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 2000[2] (the Open Democracy Bill was later renamed and became the Promotion of Access to Information Act).[3]

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

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

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

1.1.4 The Committee therefore requested the Minister for Justice and Constitutional Development to introduce privacy and data protection legislation in Parliament, after thorough research of the

---

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

2 ***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.

matter, as soon as reasonably possible.[4] The Minister, in turn, approached the Commission to consider the possible inclusion of such an investigation in its programme.

1.1.5 The investigation was included in the programme of the Commission and the Minister appointed a Project Committee, at the request of the Commission, to assist the Commission in its task. The Chairperson of the Committee is The Honourable Mr Justice Craig Howie. Prof Johann Neethling was appointed as project leader and the other members are Prof Iain Currie, Ms Caroline da Silva, Ms Christiane Duval, Prof Brenda Grant, Ms Adri Grobler, Mr Mark Heyink, Ms Saras Jagwanth and Ms Allison Tilley. The Committee had its first meeting on 22 July 2002.

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 person [6] (the data subject) in instances where such a person's personal particulars (data) 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/media threatens the personality in two ways:[7]

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

---

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

5 Neethling J ***Persoonlikheidsreg*** Butterworths Durban 1998 (hereafter referred to as " Neethling ***Persoonlikheidsreg***") at 39 fn 329; ***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 is 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 "scope of this inquiry" in para 1.3 below.

7 Neethling J, Potgieter JM & Visser PJ ***Neethling's Law of Personality*** Butterworths Durban 1996 (hereafter referred to as "***Neethling's Law of Personality***") at 295. 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 data 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 suggests that every society, even the most primitive, adopts mechanisms and structures that allow 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 law[13] and in sec

---

8 ***Neethling's Law of Personality*** at 295: 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 296: 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 is wrong.

10 Westin, A ***Privacy and Freedom*** New York Antheum 1967 as referred to by Bennett CJ "What Government Should Know About Privacy: A Foundation Paper" Paper prepared for the Information Technology Executive Leadership Council's Privacy Conference, June 19, 2001 (Revised in Aug 2001)(hereafter referred to as "Bennett").

11 Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948. See further Ch 3.

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, 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 European Convention for the Protection of Human Rights and Fundamental Freedoms ,1950. The American Convention on Human Rights (Art 11,14) and the American Declaration of the Rights and Duties of Man (Article V,IX and X) contain provisions similar to those in the Universal Declaration and International Covenant; The European Convention furthermore created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been active in the enforcement of privacy rights and have consistently viewed Article 8's protections expansively and interpreted the restrictions narrowly. In trying to give the necessary focus and relevance to international law, in 1994, South Africa signed and ratified three major human rights treaties of which ICCPR was one. There has however not been any real strategy for reviewing international human rights instruments to determine whether and how to sign and ratify them. Sarkin J "Implemetation of Human Rights in South Africa: Constitutional and Pan-African Aspects: A South African and Belgium Perspective" in Vande Lanotte J, Sarkin J & 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 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 38.

14 of the Constitution. [14] The common law protects rights of personality under the broad umbrella of 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 application[18] 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]

---

14 The Constitution of the Republic of South Africa, Act 108 of 1996 (hereafter referred to as "the Constitution") which came into operation on 4 February 1997. Section 14 of the Constitution reads as follows:

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

Secs 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 3 below.

16 See discussion in Ch 3 below.

17 ***Neethling's Law of Personality*** at 292.

18 Sec 36 of the Constitution.

19 See the discussion of sec 16, 22 and 32 of the Constitution in Ch 3 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.

20 See s 22 of the Constitution. See discussion Ch 3.

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

22 See secs 16 and 32 of the Constitution. See further discussion Ch 3.

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

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

1.2.9 There are many reasons why individuals disclose information about themselves and allow organisations to keep personal information about them. Sometimes it is because they are required to do so or because the provision of a particular product or service is conditional upon their 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.[24]

1.2.10 Interest in the right to privacy increased worldwide in the 1960s and 1970s with the advent of information technology. [25] The surveillance potential of powerful computer systems prompted demands for specific rules [26] governing the collection and handling of personal information.[27] 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. 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

---

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") at 21.

24 See discussion on public data users in Ch 4 below.

25 Piller C "Privacy in peril" ***Macworld*** v10 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 at a price; Neethling ***Huldigingsbundel WA Joubert*** at 105 et seq.

26 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 Report 2002") at 8.

27 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 Mc Nealy'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/.

of that decision-making process.[28]

1.2.11 The genesis of modern legislation in the area of data protection can be traced to the first data 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 that have enacted data protection statutes at national or federal level and the number of such countries is steadily growing. [30]

1.2.12 Early in the debates, it was, however, recognised that information privacy could not simply be regarded as a domestic policy problem. The increasing ease with which personal data 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 data 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,

---

28 Bennett at 6.

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") at 30.

31 Bennett at 6.

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

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.[34]

1.2.16 In 1995, the European Union enacted the Data Protection Directive[35] 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. 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 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" (the so-called safe-harbour principles).[36]

1.2.17 The Directive sets a baseline common level of privacy that not only reinforces current data protection law, but also establishes a range of new rights. The Directive contains strengthened protection over the use of sensitive personal data relating, for example, to health, sex life or religious or philosophical beliefs. In the 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.[37] It provides only a basic framework which will require to be developed in national laws.[38]

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.[39] The Guidelines are intended to encourage those UN Member States without data protection legislation in place to take steps to

---

34 A copy of the OECD Guidelines is available at http://www.oecd.org/documentprint/.

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 Ch5 below.

37 A copy of the Directive is available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

38 As referred to in Strathclyde Law School ***LLM in Information Technology and Telecommunications Law (Distance Learning)*** Web Est. 1994 Updated Oct 16 2001 "Notes for Information Security Theme Two: Data protection" (hereafter referred to as "Strathclyde") 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.

39 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")

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 data regimes than the other instruments.[40]

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 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.[41]

1.2.22 The international instruments referred to above will form the basis of discussion throughout this issue paper. The reasons for this are that they contain clear basic principles of data protection and that they serve as influential models of national and international initiatives on data protection.[42]

1.2.23 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 specified purpose for which it was originally obtained;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;

---

40 Bygrave at 33.

41 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.

42 Bygrave at 30.

- 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.[43]

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 data 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 (data protection) have not yet been enacted. South African commentators[44] are unanimous that the creation of such measures through legislation is a matter of great urgency.[45]

1.2.25 It should be noted that the Promotion of Access to Information Act,[46] inter alia, recognises the data protection principle that personal information should be accessible to the subject. This Act and the Electronic Communications and Transactions Act[47] also do have interim provisions dealing, respectively, with the correction of data and the voluntary adherence to data protection principles. These sections are regarded as interim measures until specific data privacy legislation has been finalised. The Department of Trade and Industry is also considering whether regulations should be formulated to regulate the credit bureau industry.[48] The promulgation of data protection legislation in South Africa will necessarily result in amendments to these statutes and other South

---

43 See discussion in Ch 6 below.

44 ***Neethling's Law of Personality*** at 296 and the references made in fn 51. For the opposite view see the reference in fn 50 to the views of Van der Merwe.

45 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 1983 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.

46 Act 2 of 2002, see sec 88.

47 Act 25 of 2002, see secs 51 and 52.

48 The Consumer Affairs Committee of the Department of Trade and Industry is undertaking an investigation in terms of sec 8(4) of the Consumer Affairs (Unfair Business Practices) Act 71 of 1988 into the role of the Credit Bureau Association with reference to its ability to enforce its existing Code as well as into credit bureaux and their compliance with the Code. The investigation will also consider whether the existing Code should be amended. Report 97 was published in the Government Gazette in May 2003. Comments are being considered at present.

African legislation.[49]

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 data 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 data protecting laws and was adopted by the European Union to ensure compliance with its data protection regime. A variation of these laws, which is described as a co-regulatory model, was adopted in Canada and 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 data 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 - protections therefore frequently lag 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.

---

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.

50 Exposition as set out in EPIC Report 2002 at 3-5.

51 See discussion in Ch 7 below.

c) Self-regulation

Data protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. However, in many countries, 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, data 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. These include encryption, anonymous remailers, proxy servers and digital cash.[52] Users should be aware that not all tools are effective in protecting data privacy. Some are poorly designed while others may be designed to facilitate law enforcement access.

1.2.27 The Commission will be putting forward these and other proposals for discussion and evaluation. It is clear that the process of establishing policy goes beyond the level of basic statutory data protection principles to include the ways in which these principles should be enforced, eg, through supervisory authorities.

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

---

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

53 Victorian Law Reform Commission at 6: The USA is currently 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.

consultation process is of such great importance in this investigation. [54]

1.2.29 On the other hand, business interests may be enhanced by a statutory data protection regime. Many countries, especially in Asia, have developed or are currently developing data protection laws in an effort to promote electronic commerce. These countries recognise that consumers are uneasy with the increased availability of their personal data, particularly with new means of identification and forms of transactions, and therefore that their personal information is being utilised worldwide. Data 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 legislation[55] will ensure South Africa's future participation in the information market, if it is regarded as providing "adequate" data 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]

---

54 The Hon Justice Michael Kirby AC CMG in a foreword to Bygrave states that when a completely new problem comes along, the legal mind is often paralysed for a time. Attempts are made to squeeze the problem into old familiar bottles. And when this does not work, attempts are made to create new receptacles by analogy with those that seem most suitable.....Not only is the legal mind resistant to the idea of new approaches to new problems. The institutions of lawmaking are often highly inflexible. Typically, the emerging issues are complex, beyond the easy comprehension of the elected lay people who sit in the legislatures and even the overworked 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 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") at 499.

57 Piller at 7.

58 Bennett at 28.

1.3 Scope of the inquiry

Terms of reference

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 will therefore be 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. Processing of information generally refers to the collecting, storing, using and communicating of information.

Automatic and manual files

1.3.3 The investigation will cover both electronic and manual files. From the definition in the Open Democracy Bill 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.

1.3.4 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.

It should however be noted that in the Electronic Communication and Transactions Act, 2002 paper based databases are not included.[59]

---

59 The Electronic Communications and Transactions Act 25 of 2002 (hereafter referred to as "ECT 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.

Natural v juristic persons

1.3.5 The applicability of the Bill of Rights to a juristic person is set out 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.'

1.3.6 The courts apply the common law principles developed for the protection of the privacy of natural persons also to juristic persons. [60]

1.3.7 In ***Investigating Directorate: Serious Economic Offences ao v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty) Ltd ao v Smit NO ao***[61] it was held that although juristic persons enjoy the right to privacy, it is not protected to the same extent as that of natural persons. 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.

1.3.8 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" [62] is defined

---

60 See ***Motor Industry Fund Administrators (Pty) Ltd ao v Janit* ao**1994 (3) SA 56 (W) at 60 (confirmed on appeal: 1995 (4) SA 293 (A)) and ***Financial Mail (Pty)Ltd ao v Sage Holdings Ltd ao*** 1993 (2) SA 451 (A) 462-463. Neethling ***Persoonlikheidsreg*** 40 fn 331, 85 ff 89-91.

61 2001 (1) SA 545 (CC) .

62 "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.

as information about an identifiable individual. [63] The definition of "personal information" in the Electronic Communications and Transactions Act is based on that of PAIA.

Public v private sector

1.3.9 This investigation will deal with both sectors.

Critical data

1.3.10 The EU Directive stipulates that the processing of critical data shall be excluded from the data protection principles. This relates to processing -

> in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law .

1.3.11 In South Africa the ECT Act[64] grants to the Minister of Communications the power to determine what constitutes a critical database, but the regulations in this regard are yet to be drafted.

1.3.12 It may be premature, at this stage, to exclude critical databases from the data protection principles. The more critical the data, the more important it will be to ensure that the personal information collected is correct. Some of the data principles may therefore perhaps be applicable.

Household activity

1.3.13 Legislation will not cover personal information kept by a natural person in the course of a purely personal or household activity.

---

63 Roos at 499.

64 Sec 53 of Act 25 of 2002. See Ch 2 below.

1.3.14 The Commission's proposal is that the investigation into the protection of personal information should as a starting-point include:

a) Automatic and manual 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 data.

Personal information kept in the course of a purely personal or household activity will be excluded. Critical data is included at this stage pending consultation in this regard.

Comment is invited in all instances

1.3.15 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.

1.3.16 The Victorian Law Commission in Australia has recently published an Information Paper entitled "Privacy Law: Options for Reform".[65] In this paper it 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 existing laws in order to determine which of those areas the 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.

65 Victorian Law Reform Commission at 4.

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.

1.3.17 It is clear that information privacy overlaps with all of these areas in so far as problems of regulating the collection, storage, use and dissemination of the information gained as a result of the intrusions referred to (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.

1.4 Methodology

1.4.1 The issues raised need to be debated thoroughly. The comments of all parties who are interested in these issues are therefore of vital importance to the Commission. The publication of this issue paper for information and comment is the first step in the consultation process. The problems that have given rise to the investigation will be explained and possible options for solving these problems will be pointed out.

1.4.2 The manner in which the investigation will progress will depend primarily on the responses received from interested parties. Respondents may also raise new issues that fall outside this issue paper.

