The Commission is seeking feedback regarding all its proposals as set out in the proposed draft Bill. Respondents are requested to respond as comprehensively as possible.

ANNEXURE A

LIST OF RESPONDENTS: 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
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
29. South African History Archive
30. South African Human Rights Commission
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

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 Commission; and to provide for matters incidental thereto

To be introduced by the Minister for Justice and Constitutional Development

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows --

CONTENTS OF THE ACT

Section

**CHAPTER 1
GENERAL PROVISIONS**

1. Objects of the Act
2. Interpretation

**CHAPTER 2
APPLICATION PROVISIONS**

3. Application of this Act
4. Exclusions
5. Saving
6. This Act binds the State

**CHAPTER 3
CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION**

/

Part A

Processing of personal information in general: Information Protection Principles

**PRINCIPLE 1
PROCESSING LIMITATION**

- 7. Lawfulness of processing
- 8. Minimality
- 9. Consent and necessity conditions
- 10. Collection directly from data subject

**PRINCIPLE 2
PURPOSE SPECIFICATION**

- 11. Collection for specific purpose
- 12. Data subject aware of purpose of collection and intended recipients
- 13. Retention of records

**PRINCIPLE 3
FURTHER PROCESSING LIMITATION**

- 14. Further processing not incompatible with purpose of collection

**PRINCIPLE 4
INFORMATION QUALITY**

- 15. Quality of information to be ensured

**PRINCIPLE 5
OPENNESS**

- 16. Notification to Commission and to data subject

**PRINCIPLE 6
SECURITY SAFEGUARDS**

- 17. Security measures to ensure integrity of personal information
- 18. Information processed by person acting under authority
- 19. Security measures regarding information processed by processor
- 20. Notification of security compromises

**PRINCIPLE 7
INDIVIDUAL PARTICIPATION**

- 21. Access to personal information
- 22. Correction of personal information

PRINCIPLE 8 ACCOUNTABILITY

23. Responsible party to give effect to principles

Part B: Processing of special personal information

24. Prohibition on processing of special personal information
25. Exemption to the prohibition on processing of personal information concerning a person's religion or philosophy of life
26. Exemption to the prohibition on processing of personal information concerning a person's race.
27. Exemption to the prohibition on processing of personal information concerning a person's political persuasion.
28. Exemption to the prohibition on processing of personal information concerning a person's trade union membership.
29. Exemption to the prohibition on processing of personal information concerning a person's health and sexual life.
30. Exemption to the prohibition on processing of personal information concerning a person's criminal behaviour.
31. General exception to the prohibition on processing of special personal information.

CHAPTER 4 EXEMPTIONS FROM INFORMATION PROTECTION PRINCIPLES

32. General
33. Commission may authorise processing of personal information

CHAPTER 5 SUPERVISION

Part A: Information Protection Commission

34. Establishment of Commission
35. Constitution of Commission and period of office of members
36. Remuneration, allowances, benefits and privileges of members
37. Secretary and staff
38. Funds
39. Powers and duties of Commission
40. Commission to have regard to certain matters
41. Programmes of Commission
42. Protection of the Commission
43. Meetings of Commission
44. Reports of Commission
45. Committees of Commission

Part B: Information Protection Officer

- 46. Information protection officer to be appointed

**CHAPTER 6
NOTIFICATION AND PRIOR INVESTIGATION
*Part A: Notification***

- 47. Processing to be notified to Commission
- 48. Notification to contain specific particulars
- 49. Exemptions to notification requirements
- 50. Register of information processing
- 51. Failure to notify

Part B: Prior investigation

- 52. Processing subject to prior investigation
- 53. Responsible party to notify Commission where processing is subject to prior investigation

**CHAPTER 7
CODES OF CONDUCT**

- 54. Issuing of codes of conduct
- 55. Proposal for issuing of code of conduct
- 56. Notification, availability and commencement of code
- 57. Amendment and revocation of codes
- 58. Procedure for dealing with complaints
- 59. Guidelines about codes of conduct
- 60. Register of approved codes of conduct
- 61. Review of operation of approved code of conduct
- 62. Effect of code

**CHAPTER 8
ENFORCEMENT**

- 63. Interference with the protection of the personal information of a person
- 64. Complaints
- 65. Mode of complaint to Commission
- 66. Investigation by Commission
- 67. Action on receipt of complaint
- 68. Commission may decide to take no action on complaint
- 69. Referral of complaint to regulatory body
- 70. Pre-investigation Proceedings of Commission
- 71. Settlement of complaints
- 72. Investigation proceedings of the Commission
- 73. Issue of warrants
- 74. Requirements for issuing of warrant
- 75. Execution of warrants

- 76. Matters exempt from search and seizure
- 77. Communication between legal adviser and client exempt
- 78. Objection to search and seizure
- 79. Return of warrants
- 80. Assessment
- 81. Information notice
- 82. Parties to be informed of result of investigation
- 83. Enforcement notice
- 84. Cancellation of enforcement notice
- 85. Right of appeal
- 86. Consideration of appeal
- 87. Civil remedies

CHAPTER 9 OFFENCES AND PENALTIES

- 88. Obstruction of Commission
- 89. Obstruction of execution of warrant
- 90. Failure to comply with enforcement or information notices
- 91. Penal sanctions
- 92. Magistrate's court jurisdiction to impose penalties

CHAPTER 10 MISCELLANEOUS

- 93. Automated decision making
- 94. Transborder information flows
- 95. Repeal and amendment of laws
- 96. Regulations
- 97. Short title and commencement

SCHEDULE 1 *Amendment of laws*

CHAPTER 1

GENERAL PROVISIONS

Objects of the 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 which will be in harmony with international prescripts and which will, while upholding the right to privacy, at the same time 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.

