

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: Atheneum 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 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.

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 *Huldigungsbundel 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.