1.4.3 In this paper the present position regarding the protection of data in South Africa will be discussed. However, data processing operations increasingly extend across national borders. The way in which they are to be regulated should therefore not occur without consideration of the way in which they are regulated in a wide variety of countries, such consideration being one precondition for achieving harmonised regulation. Finally, a cross-national perspective is analytically fruitful given the fact that all countries' data protection laws are based upon and embody a set of broadly

similar principles. [66]

1.4.4 Recommendations will be made 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 issue paper will later be followed by a discussion paper containing draft legislation and a report with the Commission's final recommendations and proposed legislative proposals. The Law Commission will also be organising regional workshops at which members of the Project Committee will be present to explain and discuss proposed solutions and to note comments.

66 Bygrave at 12.

CHAPTER 2: TERMINOLOGY, DEFINITIONS AND CONCEPTS

2.1 In this investigation the Commission is embarking on what for many people will be new and unknown territory. It was therefore decided to include a chapter right at the outset of this issue paper, explaining important and interesting terms and concepts that will be used throughout the investigation. Some of these concepts may eventually find their way into the definitions section of the proposed legislation. Others will form part of a Glossary of Terms at the back of the eventual report. **Commentators are encouraged to comment on the correctness and clarity of interpretation in each case.** The concepts have been listed alphabetically.

Aggregate information

2.2 Aggregate information is used to show the total number of visits made to a website at any given time. It also indicates which parts of the site are used the most. Aggregate information does not identify individuals, as it does not contain any personal data. The information ostensibly helps in developing the website and improving the service offered.[1]

Anonymised data

2.3 Data from which a person cannot be identified by the recipient of the information. The name, address and full post code must be removed together with any other information which, in conjunction with other data held by or disclosed to the recipient, could identify the person. ID numbers or other unique numbers may be included only if recipients of the data do not have access to the "key" to trace the identity of the person using the number.

Biometrics

2.4 Techniques of personal identification that are based on physical characteristics. Biometric

---

[1] Office of the Data Protection Register Isle of Man "Privacy Policy" available at http://www.gov.im/odpr/privacypolicy.html accessed on 2/4/2002 (hereafter referred to as "ODPR Isle of Man") at 1.

techniques include fingerprinting, retinal scanning and voice recognition.[2]

Cookies

2.5 A cookie is a small amount of information (small numeric text file) recording details of a person's (subject's) visit to a website, but without identifying the person. The cookie is created by the web server on the hard drive of the subject's personal computer.[3] The file can be accessed and read by the website at each return visit. Any information provided through the cookie is held on the web server and not on the subject's machine.[4]

2.6 Cookies are used for purposes such as allowing subjects to re-visit a site without having to re-enter login names and passwords. Using the cookie therefore has the advantage for subjects that they don't have to remember their user names and passwords each time they enter.[5]

2.7 The cookie may furthermore store lists of items the subject selected on an earlier visit to a virtual store and can therefore tailor products or advertisements to the subject's interests.[6] Cookies may be used to track registered and unregistered subjects as they travel through the site - for instance cookies may be used to count the number of unique subjects who are accessing the site over a particular period of time, or to ensure that you don't see a particular advert more than once. The use of cookies may help to make the system more efficient. [7]

2.8 There is, however, concern about the potential abuse of cookies. Cookies are stored in the subject's computer without his or her consent or knowledge. Information from the cookie is furthermore transmitted to the website, again without the subject's knowledge. Concerns have also

---

2 Victorian Law Reform Commission at 55.

3 ODPR Isle of Man at 1.

4 telegraph.co.uk (Telegraph Group Limited (TGL) and its subsidiary Hollinger Telegraph Ne Media (HTNM) published on the Internet) **Privacy Policy** Tuesday 5 March 2002 available at www.telegraph.co.uk.htm (hereafter referred to as "Telegraph Privacy Policy")

5 Telegraph Privacy Policy.

6 Victorian Law Reform Commission at 55.

7 Telegraph Privacy Policy.

been raised about the possibility of cookies being written that would allow access to other information that the subject has stored. Advertisers and webmasters are also currently using cookies to develop detailed profiles of users and their browsing habits. The possibility exists for these profiles to be sold and resold to other commercial interests.

2.9 Due in part to these privacy issues, web browsers have now been designed to give subjects more control as to whether to allow cookies on their disks. A subject may also require advertisers to obtain the subject's permission each time a cookie is being placed on the hard disk.

2.10 Cookies can be disabled in the user's browser. [8] Firewalls set up by a company network may also prohibit the use of browser cookies.[9] It has, however, been found that in some instances access is denied to a site once the cookies connected to that site have been disabled.

Critical data

2.11 Data that is declared by the Minister in terms of sec 53 of the ECT Act to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens. [10]

Cryptography

2.12 Cryptography is a discipline that embodies the principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use. It is therefore one of the tehnological means to provide security for data on information and communication systems.[11] It is therefore the practice of digitally " scrambling " a message using a secret key or

---

8 Telegraph Privacy Policy; If a person does not want to receive cookies or if he or she would prefer to be prompted first, he or she should check the settings in the "Internet Options" of the web browser. If a user is not sure on how to check or alter these settings, the software provider or support engineer should be contacted.

9 Telegraph Privacy Policy.

10 ECT Act.

11 Lawack-Davids VA "The Cryptographic Dilemma: Possible Approaches to Formulating Policy in South Africa" ***Obiter*** Vol 22 1 2001 at 2 and the references made therein.

keys. [12] It may also refer to the study of analysing and deciphering codes.

Cyberspace

2.13 The electronic "space" or "place" created by computer networks where online activities take place; often contrasted with the physical world where "offline" or "real life" activities occur.[13]

Data

2.14 The Common Wealth Model Law for private entities define data as information which -

(a) is recorded with the intention that it should be processed;[14] or

b) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

2.15 The ECT Act, however, restricts the definition of data for the purposes of that Act to "electronic representations in any form."[15]

2.16 Examples of the nature of data collected are for instance information on companies, economic trends, or socio-political issues. It could also be personal information: address, marital status, salary, driving, and employment history; corporate affiliations, who a person's neighbours are; vehicle and real estate holdings, civil and criminal court records.[16] Less than scrupulous brokers may even collect legally shielded data such as credit and phone records, as well as information regarding arrests that did not result in convictions. Medical records, banking, tax, insurance and credit records are top of the list of data that should be better protected.[17]

---

12 Department of Communications ***Making IT your business*** Green paper on E-commerce November 2000 (hereafter referred to as "Greenpaper") at 109.

13 Victorian Law Reform Commission at 55.

14 Recording data may be seen as the first step in processing data.

15 ECT Act referring to Canadian Uniform Electronic Evidence Act.

16 Piller at 4.

17 Piller at 5.

Data bank

2.17 The use of electronic computers for storing data.[18]

Data collector

2.18 Any public or private body who electronically or manually requests, collects, collates or stores personal data from or in respect of a data subject. Also referred to as a data processor.[19]

Data user[20] (or data medium[21] or data controller[22])

2.19 A data user is the person through or on behalf of whom the data is processed and who controls the use and content of the data (for his own purposes or that of another). It is therefore the person or organisation who determines the purposes and means of data processing. The user need not be in possession of the data; the crucial criterion is control.[23] The distinctions between different roleplayers are not hard and fast. In some instances the data user may also function as the data processor.

2.20 A distinction must, however, be made between a data user and a so-called computer bureau which would fall under the definition of a data collector. A computer bureau is the person who either:

(a) acts as an agent of the data user and processes the data on behalf of the latter; or

---

18 McQuoid-Mason DJ ***The Law of Privacy in South Africa*** Juta & Co Ltd Johannesburg 1978 (hereafter referred to as "McQuoid-Mason") 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.

19 ECT Act only refers to electronically collected data.

20 Bygrave at 21.

21 Neethling ***Huldigingsbundel WA Joubert*** at 105 fn 3 refers to the data user as a "data medium".

22 Bygrave at 21.

23 Bygrave at 21.

(b) allows his equipment to be used by a data user for the processing of data[24]

Data processing

2.21 For the purposes of this discussion the processing of data means the storage, arrangement, amendment, use, communication and deletion of personal data:

a) Storage includes the recording, acquisition, collection, reception, consultation, collection, retention or retrieval of data for the purposes of further use;
b) Amendment means the extension, rearrangement or changing of the meaning of stored data;
c) Deletion refers to the destruction of stored data; and
d) Communication refers to the transfer or disclosure of stored data to any third party.

Data protection

2.22 Data protection entails the legal protection[25] of a person (the *data subject*) with regard to the processing of data[26] concerning him, her or itself [27] by another person or institution (the data medium/user).

2.23 This concept to be distinguished from data security. See below.

Data security

2.24 Data security pertains to a broader range of concerns than data protection. Whereas the

---

24 Bygrave at 21.

25 See generally Neethling ***Huldigingsbundel WA Joubert*** at 105 *et seq* for a discussion of private law protection relevant in this regard.

26 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 ***Huldigingsbundel WA Joubert*** at 105 fn 2.

27 Neethling ***Huldigingsbundel WA Joubert*** at 105 fn 3.

primary goal of the latter is protection of data subjects' personal privacy, data security is also very much concerned with safeguarding the interests of users and processors of all kinds of data (not just personal data), inter alia for consideration for national security, commercial profit or administrative efficiency. Data security measures are mainly directed to ensuring that data are processed in accordance with the expectations of those who steer or use a given information system. The chief sub-goals for these measures are maintenance of confidentiality, integrity/quality and availability of information in information systems as well as appropriate protection of the system itself. See Steinmuller's more simplistic formulation: "whereas data protection protects against data processing, data security simply protects data processing".[28]

Data subject

2.25 Any natural (or juristic) person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act.[29]

De-identify

2.26 In relation to personal information of an individual, means to remove any information that–

(a) identifies the individual;

(b) can be manipulated by a reasonably foreseeable method to identify the individual; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the individual or that can be used or manipulated by a reasonably foreseeable method to identify the individual.[30]

Digital

2.27 The representation of data by the bits and bytes of binary code. Vinyl records and cassette

---

28 Bygrave at 23.

29 ECT Act.

30 Commonwealth Secretariat ***Model Privacy Bill for Public Sector*** LMM(02)7 November 2002 (hereafter referred to as "Model Bill").

music tapes carry analogue media.[31]

Disclose

2.28 In relation to personal information in the custody or under the control of the data user, means to make the information available to a person or an organisation that is not an employee of the data user, and “disclosure” has a corresponding meaning.[32]

Disclosure Notice

2.29 A disclosure notice discloses a data user’s data protection policy and gives consumers an opportunity to "opt out" of the exchange of marketing data. It shows consumers and legislators that the data user respects their concerns regarding privacy, the environment, or the receipt of unwanted mail. The opportunity to opt out should be made as soon as possible at the beginning of the relationship, and before information is shared with third parties. Notices come in different type sizes and with different language,[33] but normally include an explanation of the data user’s list usage policy, even in instances where no information is disclosed to third parties. Notices are generally included in consumer information sections, on order forms and applications, on the bottom of the first page of the solicitation, or in invoice stuffers.

Document

---

31 Greenpaper at 21.

32 Model Bill.

33 The Direct Marketing Association provides members with the following examples of Disclosure Notices:
Example A: If you decide you no longer wish to receive our catalogue send us your mailing label indicating your request. Likewise, if you prefer not to have your name passed on to other mailing list companies, simply tell us and we’ll respect your wishes.
Example B: We make your name and address available to other companies whose products and services may interest you. If you prefer not to receive such mailings please tick the box alongside and return this mailing to...
Example C: If you prefer not to have your name[passed on to other marketing companies, please let us know. We’ll make sure your name goes no further than....
Example D: We occasionally make lists of our customers available to carefully screened marketers of quality goods and services. If you do not wish to receive such offers simply call 0800....
Example E: We will not share your personal information with any organisation outside of the XYZ group of companies. If you would like us to stop sending you our marketing information tick the box alongside.
Example F: Thank you for completing this application. If you do not wish this information to be shared with pother reputable companies, check here.....

2.30 Any medium in which information is recorded, whether printed or on tape or film or by electronic means or otherwise and includes any map, diagram, photograph, film, microfilm, video-tape, sound recording, or machine-readable record or any record which is capable of being produced from a machine-readable record by means of equipment or a programme (or a combination of both) which is used for that purpose by the data user (public authority) which holds the record.[34]

EDI (Electronic Data Interchange)

2.31 A de facto standard format for exchanging business data between companies. It is a computer application in a standardised form, but usually refers to a proprietary system of delivery.[35]

Electronic

2.32 Includes created, recorded, transmitted or stored data in digital or other intangible form by electronic, magnetic, optical or any similar means.[36]

Encryption

2.33 The coding of data for the purpose of security or privacy .

Filing system

2.34 Any structured set of personal data which are accessible according to specific criteria (eg date of birth and name).

Firewall

2.35 Firewalls is the name given to a set of related programmes that protects the resources of

---

34 Sec 4 (Interpretation) of the Model Bill refers to “public authority” as the applicable data user.

35 Green Paper at 109.

36 ECT Act (supporting documentation) referring to the Manitoba Electronic Commerce and Information Act.

an intranet by ensuring that users of other networks (ie outsiders) do not gain access to the intranet.[37]

Hacking

2.36 To gain access to a computer file or network illegally or without permission.[38]

Hosting

2.37 The storage and maintenance of the data making up the content of websites.[39]

Identity

2.38 Identity constitutes the uniqueness of a person which identifies him as a particular person and thus distinguishes him from others; identity is made up of various *indicia* through which a person may be recognised for who he/she/it is, and that identity is infringed if such *indicia* are used in a manner which cannot be reconciled with the true personality image of the person in question.