Interpretation

2. In this Act, unless the context otherwise indicates -

“biometric” means techniques of personal identification that are based on physical characteristics including fingerprinting, retinal scanning and voice recognition;

“Commission” means the Information Protection Commission as established in section 34 of this Act;

“consent” means any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal information relating to them;

“Constitution” means the Constitution of the Republic of South Africa 108 of 1996;

“data subject” means the person to whom personal information relate;

“information protection principle” means any of the principles set out in Chapter 3 of this Act;

“Minister” means the Minister for Justice and Constitutional Development;

“personal information”¹ means information about an identifiable, natural person, and in so far as it is applicable, an identifiable, 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;

¹ The definition of “personal information” in this Bill corresponds to the definition of “personal information” in the Promotion of Access to Information Act 2 of 2002. Since the two pieces of legislation are so closely related and the Commission has furthermore proposed that one supervisory authority be appointed to oversee both Acts it is important to ensure consistency in the terminology used. The Commission would, however, like to propose the following changes to this definition, which, if approved, would then be effected in the definition in both Acts:

- * the word “financial” included before the word “criminal” in subparagraph (b)
- * subpara (d) to read as follows: “(d) the address, blood type or any other biometric information of the person;
- * a semi-colon to be inserted after the words “the person” in para (e) and the rest of the sentence to be deleted.
- * Paragraphs (g) and (h) to be deleted.

The definition also provides for information about an identifiable juristic person in so far as it is applicable. (See also the definition of “personal information” in the ECT Act.)
Comment is invited in all instances.

- b) information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
- c) any identifying number, symbol or other particular assigned to the person;
- d) the address, fingerprints or blood type of the person;
- e) the personal opinions, views or preferences of the person, 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 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;
- h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, 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 person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
- j) but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years;

“prescribed” means prescribed by regulation;

“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;

“processor” means the person or body which processes personal information for the responsible party, without coming under the direct authority of that party;

"processing" means any operation or any set of operations concerning personal information, including in any case the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making

available in any other form, merging, linking, as well as blocking, erasure or destruction of information;

“public body” includes-

- (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; and
- (c) Parliament or a committee of Parliament;
- (d) the Cabinet as constituted under the Constitution;
- (e) any other body designated by the Minister by regulation made under this Act, to be a public authority for the purposes of this Act;

“record” means any recorded information -

- (a) regardless of form or medium; and includes any -
 - (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 public or private body, respectively;
- (c) whether or not it was created by a public or private body, respectively; and
- (d) regardless of when it came into existence;

"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.

CHAPTER 2

APPLICATION PROVISIONS

Application of this Act

3. This Act applies to-

- (a) the fully or partly automated processing of personal information, and the non-automated processing of personal information entered in a record or intended to be entered therein;
- (b) the processing of personal information carried out in the context of the activities of a responsible party established in the Republic of South Africa;
- (c) the processing of personal information by or for responsible parties who are not established in South Africa, whereby use is made of automated or non-automated means situated in South Africa, unless these means are used only for forwarding personal information.

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) that has been exempted from the application of the information principles in terms of sec 33.²

Saving

5. This Act will not affect the operation of any enactment that makes provision with respect to the processing of personal information and is capable of operating concurrently with this Act.

² Once the harmonisation of the legislation has taken place as recommended above in para 3.6.39 of the Discussion Paper, section 4 may read as follows:

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 intelligence or security services referred to in theAct;*
 - (d) *for the purposes of implementing the police tasks defined in the Act;*
 - (e) *by the armed forces in terms of theAct with a view to deploying or making available the armed forces to maintain or promote the international legal order.*

This Act binds the State

6. This Act binds the State.

CHAPTER 3

CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A: Processing of personal information in general: Information protection principles

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.

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.³

Consent and necessity conditions

³ Sec 8 (embodying the minimality principle, see paras 4.2.23-4..2.28 above) can also be included under Principle 2: Purpose specification and Principle 4:Data quality. Comment is invited.

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 93⁴ below.

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

⁴ This section furthermore to be read with the other information principles; See also ss 10, 11 and 12 of the UK DPA; arts 14 and 15 of the EU Directive; See also sec 45 of the ECT Act for the opt-out option regarding unsolicited commercial communications.

- 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.

PRINCIPLE 2

Purpose specification

Collection for specific purpose

11. Personal information must be collected for a specific, explicitly defined and legitimate purpose.

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 proceedings that 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.