Information

2.39 It is a very complex and multi-layered concept. [40] It includes all forms and types of financial, business, scientific, technical, economic or engineering information including patterns, plans, compilations, program devices, formulas designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and stored or compiled in digital or electronic format. The term is sometimes used interchangeably with "data".

Information practices

---

37 Kang T "How Does the Internet Work?" March 1 2001 in Module I Return to Privacy in 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.

38 Victorian Law Reform Commission at 56.

39 Green Paper at 21.

40 Bygrave at 20.

2.40 In relation to a data user, means the policy of the data user for actions in relation to personal information, including -

(a) when, how and the purposes for which the data user is to collect, use, modify, disclose, retain or dispose of personal information;

(b) the administrative, technical and physical safeguards and practices that the data user maintains with respect to the information.

Information system

2.41 A system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet.[41] It therefore encompasses computer and communication facilities and networks, and data/information processed by them including programmes, specifications and procedures for their operation. IS can also refer to the technical infrastructure that facilitates and structures the processing of data/information.[42]

Information system services

2.42 Includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a data user, and the processing and storage of data, at the personal request of the recipient of the service.[43]

Internet Service Provider (ISP)

2.43 A company that provides persons with access to the Internet.[44]

---

41 ECT Act (supporting documentation) referring to the Uncitral Model Law.

42 Bygrave at 20.

43 ECT Act.

44 Victorian Law Reform Commission at 56.

Intranet

2.44 An intranet is a type of local area network(LAN) that is set up as an in-house website that serves the employees of a given company or business.

Media Preference Service (MPS)[45]

2.45 The MPS is a database of information about individuals who have requested to be excluded from mail, fax and telephone marketing. The service is managed and administered by the Direct Marketing Association and is provided at no cost to DMA members. Each quarter a copy of the database is made available to subscribers. This file copy is used by data users to flag the records on their own databases of persons who have registered with the MPS. The flagging enables companies to prevent the use or disclosure of these persons' information for marketing purposes.[46]

2.46 There are three distinct areas of consumer preference:

- Mail Preference Service: allows consumers to opt out of receiving unwanted direct mail;
- Telephone Preference Service: allows consumers to restrict unwanted telemarketing calls;
- Fax Preference Service: provides for the suppression of fax marketing.

2.47 The DMA is investigating the creation of an international E-mail Preference Service in conjunction with the International Federation of Direct Marketing Associations (IFDMA), of which the DMA is a founder member. In addition, attention is currently being paid by the DMA to the development of a means to manage unwanted SMS marketing messages.

Personal data [47]

---

45 Direct Marketing Association of South Africa "The Privacy File" April 2001.

46 The Media Preference Service offers benefits to both marketers and consumers. From a consumer perspective the MPS affords consumers the right to marketing privacy at a national level. The marketer, on the other hand, is able to use the MPS to demonstrate his commitment to consumer privacy, and to remove from his marketing lists those consumers who do not wish to be contacted. At a macro level the MPS is a visible demonstration of the industry's commitment to pro-active privacy protection. The service also acts to silence privacy zealots who may promote stricter privacy legislation.

47 EU Directive.

2.48 Any information relating to an identified or identifiable natural (or juristic) person. An identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Sometimes used interchangeably with personal information. See the definitions of personal information in the ECT Act and PAIA.[48] The Common Wealth definition differs only slightly in so far as the Model Laws for public and private bodies are concerned.[49]

Privacy

2.49 Neethling [50] defines "privacy" as follows:

---

48 "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.

49 The following is the definition as found in both model laws, with references to the relevant changes:
Information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing –
- a) information relating to the race, national or ethnic origin, religion, age or marital status 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 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;
- (f) correspondence sent ["to a public authority" - these words only found in the Model Law on public bodies] by the individual that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence; or
- (g) the views or opinions of any other person about the individual;
- ["(h) information that can be manipulated by a reasonably foreseeable method to identify the individual; or
- (i) information that can be linked by a reasonably foreseeable method to other information that identifies the individual or that can be manipulated by a reasonably foreseeable method to identify the individual;" - subparas (h) and (i) only found in the Model Law on private bodies]

50 ***Neethling's Law of Personality*** at 36; See full discussion in Ch 3 below.

> Privacy is an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself or herself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he or she evidences a will for privacy.

2.50 This court referred to this definition with approval in ***National Media Ltd ao v Jooste*** [51] and ***Bernstein ao v Bester ao NNO***. [52] See also references in ***Universiteit v Pretoria v Tommie Meyer Films (Edms) Bpk*** [53] and ***Swanepoel v Minister van Veiligheid en Sekuriteit***.[54] The Constitutional Court also includes autonomy under the concept of privacy.[55]

Privacy policy

2.51 The privacy policy explains what information the data controller collects and the purpose for which that information is used.

Private body[56]

2.52 A private body is:

- A natural person who carries on or has carried on any trade, business or profession, but only in such capacity;
- A partnership which carries on or carried on any trade, business or profession; or
- Any former or existing juristic person, but not a public body.

Profiling

2.53 The compilation of information, usually from a variety of sources (such as Internet sites visited, items purchased, public records), to create a profile of a particular person. Profiling involves

---

51 1996 (3) SA 262 A 271.

52 1996 (2) SA 751(CC) 789.

53 1977 (4) SA 376(T) 314.

54 1999 (4) SA 549 T 553.

55 ***Case ao v Minister of Safety and Security ao; Curtis v Minister of Safety and Security ao*** 1996 (3) SA 617 CC 656.

56 ECT Act.

the inference of a set of characteristics (typical behaviour) about a person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics.[57] This profile is often used to market products to that person.[58]

Public authority

2.54 This may include –

(a) a House of Parliament or a committee of any House of Parliament;
(b) the Cabinet as constituted under the Constitution;
(c) a Ministry, a department or division of a Ministry, or the private office of a Minister, wherever located;
(d) a local authority;
(e) a public statutory corporation or body;
(f) a body corporate or an incorporated body established for a public purpose, which is owned or controlled by the state;
(g) any other body designated by the Minister by regulation made under this Act, to be a public authority for the purposes of this Act.

Public body

2.55 A government department, ministry or organ of State[59] including

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;

---

57 Bygrave at 1.

58 Victorian Law Reform Commission at 57.

59 ECT Act.

(ii) exercising a power or performing a function in terms of any legislation.[60]

Public domain

2.56 Information is in the public domain when it is not confidential, when it is legally available for anyone to use and may be freely copied and used. It is information that has been made available to the general public and can be distributed and redistributed without copyright or patent.

Public records

2.57 The records of organisations that are accessible by the general public. Examples include court records and planning applications held by local councils. [61]

Public registers

2.58 Public registers are lists that are required to be made available to the public by legislation or regulation. Examples include the Motor Vehicle Register, the Land Titles Register and the Births, Deaths and Marriages Register.[62]

Record

2.59 Data that is recorded or stored on any medium in or by an information system or other similar device that can be read or perceived by a person or an information system or other similar device. It includes a display, printout or other output of that data.

Relevant filing system

2.60 Any set of information relating to persons to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for

---

60 ECT Act.

61 Victorian Law Reform Commission at 58.

62 Victorian Law Reform Commission at 58.

that purpose, the set is structured, either by reference to persons or by reference to criteria relating to persons, in such a way that specific information relating to a particular individual is readily accessible.

Screen scraping

2.61 Lifting content from commercial sites (especially of competitors) and using it for own purposes.

Search engine

2.62 A remotely accessible computer programme that enables keyword searches for information on the Internet to be performed.[63]

Second click[64]

2.63 This is a navigation programme to download to the Internet user account, unsolicited banners. With the first click the Internet user consciously obtain information during a visit. The second click is done by the navigation programme, towards an invisible site, unknown to the user, telling many details about the user's behaviour.

Service provider[65]

2.64 Entity that provides the connections for information systems, or provides information system services or access; or operates facilities for such services or access, or transmits or routes data messages between or among points specified by a data user; but excludes the modification to data or data messages sent or received.

---

63 Victorian Law Reform Commission at 58.

64 Dinant J-M "The Arrival of the New Internet Network Numbering System and its Major Risks to Data Protection" Presentation at the 23rd International Conference of Data Protection Commissioners, Paris, 24-26 September 2001.

65 ECT Act .

Smart card

2.65 Card containing memory and a microprocessor, that can serve as personal identification, credit card, ATM card, telephone credit card, critical medical information record and as cash for small transactions.[66]

Sniffing

2.66 The use of computer hardware and/or software to search for designated keywords. For example, a sniffing programme could be used to search a person's e-mail for any mention of the word "drugs".[67]

Transaction

2.67 A transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services.[68]

Transborder data flow

2.68 The movement of information or computer data across national or state boundaries.[69]

Unique identifier

2.69 An identifier (usually a number) assigned by an organisation to a person uniquely to identify that person for the purposes of the operations of the organsation but does not include an identifier that consists only of the person's name.[70]

---

66 Green Paper at 22.

67 Victorian Law Reform Commission at 58.

68 ECT Act.

69 Victorian Law Reform Commission at 58.

70 Victorian Law Reform Commission at 59.

World Wide Web

2.70 An information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer.[71] (Tim Berners-Lee : inventor of the Web).

World Wide Web Consortium (W3C)[72]

2.71 The W3C was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C has around 500 member organisations from all over the world and has earned international recognition for its contributions to the growth of the web. One of the long terms goals for the Web is to guide the Web's development with careful consideration for the novel, legal, commercial, and social issues raised by this technology.

---

71 ECT Act.

72 World Wide Web Consortium (W3C) "About the World Wide Web Consortium (W3C)" available at http://www.w3.org/Consortium/accessed on 4/11/2002.

CHAPTER 3: PRIVACY

3.1 Recognition of the right to privacy

3.1.1 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.

3.1.2 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]

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

---

1 ***Neethling's Law of Personality*** at 33; also Neethling ***Persoonlikheidsreg*** at 36-37.

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 on April,28 2001 and made available at the 23rd International Conference of Data Protection Commissioners in Paris in Sept 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 intentional concealment of personal information does not always amount to lying: the hallowed example is the secret ballot.

3 See Neethling ***Persoonlikheidsreg*** at 52, 55, 57 for the position in the Roman and Roman-Dutch law. EPIC 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 Moore B ***Privacy: Studies in Social and Cultural History*** 1984. Jewish law has long recognised the concept of being free from being watched. See 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 Philipines, 1987), Russian Federation (art 23, Constitution of the Russian Federation,1993). While the Constitution of the United States of America does not contain an explicit right to privacy, the Courts in that country, going back as far as 1891 (***Union Pacific R.R Co v Botsford***, 141 US 251 11 S.Ct 1000, 35 L.Ed 734(1891) have interpreted the Constitution as providing a right to personal privacy. The UK has recently enacted general human rights legislation that protects the right to privacy in their Human Rights Act, 1998 (UK).

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

3.1.4 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]

3.1.5 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

---

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

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

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

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

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

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

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

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

(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks.

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

Fundamental Freedoms 1950 [11] states:

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

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

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

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

3.1.6 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]

3.1.7 In South Africa the right to privacy is protected by both our common law[17] and the

---

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

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

13 Approved by the Ninth International Conference of Amercian 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 October,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 the EPIC Report 2002 at 7 and the references made therein.

17 See Neethling ***Persoonlikheidsreg*** Ch 8; ***Neethling's Law of Personality*** Ch 8.

Constitution.[18] The Constitutional Court[19] has emphasised the interdependency between the common law and constitutional right to privacy. A fundamental issue at stake, however, concerns the extent to which the Bill of Rights has application in common law disputes.

3.1.8 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]

3.1.9 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]

3.1.10 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

---

18 See discussion below.

19 ***Bernstein ao v Bester ao NNO*** supra at 787 ff.

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 ***Persoonlikheidsreg*** at 68-69; 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") 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).

(sec 39(2)).[22]

3.1.11 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]

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

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

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

---

22 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 ***Persoonlikheidsreg*** at 94-95.

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

25 Neethling, Potgieter & Visser ***Delict*** at 22-23.

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

3.1.14 In ***Bernstein ao v Bester ao NNO*** [29] in deciding whether secs 417 and 418 of the Companies Act[30] 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]

3.1.15 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

---

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

27 McQuoid-Mason DJ "Privacy" in Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D & Woolman S (eds) ***Constitutional Law of South Africa*** Juta Kenwyn 1996 Revision Service 5 1999 (hereafter referred to as "McQuoid-Mason in Chaskalson et al") 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 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 ***Persoonlikheidsreg*** at 268 ff, 288 ff).

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 and the ECT Act also have interim provisions dealing with the correction of data and the voluntary adherence to data protection principles respectively. These sections are being regarded as interim measures until the Data Protection Bill has been finalised. The Department of Trade and

law and the Constitution.

3.1.16 In terms of the common law every person has personality rights such as the rights to physical integrity, freedom, reputation, dignity, and privacy.[34]

3.1.17 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.***[35]

3.1.18 In this case Watermeyer AJ correctly interpreted[36] 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".[37]

Industry is also considering whether regulations should be formulated to regulate the credit bureau industry. 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 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 See Neethling ***Persoonlikheidsreg*** at 64, 103, 137, 157, 233, 265.

35 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 ***Persoonliheidsreg*** at 63-64, 265; Joubert WA "Die Persoonlikheidsreg: •n Belangwekkende Ontwikkeling in die Jongste Regspraak in Duitsland" 1960 ***THRHR*** 23 (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 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.

36 Various writers agreed: Neethling ***Persoonlikheidsreg*** at 63-64, 265; cf also McQuoid-Mason at 124-125.

37 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*** supra 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 . . ."

3.1.19 Very important is the fact that the court, in following ***Foulds v Smith***,[38] correctly rejected the view that contumelia in the sense of "insult" is the "essence of an injuria".[39]

3.1.20 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,[40] 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.[41]

3.1.21 It has, however, been argued[42] that the equation of privacy and dignity should be rejected and that the approach in ***O'Keeffe*** should be endorsed.[43] Many recent cases (also of the Appeal

---

38 1950 1 SA 1 (A) at 11; see also Neethling ***Persoonlikheidsreg*** at 63, 265.

39 Neethling ***Persoonlikheidsreg*** at 265 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).

40 Neethling ***Persoonlikheidsreg*** at 266 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 aconviction. (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.

41 Eg, in ***Kidson ao v SA Associated Newspapers Ltd*** 1957 (3) SA 461 (W) (see also ***Mhlongo v Bailey ao*** 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).

42 See Neethling ***Persoonlikheidsreg*** at 63, 267; Joubert 1960 ***THRHR*** at 41.

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

Court) have by implication followed this approach. [44] Even the Constitutional Court in ***Bernstein ao v Bester ao NNO*** [45] 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.

3.1.22 The conclusion is therefore that, despite the decisions equating privacy with dignity (or honour), it can safely be accepted that nowadays the right to privacy is recognised by the common law as an independent right of personality[46] and that it has been delimited as such within the dignitas concept.[47]

3.1.23 The enactment of the Constitution,[48] with the express constitutional recognition of the right to privacy in sec 14, independent of the right to dignity in sec10,[49] furthermore confirms the independent existence of the right to privacy.[50] It hopefully finally lays to rest the possible equation of, and thus confusion between, these two personality rights.[51] 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

---

44 See ***Jansen van Vuuren ao NNO v Kruger*** 1993 (4) SA 842 (A) at 849 ; ***National Media Ltd ao v Jooste*** 1996 (3) SA 262 (A) 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 ***Persoonlikheidsreg*** at 267-268).

45 Supra at 789.

46 The decision in ***Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk*** 1977 (4) SA 376 (T) clearly confirmed this viewpoint. Mostert J stated (at 383-384): "Die reg op privaatheid is een van die verskyningsvorms van die breër groep persoonlikheidsregte. In ons regspraak is erkenning aan sowel persoonlikheidsregte as die reg op privaatheid as beskermde regte verleen." See again also ***Jooste v National Media Ltd*** 1994 (2) SA 634 (C); ***Financial Mail (Pty) Ltd v Sage Holdings Ltd*** 1993 (2) SA 451 (A); ***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.

47 In ***Jansen Van Vuuren ao NNO v Kruger*** 1993 (4) SA 842 (A) 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."

48 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.

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

50 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.

51 See Neethling ***Persoonlikheidsreg*** at 268 fn 27.

other rights.[52]

3.1.24 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.[53]

3.2 Nature and scope of the right to privacy

3.2.1 Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define.[54] Definitions of privacy vary widely according to context and environment.[55] In ***Bernstein ao v Bester ao NNO*** [56] Ackermann J stated:

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

3.2.2 The lack of a single definition should, however, not imply that the issue lacks importance. The need to understand the nature of the right to privacy in order to have legal certainty and protection has always been emphasised. Gross[57] warns that a lack of understanding could have the following effect:

---

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

53 See Neethling ***Persoonlikheidsreg*** at 327; 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.

54 EPIC 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.

55 EPIC 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).

56 Supra at 787-788.

57 "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.

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

3.2.3 In 1996 Harms JA accepted the following definition of privacy (as proposed by Neethling[58]) in ***National Media Ltd ao v Jooste***[59]

> Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private[60] (translation from the Afrikaans)

In the same year the Constitutional Court also referred to Neethling's definition in ***Bernstein ao v Bester ao NNO.***[61]

3.2.4 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.[62] If such a will for privacy is absent, then a person usually has no interest in the legal protection of his privacy.[63]

3.2.5 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;

---

58 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 36; Neethling ***Persoonlikheidsreg*** at 39-40.

59 1996 (3) SA 262 (A) at 271.

60 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*** supra 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.

61 Supra at 789.

62 ***Neethling's Law of Personality*** at 35. See also the discussion by Rautenbach 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.

63 See ***National Media Ltd ao v Jooste*** supra at 271. Rautenbach 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.

(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.

3.2.6 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.[64]

3.2.7 In ***Mistry v Interim Medical and Dental Council of South Africa ao***[65] 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.

3.2.8 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)[66].

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

3.2.10 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.

---

64 De Waal J, Currie I & Erasmus G ***The Bill of Rights Handbook*** 3ed Juta Kenwyn 2000 (hereinafter referred to as "De Waal et al") 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.

65 1998 (7) BCLR 880 (CC) at para 14.

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

3.2.11 For convenience the constitutional right to privacy can be divided into three[67] groups:[68]

(a) protecting privacy againt intrusions and interferences with private life;

(b) protecting privacy against disclosures of private facts; and

(c) protecting privacy against infringement of autonomy.

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

3.2.13 The protection of information privacy generally limits the ability of people to gain, publish, disclose or use information about others without their consent.[69] Individuals therefore have control not only over who communicates with them but also who has access to the flow of information about them.[70]

3.2.14 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.[71]

---

67 Cf De Waal et al 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.

68 McQuoid-Mason in Chaskalson et al 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 ao NNO*** supra at 789; ***Neethling's Law of Personality*** at 26; Neethling ***Persoonlikheidsreg*** at 40-41; McQuoid-Mason at 99, McQuoid-Mason in Chaskalson et al at 18—1, 18—8. See further ***Case ao v Minister of Safety and Security ao; Curtis v Minister of Safety and Security ao*** supra at 656 as regards protection of autonomy (Neethling ***Persoonlikheidsreg*** at 43).

69 McQuoid-Mason in Chaskalson et al 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.

70 McQuoid-Mason 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 ***Persoonlikheidsreg*** 40.

71 De Waal et al 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.

3.2.15 In terms of sec 39 of the Constitution,[72] 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.[73]

3.2.16 Of importance is Ackermann J 's dictum in ***Bernstein ao v Bester ao NNO*** [74] where he stated:

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

3.2.17 Earlier he explained it as follows:[75]

> 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.

---

72 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.

73 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 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.

74 Supra at 789.

75 At 788-789.

3.2.18 Neethling[76] 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.[77] Thus in principle compiling the data record and obtaining knowledge thereof constitutes an intrusion into the private sphere.[78]

3.2.19 His criticism was validated by Langa DP in ***Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty) Ltd ao v Smit NO ao***,[79] where the court held that the statements in ***Bernstein ao v Bester ao NNO*** 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.

3.2.20 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.[80]

3.2.21 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.[81] 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.[82] In each case a careful weighing up

---

76 See Neethling 1997 ***THRHR*** at 140.

77 See on this Neethling ***Persoonlikheidsreg*** at 326, ***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") at 392.

78 This view also appears by implication from the decision in ***S v Bailey*** 1981 (4) SA 187 (N) at 189-190. Here the court held that the compulsory furnishing of information to the state in terms of the 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.

79 2001 (1) SA 545 (CC).

80 Para 16 at 557.

81 See Neethling ***Persoonlikheidsreg*** at 288 ff.

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

of the right to privacy and the opposing interests or rights will have to take place.

3.2.22 Any data 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,[83] their fundamental right to access to information,[84] their fundamental right to freedom of expression,[85] as well as other legitimate interests or rights.

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

3.3 Infringement of the right to privacy

3.3.1 The elements of liability for an action based on an infringement of a person's privacy are 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.

---

83 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.

84 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.

85 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.

(1) 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.

3.3.2 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.[86]

3.3.3 Although it is possible that a new constitutional delict may emerge in future,[87] 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.[88] 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

3.3.4 For a common-law action for invasion of privacy based on the *actio iniuriarium* to succeed, the plaintiff must prove the following essential elements: (i) impairment of the plaintiff's privacy, (ii) wrongfulness and (iii) intention (animus iniuriandi).[89]

3.3.5 As shown above, the Constitutional Court has pointed out[90] 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?[91] [92] (b) If so, is such an infringement justifiable in terms of the

---

86 See discussion above.

87 See discussion above.

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

89 See McQuoid-Mason in Chaskalson et al at 18—2 and the references there.

90 ***Bernstein ao v Bester ao NNO*** supra at 790.

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

92 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.

requirements laid down in the limitation clause (sec 36) of the Constitution?[93] For this reason the Constitutional Court has cautioned against simply using common law principles to interpret fundamental rights and their limitations.[94]

3.3.6 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.[95] They should also be in harmony with the intrinsic values set out in the Constitution.[96] 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.[97]

(i) Invasion of privacy

3.3.7 The concept of privacy was defined earlier and applies to both common law and constitutional infringements of the right to privacy.[98] 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.[99]

3.3.8 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.[100] An individual's expectation of privacy must be weighed against the conflicting rights of the

---

93 ***S v Makwanyane ao*** supra at para 102.

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

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

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

97 See Neethling ***Persoonlikheidsreg*** at 67-70; Burchell ***Personality Rights*** at 416.

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

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

100 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 ***Persoonlikheidsreg*** at 268-269).

community. Such expectations may also be tempered by countervailing fundamental rights, such as freedom of expression or the right to access to information.[101]

3.3.9 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.[102]

3.3.10 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 data (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

3.3.11 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,[103] but also that such violation was contra bonos mores or

---

101 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 ao*** 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.

102 McQuid-Mason in Chaskalson et al at 18---4. Cf also the reference above fn 64 to infringement of autonomy.

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

unreasonable.[104]

3.3.12 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.[105] This view is also apparent in South African case law.[106]

3.3.13 It has been pointed out, however, that "legal protection of private facts is extended to ordinary or reasonable sensibilities and not to hypersensitiveness."[107] Therefore the courts will not protect facts whose disclosure will not "cause mental distress and injury to anyone possessed of ordinary feelings and intelligence".[108]

3.3.14 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.[109]

3.3.15 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, purport and

---

104 See Neethling ***Persoonlikheidsreg*** at 268-269, 329.

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

106 See eg ***S v A ao*** 1971 (2) SA 293 (T) 299 where Botha AJ set the limits of the right to privacy according to the "prevailing *boni mores* in accordance with public opinion". In ***Financial Mail (Pty) Ltd ao v Sage Holdings Ltd ao*** supra at 463 the Appelate Division held that "in demarcating the boundary between lawfulness and unlawfulness in the field, the Court must have regard to the particular facts of the case and judge them in the light of contemporary boni ores 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*** 1975 (1) SA 590 (RA) 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.

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

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

109 McQuoid-Mason ***Acta Juridica*** at 232 and the references therein. See also supra fn 96.

objects - will play a major role in determining the “new” boni mores of South African society.[110] 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.

3.3.16 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.[111]

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

Intrusion

3.3.18 A violation of privacy by means of an act of intrusion[112] 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.[113] 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

---

110 McQuoid-Mason in Chaskalson et al at 18---3.

111 See the discussion supra.

112 See Neethling ***Persoonlikheidsreg*** at 269 ff.

113 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 tales 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 ***Persoonlikheidsreg*** at 269-274.

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 data, viewed in isolation, is not "private" in the above sense. Thus in principle the compiling of a data record and obtaining knowledge thereof constitutes an intrusion into privacy.[114]

3.3.19 Generally speaking no person has to tolerate information concerning him being collected.[115] 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.[116]

3.3.20 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.[117]

Disclosure or revelation

3.3.21 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.[118]

3.3.22 It is important to note that the question of an infringement of privacy arises only if the plaintiff is identified with the disclosed facts.[119] If this element of identification is lacking, the

---

114 See Neethling ***Persoonlikheidsreg*** at 326.

115 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 ***Persoonlikheidsreg*** at 273).

116 See Neethling ***Persoonlikheidsreg*** at 329.

117 See Neethling ***Persoonlikheidsreg*** at 326, 329.

118 See Neethling ***Persoonlikheidsreg*** 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. as referred to by Neethling ***Persoonlikheidsreg*** 274. 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.

119 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.

disclosure does not relate to a specific person in his state of privacy.

3.3.23 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.[120]

3.3.24 As far as the first is concerned, if the storage of data is in principle wrongful, then it goes without saying – in view of the continuous nature of the wrongful conduct – that the communication thereof to third parties[121] should also be regarded as unlawful.[122]

3.3.25 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.[123] These examples mentioned should, however, not be regarded as a numerus clausus.[124] Whether a specific relationship deserves protection will depend entirely on the surrounding circumstances. Giesker[125] 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).[126] In such instances disclosure of the private facts will, besides breach of contract, also constitute an

---

120 See Neethling ***Persoonlikheidsreg*** at 274 ff.

121 Which amounts to a disclosure of private facts (see Neethling ***Persoonlikheidsreg*** at 329).

122 This view is supported by the rule that, eg, the disclosure of the contents of stolen private documents is wrongful (see Neethling ***Persoonlikheidsreg*** at 274).

123 See Neethling ***Persoonlikheidsreg*** at 278-280.

124 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.