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).

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.

PRINCIPLE 4

Information quality

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.

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.

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 required in terms of specific industry or professional rules and regulations.

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).

Notification of security compromises

Option 1:⁵

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.

⁵ 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 sec 20 of this Act.

(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.

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.

PRINCIPLE 7

Individual participation ⁶

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.

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.

⁶ The Commission's proposal in this regard is that this Act will deal with the access to the personal information of the requester and that the Promotion of Access to Information Act 2 of 2002 will deal with the right of access to all other information. See discussion in Chapter 4 of the Discussion paper, para 4.2.186 and further, especially para 4.2.207. A single authority will furthermore administer both Acts. If this proposal is accepted provision will be made in this act for the procedures to be followed in this regard and PAIA will be amended accordingly.

(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.

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.

Part B

Processing of special personal information

Prohibition on processing of special personal information

24. It is prohibited to process personal information concerning⁷ 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.

Exemption to the prohibition on processing of personal information concerning a person's religion or philosophy of life

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.

⁷ Sometimes the words "revealing" or "on" are used and the words "directly or indirectly" are included.

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.

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.

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;

(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 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;
- (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).

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.

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.

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.

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 (Proclamation 103 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 Commission⁸

39.(1) The powers and duties of the Commission will be---

education⁹

- (a) to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles;

⁸ The current proposal of the Law Commission is that the Information Commission will be responsible for the supervision of both the Promotion of Access to Information Act and the Protection of Personal Information Act. See Chapter 5 and para 4.2.203 in Chapter 4 of the discussion paper. Should this proposal be approved, the powers and duties of the Commission will be extended and PAIA amended accordingly.

- (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

⁹ Headings inserted for ease of reading, not part of the Bill.

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;¹⁰

general

- (y) to do anything incidental or conducive to the performance of any of the preceding functions;

¹⁰ This section will only apply if the Act provides for the appointment of self-regulating adjudicators.

- (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 sec 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

- 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 Officer¹¹

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.

¹¹ See sec 1 of PAIA for the definition of "information officer" and sec 17 regarding the designation of deputy information officers. It is envisaged that one officer should be designated in an organisation to deal with both privacy and information matters. It should be noted that PAIA does not currently make provision for the appointment of officers in private bodies. Comment is invited.

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 47.¹²

(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(1)(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.

¹² It is envisaged that the exemptions granted to certain categories of bodies from the provisions set out in Chapter 2 (publication and availability of certain records) of PAIA will also be applicable in so far as the notification requirements in terms of this Act are concerned.

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;¹³
- (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.

(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.

¹³ Exemptions.

(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 sec 83 of this Act.

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 the 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.

(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.

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 -

- (a) the action breaches an information privacy principle; or
- (b) the provisions of section 20 of this Act have not been complied with; or
- (c) the provisions of section 93 of this Act have not been complied with;¹⁴ or
- (d) the provisions of section 94 of this Act have not been complied with.

¹⁴ The New Zealand definition includes subparagraph (b) set out below. Comment is invited.

- 1.(1) For the purposes of this Part of this 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 principle; 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

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 conduct 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 sec 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 sec 73; and
- (f) otherwise carry out in those premises any inquiries that the Commission sees fit in terms of sec 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 record, other material or equipment 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

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.

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 sec 63, must make an assessment, subject to subparagraph (2), as to whether it is likely or unlikely that the processing being conducted 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.

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 an independent auditor's report indicating that the processing is occurring in compliance with the principles of the Act, or 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 must 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.

(12) A report made by the Commission under section 81(10) is deemed to be the equivalent to an enforcement order served in terms of sec 83 of this Act.

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.

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 Commission, that it ought to have exercised its discretion differently,

the court must allow the appeal or substitute such other notice or decision as could have been served or made by the Commission; 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.

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.

(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.

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 sec 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.

CHAPTER 10 MISCELLANEOUS

Automated decision making

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.

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 Principles set out in Chapter 3 of this Act; or
- (b) the data subject consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the data subject's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is reasonably impracticable to obtain the consent of the data subject to that transfer;
 - (iii) if it were reasonably practicable to obtain such consent, the individual would be likely to give it.

Repeal and amendment of laws

95. The laws mentioned in the Schedule to this Act are hereby amended to the extent indicated in the third column thereof.

Regulations

96. The Minister for Justice and Constitutional Development may make regulations on –

- (a) any matter which is required or permitted in terms of this Act to be prescribed;
- (b) the monitoring of this Act and the establishment of the Office of the Information Commissioner; and
- (c) any other matter which may be necessary for the application of this Act.

Short title and commencement

97.(1) This Act is the Protection of Personal Information Act, 2005, which takes effect on a date fixed by the President by notice in the Gazette.

(2) Different dates may be fixed under subsection (1) in respect of different provisions of this Act or in respect of different industries.

SCHEDULE 1
AMENDMENT OF LAWS

Number and year of law	Short title	Extent of amendment
-------------------------------	--------------------	----------------------------

.