125 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 ***Persoonlikheidsreg*** at 275-277.

126 See Giesker at 129 ff; Neethling ***Persoonlikheidsreg*** at 277. It is obvious that the agreement must be valid (Giesker at 142).

infringement of the right to privacy.[127]

3.3.26 Thirdly, the mass publication of private facts is in principle wrongful.[128] [129]

3.3.27 It stands to reason that the use and disclosure of false or misleading data should also be wrongful – that such conduct is contra bonos mores requires no argument.[130]

iii) Intention

3.3.28 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.[131] 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

---

127 Apart from confidential relationships, a duty not to disclose private facts in the present cirucumstances – ie where an outsider acquired authorised knowledge of the facts involved – may also arise in certain circumstances of authorised fixation or embodiment of the facts (by eg photography or tape-recording). Unauthorised disclosure of the embodied facts (eg the photograph) may then nevertheless be wrongful. An example can be found in ***Culverwell v Beira*** 1992 (4) SA 490 (W) where the alleged threatened disclosure of photographs of a naked woman taken by her lover was at stake. The court held that the woman had no legal basis to claim from her lover delivery of the photographs and negatives, or to prevent him from making copies from the negatives, since he was the owner thereof. She could not succeed merely because of the intimate and private nature of the photographs. However, the court by implication found that a disclosure of the photographs would be wrongful unless justified (see Neethling ***Persoonlikheidsreg*** at 277 fn 81). 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).

128 See Neethling ***Persoonlikheidsreg*** at 280 ff.

129 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 ***Persoonlikheidsreg*** at 285-286). 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.

130 See supra fn 113 as to violation of identity (see also Neethling ***Persoonlikheidsreg*** at 329).

131 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 at 100 ff; Neethling ***Privaatheid*** at 256-257.

wrongfulness). In the absence of any of these elements, there is no question of intent.[132] Where, for example, a person bona fide but incorrectly believes that she is entering her own hotel room, the intent to infringe privacy is certainly lacking[133] and she should go free.[134]

3.3.29 Animus iniuriandi is presumed as soon as wrongful infringement of privacy has been proved.[135] The defendant may then rebut the presumption.[136]

3.3.30 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.

3.3.31 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.[137] 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

---

132 Cf Neethling ***Persoonlikheidsreg*** at 70 ff, 303-304.

133 See also McQuoid-Mason 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).

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

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

136 As far as liability of the mass media for the infringement of privacy is concerned, cf 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.

137 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 injuriarium (McQuoid-Mason ***Acta Juridica*** at 261).

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.[138]

3.3.32 Neethling[139] is indeed of the opinion that the collection and use of personal data (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 intent in each case. However, as an alternative to strict liability, he proposes that negligence liability should also be considered.[140]

b) Defences/Justification

3.3.33 Defences to a common law action for invasion of privacy are similar to those for other actions under the actio iniuriarium.[141] 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.[142]

3.3.34 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).[143]

3.3.35 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.[144]

---

138 McQuoid-Mason ***Acta Juridica*** at 234.

139 See Neethling ***Persoonlikheidsreg*** at 333-334, 2002 ***THRHR*** at 584; infra chapter 5 para 3.2.

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

141 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.

142 See discussion above.

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

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

3.3.36. Sec 36 of the Constitution [145] is a general limitation clause and sets out specific criteria for the limitation of the fundamental rights in the Bill of Rights.[146]

3.3.37 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.[147]

3.3.38 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.

3.3.39 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

---

145 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
(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.

146 Sec 36 is a codification of the approach set out in ***S v Makwanyane ao*** 1995 (3) SA 391 CC; 1995 (6) BCLR 665 CC. 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.

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

whether a limitation is justifiable.[148] 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.[149]

3.3.40 The High Court has explained that the criteria should be applied as follows:[150]

> 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.

3.3.41 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.[151]

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

i) Defences excluding wrongfulness

3.3.43 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

---

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

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

150 ***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.

151 Cockrell at 3A10.

society.[152]

Consent

3.3.44 Consent to infringement of privacy is a unilateral act. Therefore it may be revoked at any time preceding the defendant's injurious conduct.[153] Consent can be given expressly or tacitly.[154]

3.3.45 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.[155] 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.[156]

3.3.46 Where a person has given valid consent to the processing of data 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 data is invalid if it is set as a condition of employment, or of the continuance of a contract of employment, by an employer.[157] It is a question of fact whether consent was given in a particular instance.[158]

Necessity [159]

---

152 See Neethling ***Persoonlikheidsreg*** at 69-70.

153 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.”

154 See Neethling ***Persoonlikheidsreg*** at 300.

155 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.

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

157 See Neethling ***Persoonlikheidsreg*** at 329-330; see also supra fn 151.

158 See Neethling ***Persoonlikheidsreg*** at 300.

159 See Neethling ***Persoonlikheidsreg*** at 289-290. 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 ***Persoonlikheidsreg*** at 300).

3.3.47 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.[160]

3.3.48 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.[161] The need to process data which infringes the privacy of "innocent" data subjects demonstrates a particular application of necessity[162] 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.[163]

3.3.49 For the processing of data to be deemed lawful under the present circumstances, the following requirements must be satisfied:[164]

(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.[165] The same notion also forms the basis of the view[166] that data may be processed only for one or more specified lawful purposes. Data processing can have a lawful purpose only if the object is to further or protect a legitimate interest;[167] 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

---

160 See Neethling ***Persoonlikheidsreg*** at 289; see also McQuoid-Mason at 233.

161 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 ***Persoonlikheidsreg*** at 330).

162 See Neethling ***Persoonlikheidsreg*** at 289-290, 330.

163 Apart from business interests, other private interests, such as scientific interests, may also justify the processing of data (cf Neethling ***Persoonlikheidsreg*** at 299).

164 Cf generally Neethling ***Privaatheid*** at 361-363, ***Persoonlikheidsreg*** at 330-332; cf also McQuoid-Mason 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).

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

166 See the comparative law discussion infra (chapter 6) with regard to “purpose specification” as data protection principle.

167 Which includes the public interest: see the discussion below.

of data is lawful – in other words, whether a legitimate interest is protected.

(ii) From the foregoing it follows that the data may be used or communicated only for the protection of the legitimate interest(s) involved,[168] and that the use of data 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 data is not in accordance with the defined purpose.[169]

(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.[170] A requirement which plays an important role in this regard is that the type and extent of the compiled data must be reasonably necessary for,[171] 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.[172] The defined or specified purpose thus also circumscribes the limits of data processing. The activities of credit bureaux may serve as an example. The purpose of these institutions is to process data for the protection of business interests in creditworthiness; thus only data 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.[173] If information which is unnecessary for the protection

---

168 See the comparative law discussion in Ch 6 with regard to "limitation" as data protection principle. The ground of justification priviledged occasion may also be applicable here (see Neethling ***Persoonlikheidsreg*** at 302, 331 fn 86; see also McQuid-Mason in Chaskalson et al 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 excercise or protection of a right (see Neethling ***Persoonlikheidsreg*** at 331 fn 86).

169 A further principle flowing from this is that unauthorised access to processed data by a third party should in principle also constitute a wrongful intrusion into the privacy of the individual involved, even though such outsider may have a legitimate interest in the data. See Neethling ***Huldigingsbundel WA Joubert*** at 118 fn 90 91, ***Persoonlikheidsreg*** at 331 fn 87.

170 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 at 64 ff); cf also the discussion of ***Gosschalk v Rossouw*** supra at 490-492 in Neethling ***Persoonlikheidsreg*** at 293 fn 180; infra fn 175.

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

172 See the comparative law discussion in Ch 6 with regard to "minimality" as data protection principle.

173 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)

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 data is generally not reasonably necessary for the protection of a legitimate interest. Therefore data may not be stored or used for longer than is reasonably necessary for the specified purpose.[174]

(v) The bounds of reasonableness in relation to protecting a legitimate interest are also exceeded if data which has been obtained in an unlawful manner (such as by reading private documents, illegal wire-tapping or shadowing a person) is processed.[175] Put differently, on account of the continuing wrongfulness in these instances, such data 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

3.3.50 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.[176]

3.3.51 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.[177] Obviously,

---

(cf Neethling ***Persoonlikheidsreg*** at 290-291).

174 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 at 84 fn 88).

175 See the comparative law discussion in Ch 6 with regard to "fairness and lawfulness" as data protection principle. See also the discussion supra.

176 See Neethling ***Persoonlikheidsreg*** at 292-293, 332-334.

177 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 Post Office Act 44 of 1958. The

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.[178] 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.[179]

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

3.3.53 In order for the collection and processing of data 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.[180]

(i) First, the state must be expressly authorised by a valid statutory provision to process

---

state is also empowered by statute to gather and use personal information (see eg ***S v Bailey*** 1981 (4) SA 187 (N) at 189-190 on the powers in terms of the Statistics Act 66 of 1976 in this regard - see also Neethling ***Persoonlikheidsreg*** at 325) and (in terms of the Criminal Procedure Act 51 of 1977) to search persons and homes (see on this McQuoid-Mason at 136-141). For further examples of statutory powers justifying a violation of privacy, see in general McQuoid-Mason 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.

178 Cf Neethling ***Persoonlikheidsreg*** at 292-293.

179 A important case in this regard is ***Gosschalk v Rossouw*** supra. There the court recognised that police questioning may violate a person's right to privacy (at 490-492). However, Corbett J stated very clearly that this right does not apply absolutely, but is restricted especially by statutory capacities (at 491). The judge stated: "The right of the citizen to enjoy these immunties *vis-à-vis* the State, or the Executive, constitute what are often termed 'civil liberties' or 'the liberty of the individual or the subject'. In some countries these rights are enshrined in the Constitution or in a Bill of Rights. This is not so in this country. Here they are enshrined in the common law. At the same time the Parliament of this country may make any legislative encroachment it chooses upon the life, liberty or property of its citizens and it is the function of the courts to enforce Parliament's will." (See also ***S v Bailey*** supra at 189-190. Of course, this statement is no longer correct as the Constitution now protects fundamental rights in 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.

180 See generally Neethling ***Privaatheid*** at 362-363, ***Huldigingsbundel WA Joubert*** at 120-121; ***Persoonlikheidsreg*** at 333.

data.[181] As said, in view of the constitutional protection afforded the right to privacy,[182] any such legislation must be reasonable and justifiable in an open and democratic society based on freedom, human dignity and equality.[183]

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

(iii) Third, the protection of the public interest must take place in a reasonable manner, which means that the information must be reasonably necessary for and related to the statutory purpose.[184]

(iv) Fourth, the data may not be processed for longer than is necessary for the statutory purpose.

(v) Fifth, data 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.

3.3.54 If the private or public data controller[185] acts wrongfully in terms of the abovementioned data protection principles, the ordinary delictual remedies,[186] 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.[187] The actio iniuriarum is an action by which a person

---

181 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).

182 See the previous fn.

183 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 at 18---12).

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

185 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).

186 See Neethling ***Persoonlikheidsreg*** at 333; also Faul W ***Grondslae van die Beskerming van die Bankgeheim*** LLD thesis RAU Johannesburg 1991 at 536-537.

187 See McQuoid-Mason at 198-199.

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 data (especially by means of electronic data banks) pose such a serious threat to an individual's personality[188] that it is probably fair and justifiable to hold a data institution liable even where intention or negligence is not present.[189]

Private defence

3.3.55 Private defence is present when the defendant defends himself against another's actual or imminently threatening wrongful act in order to protect his own legitimate interests or such interests of someone else. Acts of private defence justifying an infringement of privacy seldom occur.[190] Nevertheless, although such situations are not ruled out, this defence is not relevant in the data-protection field.

Impossibility

3.3.56 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.[191] This defence is particularly apposite with regard to data processing. If a data controller can prove that it has done everything reasonably possible to ensure compliance with the data protection principles, the wrongfulnees of its processing will be excluded. [192]

(ii) Defences excluding intention

3.3.57 In the common law the general principles of the actio injuriarium apply to defences excluding intention. Once the other elements of an action for invasion of privacy have been proved, animus injuriandi will be presumed. The evidential burden then shifts to the defendant to show

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

189 See Neethling ***Privaatheid*** at 363, ***Persoonlikheidsreg*** at 333-334.

190 See Neethling ***Persoonlikheidsreg*** at 290-292.

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

192 See Neethling ***Persoonlikheidsreg*** at 336 fn 119.

absence of intention.[193]

3.3.58 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.[194]

3.3.59 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.

3.3.60 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.[195]

c) Remedies

3.3.61 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.[196] It has also been decided that the disused common law remedy of a right to retraction and apology should be revived.[197]

3.3.62 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 ot threatened person is entitled to approach a competent court for appropriate relief, including a declaration of rights.[198] 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

---

193 McQuoid-Mason at 237 and references to courts cases therein.

194 McQuoid-Mason in Chaskalson et al at 18---8.

195 Cf McQuoid-Mason at 237.

196 See Neethling ***Persoonlikheidsreg*** at 304-305.

197 See ***Mineworkers Investment Co (Pty) Ltd v Modibane*** 2002 (6) SA 512 (W); see also Neethling J & Potgieter JM "Herlewing van die Amende Honorable as Remedie by Laster" 2003 66 ***THRHR*** (hereafter referred to as "Neethling & Potgieter 2003 ***THRHR***")329 ff; cf McQuoid-Mason ***Acta Juridica*** at 234 and his reference to Midgley JR "Retraction, Apology and Right of Reply" 1995 58 ***THRHR*** 288 at 296.

198 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).

a dual function.[199]

i) Actio iniuriarum

3.3.63 If a person's privacy is wrongfully and intentionally infringed, he may recover sentimental damages or satisfaction (solatium) for injured feelings.[200] In privacy cases the plaintiff is being compensated for the emotional suffering as a result of having his or her private life infringed.[201]

3.3.64 The amount of compensation is in the discretion of the court and is assessed on what is fair and reasonable.[202] Factors which may play a role in the assessment of the amount of the satisfaction are still largely absent from case law.[203] Also note that the Constitutional Court has held that additional constitutional punitive damages should not be awarded in terms of the Constitution for infringements of fundamental rights and freedoms.[204] But because of the constitutional entrenchment, the amount of satisfaction may nevertheless be increased.[205]

ii) Actio legis Aquiliae

3.3.65 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.[206]

iii) Interdict

3.3.66 Where a person is confronted with a threatening or continuing infringement of his or her right

---

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

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

201 McQuoid-Mason at 170.

202 See Neethling ***Persoonlikheidsreg*** at 304; ***Jansen van Vuuren ao NNO v Kruger*** supra at 857-858.

203 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 ***Persoonlikheidsreg*** at 304.

204 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.

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

206 See Neethling ***Persoonlikheidsreg*** at 305.

to privacy, an interdict should be obtainable.[207] Fault on the part of the perpetrator is not a requirement.[208]

3.3.67 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.[209] Otherwise they do not require a different approach from the previous common law position.[210]

iv) Retraction and apology

3.3.68 It was assumed that this Roman-Dutch law remedy had fallen into disuse in South African law. Now the remedy has been revived.[211] This revival can be supported for various reasons, inter alia because it is in conformity with the Bill of Rights, achieving a fairer balance of the fundamental rights to freedom of expression and a good name.[212] 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,[213] as well as a factor in the assessment of the amount of satisfaction.[214]

3.4 Conclusion

3.4.1 Neethling[215] submits that an effective common law data protection, based on general principles, can be achieved only through a two-pronged approach. On the one hand, the so-called traditional principles examined above should be fully utilised. These principles are based on the ordinary

---

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

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

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

210 McQuoid-Mason ***Acta Juridica*** at 236.

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

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

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

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

215 See Neethling ***Persoonlikheidsreg*** at 328.

delictual principles as influenced by the Constitution which regulate the area of privacy protection in South African law (the principles regarding the actio iniuriarum). Consequently, data protection should be seen merely as a particular application of those principles.

3.4.2 However, 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 such application by the courts will occur often or extensively enough in the near future. Thus the matter will have to be regulated by legislation.[216]

3.4.3 On the other hand, the individual himself should also be able to exercise a measure of active control over his personal data.[217] In fact, the traditional protective measures have little value if there is no active individual control over the processing of personal data. The active control principles differ completely from traditional privacy protection under the actio iniuriarum and therefore are unique in the field of personality protection.[218] Consequently such measures can be created by legislation only.

3.4.4 The Commission invites comment on this discussion of the common law and the provisions of the Constitution relating to privacy. What is the relationship between the Constitution and the common law of privacy? Does the Constitution's conception of privacy differ from that of the common law? What are the duties of the legislature insofar as the protection of privacy in general and informational privacy in particular are concerned?

---

216 See also Neethling 2002 ***THRHR*** at 589.

217 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 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 ***Persoonlikheidsreg*** at 334-337). As will be seen infra (chapter 6), these principles also appear in foreign statutes and bills on data protection.

218 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 ***Persoonlikheidsreg*** at 39; ***National Media Ltd ao v Jooste*** supra at 271-272; ***Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty) Ltd ao v Smit NO ao*** supra at 557).

CHAPTER 4: DATA USERS

4.1 Introduction

4.1.1 In order to obtain an idea of the current extent of the processing of data and the potential threat which this poses to a person, it is necessary to refer to the most important data users.[1] This list must not be regarded as exhaustive, as other users also exist or may be created. Generally speaking, a distinction can be made between private and public data users.[2]

4.1.2 The distinction between public and private bodies is, however, not always clear. Many bodies from the private sector routinely take decisions which have a profound impact upon public policy. In many cases they exercise, what for all practical purposes, is public, rather than private, power. For example: suppose a state-owned and controlled corporation controls every aspect of the supply of some particular resource, eg water or electricity or telecommunications. That corporation is then privatised. Before privatisation, few would doubt that the corporation was part of the government, but after privatisation, the corporation might wield exactly the same powers, in fact, and exert the same influence on national life, as it did before. Examples such as these show that the boundary between what is private and what is public - between government and governed - can be accidental and temporary.[3]

4.1.3 All the international data protection instruments are intended to apply to the processing of personal data in both the public and private sectors. The majority of national data protection laws have a similar ambit. In some of these laws, however, differentiated regulation for each sector has occurred with the processing practices of public sector bodies sometimes being subjected to more stringent regulation than those of private sector bodies. Such differentiation is expected to diminish considerably in future national legislation of EU Member States given its absence from the EC

---

1 See Ch 2 for a discussion of this term.

2 A public data user is a user belonging to a public body; a private data user is any other data user.

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

Directive.[4]

4.1.4 The Commission invites comment on the question whether a distinction should be drawn between the public and the private sector when privacy legislation is drafted and if so, what these differences should be.

4.2 Collection of data

4.2.1 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 their 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.[5]

4.2.2 Data can be collected in a variety of ways. New techniques are also emerging all the time to facilitate data collection. Personal information can be collected from three sources: internal records - records collected directly from the person; external records - records obtained from a third party who is willing to make his internal records available; and public records. [6] Public records are records collected by the government pursuant to various research, licencing, administrative and adjudicatory schemes.[7]

4.2.3 Commercial websites collect information through both voluntary and passive means.[8]

---

4 Bygrave at 53.

5 Victorian Law Reform Commission at 21.

6 See discussion on profilers in Ch 5 below.

7 United States Department of Commerce ***Privacy and the NII: Safeguarding Telecommunications-related Personal information*** 23 October 1995 available at http://www.ntia.doc.gov/ntiahome/privwhitepaper.html accessed on 23/4/2002 (hereafter referred to as "***NTIA Privacy Report***") at 33.

8 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) 1FINAL) (hereafter referred to as "OECD Hall Report") at 8.

Voluntary measures include registration pages, surveys and other online forms. With voluntary means, some action on behalf of the subject is generally required and the subject is aware that data is being provided and collected. Many sites actively collect transactional or personal information by deploying specific technologies or business processes on their websites. This could be done through online forms or accounts. Others are less obvious to a website visitor, such as cookies, web bugs or clear.gifs. [9]

4.2.4 In order to establish an account a data subject may have to provide basic contact information, preferences and credit information, where the site charges for its services. Such data collection is often desirable for consumers, and sites with privacy policies often disclose that such data is collected.[10]

4.2.5 Online and ordinary forms are also a common method for collecting information from consumers. The use is widespread. The benefits for companies in collecting this information are clear. By asking a person to fill out a registration form with personal information such as name, address, how the subject learned about the product, companies can develop valuable customer profiles and analysis. This information can be used to improve and refine services and products.[11]

4.2.6 Passive measures include aggregate data collection and site usage selection. The subject may not be aware that this (generally non-personal) information is being collected. Web servers can collect information about what pages a subject looked at, how long a page was displayed on a screen, etc. Some personally identified information can also be collected through passive means. Some websites collect information from persons who store their e-mail address or name in their browser. Subjects may not be aware that this information is being collected. However, most sites with privacy policies that do collect this information do disclose those practices.[12]

---

9 OECD Hall Report at 9.

10 Ibid.

11 OECD Hall Report at 8.

12 OECD Hall Report at 13.

4.3 Examples of private data users

a) Credit bureaux

4.3.1 South Africa does not have a specific law regulating the activities of credit bureaux. At present the credit reporting industry is self-regulated by an industry code of conduct.[13] There are, however, certain aspects of their activities that have a bearing on information privacy, and which are covered by the South African common law and the 1996 Constitution.

4.3.2 In South Africa there are currently 10 (ten) known credit bureaux,[14] the oldest operating since 1901, which are all privately owned.[15]

4.3.3 As the name indicates, the main object of credit bureaux is to collect and furnish information concerning the creditworthiness of people.[16] The information sourced by credit bureaux may be grouped into four types:[17]

---

13 See discussion of code of conduct below.

14 The larger credit bureaux are:

a) Information Trust Corporation (ITC), who store both consumer and business credit information. ITC's main shareholder is Trans Union.
b) Experian, who deals exclusively with consumer credit information, is British owned and is associated with Kreditinform and Snyman & Vennote.
c) Kreditinform, who deals exclusively with commercial credit information and who are South African owned.

The smaller bureaux are:

a) Snyman & Vennote Credit Profile Bureau, a consumer bureau, which focuses on small to medium size businesses as subscribers. They are linked to a debt recovery agency and are South African owned.
b) CIA, who deals exclusively with commercial information. CIA's main shareholder is Trans Union.
c) Medinform, a consumer information bureau who deals mainly with medical information and who is combined with a debt recovery agency, that is South African owned.
d) Creditwatch, that is a consumer bureau dealing only with the medical profession, and is South African owned.
e) Micro Lenders Credit Bureau, a consumer bureau dealing with the micro loans industry, that is South African owned.
f) Compuscan, a consumer bureau dealing with the micro loans industry, that is South African owned.

15 Kraus E ***The Legal Framework : Governing Public & Private Credit Information Registries: The South African Experience*** Credit Bureau Association, South Africa June 2000 (hereafter referred to as "Kraus") at 3.

16 See ***Neethling's Law of Personality*** at 297; Cf also Faul ***Bankgeheim*** at 525-526. With regard to juristic persons, it is in particular information on their creditworthiness which is also the subject of data processing.

17 Kraus at 5.

a) Identifying Information: This is personal information such as name, address, identity number (same as social security number), employment details, marital status and telephone numbers.

b) Court Record Information: Judgments and bankruptcies received from court records, which are public domain information. This information is obtained from the Magistrates Court and the High Court.

c) Default Information: This information is provided by the subscribers to the bureaux who report on how their customers have performed on their financial obligations with the subscriber. This is only negative information.

d) Closed User Group Information:

i) Consumer Credit Association (CCA)

This association represents 80% to 90% of the larger retailers, but has in the past few years extended to include debt recovery agencies and the banks in the last six months. Members of this association supply both positive and negative information on the monthly payment details of the accounts that are held with the member.

ii) Bank Data

The major banks share negative information on their customers amongst themselves. This information is maintained by the two major bureaux, ITC and Experian. During 1999 and 2000 the banks entered into discussions with the CCA and have agreed to share their information of existing customers with the CCA members. In addition, they have agreed to share positive information of all new account applications. The banks in turn will have access to the CCA positive and negative information. This is a significant step towards getting the banks to share their information with other industry bodies.

4.3.4 It has been argued that credit bureaux may be capable of disclosing a complete record, not only of someone's creditworthiness, but also of his entire personal life. In this regard it would seem that South African credit bureaux generally restrict their activities to information on creditworthiness.[18] However, the danger that other and further information may also be collected

---

18 See McQuoid-Mason 197 fn 9, 1982 ***CILSA*** 137.

and stored definitely exists.[19]

4.3.5 Credit bureaux have an important role to play in providing consumers with access to credit facilities. However, owing to the fact that it is often difficult to identify data subjects positively from newspaper or court reports, the real possibility exists that data reports on persons in credit bureaux may contain misleading or incorrect information.[20] It is important to note that although the data stored by credit bureaux is often available only to its clients,[21] the possibility exists that other individuals, private corporations or even the state may have access to such information.[22] In the USA the Federal Trade Commission receives more complaints about credit bureauxs than about any other industry. [23]

4.3.6 Errors are not always the fault of the credit bureau - it might be from one of its sources. The credit bureau's responsibility to its customers is to give an accurate reflection of what is in a public record, but that record may itself be inaccurate.[24]

4.3.7 Regardless of the origin of such errors, there are no clear lines of responsibilty for correcting the record. Meanwhile, the victim's life may descend into a Kafkaesque nightmare.[25]

4.3.8 In 1989 the Credit Bureau Association (CBA) drew up a self-regulatory code of conduct,[26]

---

19 It has been argued that their activities are not always restricted to this subject. Other personal facts such as drinking habits, health, characteristics, reputation, extra-marital relationships, political and religious convictions, criminal records, race etcetera may be included in the data records.

20 For examples from case law, see ***Informa Confidential Reports (Pty) Ltd v Abro*** 1975 (2) SA 760 (T); ***Pickard v SA Trade Protection Society*** (1905) 22 SC 89. Also in ***Kritzinger v Perskorporasie van Suid-Afrika (Edms) Bpk ea*** 1981 (2) SA 373 (O) 386 it was acknowledged that credit bureaux may distribute incorrect information.

21 Cf eg ***Dun and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd*** 1968 (1) SA 209 (C).

22 See Neethling 1980 ***THRHR*** 144.

23 Piller at 2.

24 Piller at 2 referring to Steve Metlitz, general counsel of the Information Industries Association, which represents about 500 companies that gather and resell data in the USA.

25 Piller at 2. It has been noted that although a credit bureau may in theory be easily accessible to consumers, callers have been known to wait in line for more than an hour without being able to reach a credit bureau by phone.

26 The Consumer Affairs Committee of the Department of Trade and Industry is undertaking an investigation in terms of sec 8(4) of the Consumer Affairs (Unfair Business Practices) Act 71 of 1988 into the role of the Credit Bureau Association with reference to its ability to enforce its existing Code as well as into credit bureaus and their compliance with the Code. The investigation will also consider whether the existing Code should be amended. Report 97 was published in the

as a result of increasing pressure from various consumer groups to protect consumers against possible credit bureau abuses. In 1994 the CBA, in association with the Business Practices Committee (BPC) of the Department of Trade & Industry (DTI), formalised the code, which applies to all credit bureaux in South Africa. The BPC has included various principles from the Fair Credit Reporting Act (USA) in the code.

4.3.9 In terms of this code a consumer who is dissatisfied with treatment which he/she has received from a credit bureau, can approach the CBA with his/her grievance. Should a consumer then still be dissatisfied with the CBA's handling of the complaint, the matter should be referred to the BPC.

4.3.10 The CBA code makes provision for the following with respect to protecting the consumer:

- Credit bureaux have a duty to treat subscribers and consumers as fairly and impartially as possible. In addition, credit bureaux may only contract with subscribers who warrant that they have a bona fide risk management reason for accessing the information and who agree not to disseminate the information to any person other than the consumer concerned.

- Bureaux must follow reasonable procedures to ensure that the information they obtain is accurate, relevant and unbiased. Furthermore, the source of information received and the subscribers who access the information must be recorded.

- Only information relating to credit and business dealings may be recorded by bureaux. Personal information such as name, date of birth, identity number, addresses, telephone numbers, employment and marital details may also be recorded.

- A bureau must upon request and presentation of positive identification, disclose to a consumer the nature and substance of all information and the sources of the information on its file on that consumer at the time of the request. No telephonic

---

Government Gazette in May 2003. Comments are being considered at present.

disclosures should be made. The disclosure can either be to the consumer in person, or in writing if the bureau is satisfied regarding the consumer's identity. Disclosure may be made to a consumer's attorney.

– A bureau must provide trained personnel to explain to a consumer any information furnished and to provide advice on how to obtain corrections to a consumer's record where possible.

– A bureau may charge a reasonable fee to allow consumers to view any information about themselves. If it is found that any information is incorrect, the bureau must refund the fee.

– If a consumer disputes the accuracy of any item of information in his file, the bureau must reinvestigate such information and if it is found to be inaccurate or can no longer be verified, it must be deleted and all subscribers who have received such information must be informed of the deletion. If the reinvestigation does not resolve the dispute, the consumer may file a brief statement explaining the nature of the dispute.

– In the case of a dispute between the bureau and a consumer on the accuracy or relevancy of information, the bureau or consumer may request the Credit Bureau Association (CBA) or the Business Practices Committee (BPC) to investigate the matter.

– Bureaux must take into account consumers' interests regarding the length of time for which information is retained, so that consumers are not burdened by stale information about long past credit defaults.

– Information on bankruptcies and rehabilitations are retained for a period of 5 years from date therefrom. In the case of judgments, information is retained for 5 years and information supplied by a subscriber is retained for 3 years.

4.3.11 During 1999 the CBA reviewed the code of conduct and submitted it to the BPC for

approval. These amendments are still under consideration by the BPC. The reviewed code includes the following:

- That the code apply to bureaux that record both consumer and business information. The reason for this is that the CBA has members who store both consumer and business information. Furthermore, the pending Data Privacy Legislation aims at protecting the right of privacy of both consumers and businesses.

- That subscribers shall warrant, via their subscription agreement to the services of a bureau, that they have obtained the necessary consent from their customers to access bureau information, and that the consumer has been informed in writing of the subscriber's intention to supply such information to the bureaux.

4.3.12 Although the code of conduct does provide recourse for consumers through the Credit Bureau Association (CBA) and the Business Practices Committee (BPC), the majority of consumers are not aware of these avenues for complaints or even the fact that credit bureaux are self-regulated by the code of conduct. There are also very few consumer bodies or even government bodies who are aware that bureaux activities are regulated by a code of conduct.

4.3.13 The reason for this situation is that there is a general lack of education and information available on credit-related issues. The credit bureau industry has indicated that it welcomes the drafting of a separate Data Privacy Act and would like to assist government in its research.

4.3.14 Comments are invited from readers recounting their personal experiences with credit bureaux as well as from credit bureaux themselves, indicating their views regarding the principles to be embodied in the proposed legislation.

b) Direct marketing

4.3.15 Specific agencies exist which make lists of the addresses of individuals, usually for advertising purposes,[27] and process statistical facts on groups (for example, research by sociologists).[28]

4.3.16 The Direct Marketing Association[29] is a non-profit trade association representing all stakeholders in the South African direct marketing industry. Members include the widest range of private and governmental bodies involved in the making of sales and the developing of relationships directly by mail, telephone, television and radio, magazines and newspapers, fax, electronic mail and the Internet - all brought together by a common interest in responsible business practice.[30] In October 2002 the Direct Marketing Association, the Association of Marketers and the Institute of Marketing Management amalgamated to form the Marketing Federation of Southern Africa. The MFSA will from now on comment on behalf of the marketing industry.

4.3.17 It is the stated object of the direct marketers to create a balance of interest between the rights of the industry and the rights of the individual. The industry's position is that businesses have the right to collect and use information about their clients and prospects, provided that process is transparent, legitimate and fair, and the individual's right to privacy and choice is respected and protected.

4.3.18 The argument has been put forward that by electing to provide their personal information to organisations, individuals give implicit permission for organisations to use that information to communicate and do business with them. However, if organisations wish to use the information for any other purpose (e.g. to share it with third parties), this should be made clear to the individual, who should then have an explicit opportunity to opt out of such use. Direct marketing organisations believe that the long-term growth and success of the industry is best served by adherence to this

---

27 Although the address lists as such do not pose a threat to an individual, the fact that suchs lists are often connected with intimate personal information (eg the fact that a person buys pornography) may pose a threat to privacy. See generally Neethling ***Privaatheid*** at 15 and McQuoid-Mason 1982 ***CILSA*** at146-147 where he remarks at146: "Mail advertisements are a reminder that there are agencies somewhere about which the consumer knows nothing, but which know something about him."

28 See ***Neethling's Law of Personality*** at 294.

29 DMA Submission on Open Democracy Bill, August 1998.

30 The Association represents some 300 companies and 1000 individuals, both local and international. Membership includes organisations ranging from entrepreneurial start-ups to the largest multi-national corporations, and is fully representative of both marketers in and suppliers to, the financial, retail, advertising, mail order, call centre, and electronic commerce industry, amongst others. All members are bound by a stringent Code of Practice based on international norms, and which has the endorsement of the Business Practices Committee of the Department of Trade and Industry.The Direct Marketing Association of Southern Africa is a founder member of the International Federation of Direct Marketing Associations (IFDMA). Over 29 DMA's from arond the world are members of IFDMA, and subscribe to its self-regulatory principles.

philosophy, and that as self-interested parties they are best positioned to ensure compliance with this position.

4.3.19 The DMA publishes a document entitled "Best Practice Guidelines for the Marketing of Goods and Services through the Internet" which addresses issues such as privacy policies, security, cookies-policy, means of opting out, unsolicited e-mail marketing and complaints. These guidelines have been written as a practical approach to conducting business with consumers on the Internet according to the best ethical practices, and in order to increase trust in the Internet.
4.3.20 The DMA also provides a Fair Information Practices Checklist[31] which offers a questionnaire to challenge a company's privacy policy and its implementation within the organisation.

4.3.21 The DMA should be distinguished from Direct Response Marketing,[32] a major player in the distribution of leaflets directly to homes in South Africa. These are not addressed to any specific individual and personal information is not utilised.

4.3.22 The Commission is interested in the views of both consumers and marketing agencies regarding direct marketing practices. Does practice indeed match theory? See also the discussion on consent in Ch 5 below.

c) Health and medical profession

4.3.23 Privacy and confidentiality have long been recognised as essential elements of the doctor-

---

31 Direct Marketing Association of South Africa ***The Privacy File*** April 2001.

32 Submission on Open Democracy Bill 12 August 1998.

patient relationship. [33] For optimal care of the patient, it is essential for the medical profession (medical practitioners, dentists, psychiatrists and psychologists) to collate information on the health of their patients[34] into a complete medical record.

4.3.24 Each time a patient sees a doctor, is admitted to hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information.[35] This record is used for a wide variety of purposes including insurance functions, co-ordination of care, and research.[36] Databases are also established containing information in health and genetic materials so as to be able to do research on diseases and disorders with a genetic component.[37]

4.3.25 The longstanding friction between these two goals, namely patient privacy and access to information, has been heightened by the transition to electronic health information and a push toward integrated information in support of health care delivery and health data networks. While these developments are intended to improve health care, they also raise many questions about the role of privacy in the health care environment. [38]

4.3.26 The public has some reason to be concerned. Today there is little consistency in approaches to patient confidentiality and no national standards or policies on patient confidentiality, apart from specific rules and the general constitutional provisions that are not aimed at the specifics of doctor-patient-medical relationship.

4.3.27 The National Health Bill of November 2001 contains the following proposal in relation to

---

33 Klinck E ***Health Data Confidentiality and Privacy : Standards*** Human Rights, Law and Ethics Unit, SAMA Document based in part on the document generated by Dr Pino Mavengere, Previous Team Leader, Privacy and Confidentiality Subcommittee of the Committee on Standardisation of Data and Billing Practices (hereafter referred to as "Klinck") at 1.

34 Neethling ***Huldigingsbundel WA Joubert*** at 109.

35 US Department of Health and Human Sciences ***HHS Fact Sheet*** May 9, 2001.

36 Klinck at 1.

37 Example of Islandic Health Sector Database as set out in Hreinsson P "Projects and people: The Islandic Health Sector Database" Presentation at the 23rd International Conference of Data Protection Commissioners, Paris, 24-26 September 2001.

38 Klinck at 1.

patient information and records:

> 14. Every user (ie patient) is entitled to confidentiality of all health information, including health status, treatment or stay in a private or public establishment. This information is only to be disclosed if the user consents in writing or if a law or a court order authorises the disclosure.

This means that any person other than the doctor or facility who wants that information has to get the patient's consent in writing or do so in accordance with a law or court order.

4.3.28 Mechanisms for the protection of health records held by any private or public health establishment are furthermore found in section 19 of the Draft Bill. It lists some 9 types of conduct that would constitute an offence.[39]

4.3.29 Medical schemes are provided with patient health information for the purpose of medical aid and one can argue that by joining a scheme the patient and his/her dependants consent to the use of their medical information for scheme purposes (e.g. pay-out or non-pay-outs, etc.). The Medical Schemes Regulations authorises the transmission of patient health information, but **only where there is a managed care arrangement**.

4.3.30 In terms of regulation 15(10) a medical scheme must have access to any treatment records held by the provider and other information pertaining to the diagnosis, treatment and health status of the member *in terms of the arrangement*. Such information may not be disclosed by the provider to any other person without the written consent of the member, unless such disclosure is in terms of any legislation. Regulation 15(9) provides for the information in relation to diagnosis, treatment or health of any member of a medical scheme or of any dependant of such member to be treated as confidential. The Medical Scheme is bound by this confidentiality and may not pass on, share,

---

39 Included are:
… (g) without authority, connects the personal identification elements of a ***use***r's record with any element of that record that concerns the ***use***r's condition, treatment or history;
(h) gains or attempts to gain, unauthorised access to a record or record-keeping system, by any means, including intercepting information being transmitted from one person, or one part of a record-keeping system, to another;
(i) without authority, connects any part of a computer or other electronic system on which records are kept to -
(i) any other computer or other electronic system;
(ii) any terminal or other installation connected to or forming part of any other computer or other electronic system; or
(iii) attempts or actually does modify or impair the operation of -
(aa) any part of the operating system of a computer or other electronic system on which a ***user's*** records are kept; or
(bb) any part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a ***user's*** records are kept.

sell or deal with the information without a law authorising it or the patient's informed consent. Intermediaries are, by implication, bound by these regulations.

4.3.31 A private organisation like IMS Health South Africa[40] has indicated[41] that the organisation's Canadian office does not collect identifiable patient information. It does however collect prescription sales data information that identifies the prescriber via electronic means from dispensing pharmacies. The company then uses these prescription sales data and various statistical methods to produce prescriber information in the form of estimates of normative prescribing patterns of physicians, as well as estimates respecting individual physicians' prescribing patterns. The company only discloses estimates respecting an individual physician's prescribing patterns with the express consent of the individual prescriber; otherwise, prescriber information is disclosed only in aggregate form.

4.3.32 The World Medical Association passed a statement on ethical considerations regarding Health Databases, which sets the tone for medical associations world-wide. As with the Canadian Code, the WMA states that the primary purpose of collecting patient information is to care for the patient. Confidentiality is at the heart of medical practice and is essential for maintaining trust and integrity in the patient-physician relationship. Knowing that their privacy will be protected gives patients the freedom to share sensitive personal information with their physician.[42]

4.3.33 Quality assurance, risk management and research are so-called secondary purposes of data collection. Care must be taken that secondary uses of information do not inhibit patients from confiding information for their own health care needs, exploit their vulnerability or inappropriately borrow on the trust that patients invest in their physicians. Where possible, data for secondary purposes should be de-identified. It defines de-identified data as data where the link between the patient and information has been broken and cannot be recovered. If this is not possible, however, the use of data where the patient's identity is protected by an alias or code should be used in

---

40 IMS Health SA is part of IMS Health, a world provider of healthcare information services to the global health sector.

41 IMS Health SA (Prop)Ltd "Submission in Response to the Draft Electronic Commerce and Transactions Bill of the Republic of South Africa" May 2002 (A Response prepared on behalf of IMS Health SA by Gunning K).

42 The World Medical Association ***Declaration on Ethical Considerations Regarding Health Databases*** Adopted by the WMA General Assembly, Washington 2002 (hereafter referred to as "WMA Declaration") at 1.

preference to readily identifiable data.[43]

4.3.34 The statement reaffirms that information may only be disclosed with informed consent or in terms of national law. The statement also requires documentation on what information is held and why, what consent has been obtained by patients, who may access data, why, how and when the data may be linked to other information and the circumstances under which data will be made available to third parties.[44]

4.3.35 National medical associations should cooperate with the relevant health authorities, ethical authorities and personal data authorities, at national and other appropriate administrative levels, to formulate health information policies based on the principles in this document.[45]

4.3.36 The Commission would appreciate input on the safeguards that should be provided.

d) Banks, financial and insurance institutions

4.3.37 The confidentiality of customer financial information has always been a key issue within the financial industry and is obviously integral to the very business of processing vast quantities of highly sensitive financial information.[46] The following data is held by banks:[47]

a) confidential information
b) personal and family data
c) transactional data

---

43 WMA Declaration at 3.

44 WMA Declaration at 3-4.

45 WMA Declaration at 4.

46 Bennett CJ "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association" and the references made therein. Prepared for the "Voluntary Codes Project" of the Consumer Affairs Industry, Canada and the Regulatory Affairs Treasury Board March 1997(hereafter referred to as "Bennett Voluntary Codes Project" .

47 Jones S "Anytime, Aywhere, Anyhow but Anybody?' Presentation at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002 .

d) personal wealth information and investment portfolios

e) payment details

f) aspirations

4.3.38 It is in the interests neither of these institutions, nor of consumer and privacy advocates, to have employees dealing carelessly with sensitive customer information. [48]

4.3.39 Similarly, there is a consonance of interests in data quality. Institutions need accurate, timely and complete information; customers generally have the same interests. To the extent that rights of access and correction can enhance data quality, these will be seen as mutually beneficial and will presumably be implemented without much difficulty.[49]

4.3.40 Privacy protection is also sometimes regarded as "good business practice". All institutions have a considerable, though immeasurable, incentive to satisfy customer concerns and to respond to complaints. Strong incentives exist to avoid bad publicity about the wrongful collection, treatment and disclosure of personal information in both the banking and insurance industries.[50]

4.3.41 Problems have however been experienced in practice:

a) Credit bureau Experian accidentally made available on its website the records on 1.5 million clients in July 1999.[51] The information was from cell phone company Vodac and banks Nedcor, Standard Bank, Mercantile, Teljoy and Homechoice and included names, addresses and identity, telephone and cellphone numbers, and bank account details.

b) In February 2000 it was discovered that First National Bank's (FNB) telephone banking service allowed callers to obtain a balance statement and available credit level for the

---

48 Bennett Voluntary Codes Project at 21; Faul in her dissertation (see fn 16 above) provides a theoretical foundation for a banker's duty of secrecy and its ambit in South African law. The foundation of a bankers's secrecy is in delict. The ordinary principles of delict are applied to the banker's duty of secrecy..

49 Bennett Voluntary Codes Project at 21.

50 Bennett Voluntary Codes Project at 22.

51 "Fears That Website Listed Confidential Bank Data " ***Africa News*** July 12 1999..

accounts of any client. The service was reported to get 170,000 calls a month.[52]

4.3.42 From the financial industry's side principles that restrict the sharing of personal information within and between banking institutions are being more strenuously fought. Institutions have tended not to support the constraints on the legitimate flow of personal information within and between financial institutions on the assumption that this would reduce the bad credit decisions made about individual and business customers.[53]

4.3.43 Sir Gordon Borrie, Director General, Office of Fair Trading stated in November 1989 :

> I am at least as concerned about over-indebtedness as I am about the demands of privacy, I do not see why a bank should not require express consent as a condition to the grant of a loan. After all, a prospective borrower has no right to credit and I do not think he or she could reasonably object to the disclosure of relevant information being a condition of the grant of credit. I recognise and accept, then, the value of externally supplied information - notably that held by credit reference agencies - to the success of the modern lending decision.

4.3.44 The most stringent constraint on banks is imposed by the principle of individual consent for new uses of personal information, particularly for attempts at cross-selling. The initial notification of the purposes for which personal data may be used and for the securing of customer consent before using that information for other purposes takes time, effort and resources. Forms have to be revised, and opt-out boxes included. Computer systems also need to be reprogrammed to flag "do not market" accounts. Staff need to be trained in these different procedures.[54]

4.3.45 Common law confidentiality provisions provided this security long before codes of practice were drawn up and promulgated. Under certain circumstances the invasion of a customer's privacy might be considered a breach of fiduciary duty or a breach of confidence. Common law remedies, however, are widely regarded as time-consuming, costly, piecemeal, unpredictable and protective of only a narrow range of abuses.[55]

---

52 "FNB allows access to account balance data," ***Business Day***, February 21, 2000.

53 Bennett Voluntary Codes Project at 22.

54 Ibid.

55 Bennett Voluntary Codes Project at 6.

4.3.46 Developments in card technology in particular have furthermore had a profound impact on the bank's personal information collection practices. Electronic fund transfers through automated teller machines (ATM) were the first to place greater banking responsibility into the hands of the individual customer. These have been followed by debit card services that allow a cardholder to undertake transactions at the point of sale. A range of decentralised services furthermore exist that allow customers to use their personal computers or telephones to perform many banking functions and raising a range of security concerns.[56]

4.3.47 The decentralisation of banking and payment systems envisaged for the "information highway" raises the potential for the collection, matching and profiling of enormous quantities of "transactional data" - information on what individuals purchase, what services they use, what entertainment products they prefer, etc. This is valuable marketing data both for institutions and for those subsidiaries that provide an increasing range of new financial products. Loan information for example may give banks a shrewd idea of when a customer may be in the market for a new car, home or whatever. Investment information may give banks advantageous opportunities to market their own investment products.[57]

4.3.48 In South Africa the Cabinet approved a plan in March 1998 to issue a multi-purpose smart card that combines access to all government departments and services with banking facilities. This is part of the information technology strategy formulated by the Department of Communications to provide kiosks for access to government services.[58] In the long term, the smart card is intended to function as passport, driver's license, identity document and bank card. The driver's license will include fingerprints. The new smart cards have not yet been issued to date and could still become a controversial issue.[59]

4.3.49 The sharing of customer financial information across the traditional "sectoral" boundaries confronts squarely the central information privacy principle that information collected for one purpose may not be used for another without the individual's consent or without statutory

---

56 Ibid.

57 Ibid.

58 Shapshak, D "SA services get `smart'" ***Mail & Guardian***, April 24, 1998.

59 "Smart Cards To Replace ID Books In SA In 2001" ***Africa News***, February 1, 2000.

authorisation.[60] The property and life insurance industries, for instance, are concerned that banks will use their unequaled access to personal financial data in order to market insurance products.

4.3.50 At present there is no evidence within the financial sector of using privacy for competitive advantage. Nowhere in publicity campaigns do we see that consumer privacy is protected better at Bank X than at its competitors. Banks are rather responding to pressure from government and consumer groups, not to large numbers of complaints about privacy from their existing customers.[61]

4.3 51 Financial institutions will, however, be worst hit if the country does not comply with the crossborder transfer regulations of the EU Directive. The interruption of the international communication of customer and client data could have serious consequences for many industries in the financial sector.[62] In South Africa financial privacy is covered by a code of conduct for banks issued by the Banking Council in March 2000. [63] The South African Insurance Association (SAIA) members also abide by a Code of Conduct.

4.3.52 The Commission would appreciate feedback regarding the need for and nature of statutory regulation in so far as financial privacy is concerned.

e) Other

Private detectives

4.3.53 In order to obtain complete information on a person, the services of private detectives are often employed.[64] Although little information is available on the practices of private detective agencies, it goes without saying that their activities also constitute a possible threat to an individual's personality rights. An interesting question is for what period of time detectives should

60 Bennett Voluntary Codes Project at 7.

61 Bennett Voluntary Codes Project at 14.

62 Bennett Voluntary Codes Project at 4.

63 EPIC Report 2002 at 2 .

64 See generally ***Neethling's Law of Personality*** *at*13 -14, 1980 ***THRHR*** 144; McQuoid-Mason 1982 ***CILSA*** at 140-142.

be allowed to keep records of people who have been investigated.

Employers

4.3.54 Employers process information on aspirant as well as actual employees.[65] There are those who consider that there should be no right to privacy in the workplace. Such a stance is not new. The paternalistic approach of factory and mill owners in England in the 19th century left little room for private life. More recently there are examples of employers who consider the private lives of their employees their business. Henry Ford is reputed to have required "my staff to have unblemished private lives".[66]

4.3.55 Employees have plenty to worry about. Ellen Bayer heads the resources team at the American Management Association and her sentiments are that "privacy in today's workplace is largely illusory.[67] Many threats are created by new technology.[68]

4.3.56 These challenges to privacy created by new technology are compounded by changes in the nature of work itself. We are moving to a 24/7 world, one where the once rigid division between home life and work life is breaking down. These days it can be increasingly difficult to know when we are in our own time, and when we are at work.[69]

4.3.57 There is a blurring too, between the workplace and the home. Teleworkers have been

---

65 See ***Neethling's Law of Personality*** at 14-15.

66 France E "Private Life - Working life" Introduction to worksession presented at the 23rd International Conference of Data Commissioners in Paris, September 2001 at 1.

67 Jennings P "Private Life- Working Life" Presentation at the 23rd International Conference of Data Protection Commissioners Paris, 24-26 September 2001(hereafter referred to as "Jennings") at 2.

68 Workers in a modern workplace can be overseen in very many ways - by monitoring of the keys depressed on a keyboard, by monitoring of e-mails sent and received or of websites visited, by closed circuit television, by the recording of telephone calls or numbers, and by smart ID cards, which track the movements of workers around a building or complex. It is not only that these practices take place, it is also that the data obtained can be stored effortlessly in digital form, and later interrogated using extremely powerful data analysis tools. Never before have some people had the capability of holding so much information about other people, and of accessing this information so easily.

69 Jennings at 3.

much discussed in recent years. Many employees are taking their work home these days, aided by the facility of being able to access corporate networks from home offices. Mobile teleworking is a growing trend, where staff who were previously office-bound are now able to keep in touch and undertake work whilst on the move, whether in cars, on trains, in hotels and airports.[70]

4.3.58 Enjoying the right to privacy means having control over your personal data and the ability to grant or deny access to others. There may, however, be reasons why employers quite legitimately need information about their employees. There may indeed be times when even electronic monitoring is appropriate. For example, closed circuit television (CCTV) can actually help workers in vulnerable jobs, such as security officers.[71]

4.3.59 These issues need to be worked through a process of consultation and negotiation between companies and their workers, not by management diktat.[72] Many of the difficult issues about privacy in the workplace can be resolved through a process of social dialogue and negotiation, through common sense and trust. This is what good employers already do.[73]

4.3.60 The International Labour Organisation (ILO) adopted a useful code of practice on the protection of workers' personal data seven years ago, but the code remains advisory and this, as in other areas, the work of the ILO needs to be strengthened.[74]

4.3.61 The Commission has noted that in-depth studies dealing specifically with privacy in the workplace are currently being conducted worldwide. Comment is invited as to the need for such research in South Africa.

---

70 Jennings at 4.

71 Jennings at 4

72 Jennings at 5.

73 Jennings at 6.

74 Jennings at 6.

Voluntary associations

4.3.62 Voluntary associations (such as churches) may collect information on their members.

SA Fraud Prevention Service

4.3.63 The SAFPS is a non-profit organisation funded by the major banks and credit retailers for the identification and filing of fraud data on credit applications.[75] The service is based on the CIFAS model[76]. When information provided by an applicant for a product or service fails verification checks, member organisations are able to exchange any details that are suspected of being fraudulent. Members can also exchange information about accounts that are suspected of being fraudulently misused. [77]

4.3.64 When an SAFPS member organisation identifies a suspected act of fraud, a warning is placed on the SAFPS databases which are sited at the major credit bureaux. The warning does not suggest that the person indicated has committed fraud. It simply means that extra precautions should be taken to ensure the application or account that has prompted the check is genuine.

4.4 Examples of public data users[78]

4.4.1 As has already been said, the state, with all its departments, agencies and other offices, personifies the public data media.[79]

4.4.2 Many details of an individual's life, activities and personal characteristics can be found

---

75 See the website of the SAFPS at : www.safps.org.za

76 The Model that has been used in the United Kingdom for the last 11 years and which has yielded in excess of 850 million Sterling in fraud prevention savings.

77 South African Fraud Prevention Services booklet.

78 See generally Neethling ***Huldigingsbundel WA Joubert*** 110-111. See also Geldenhuys 156-216 217-249.

79 See generally Du Plessis at 376 on legislation in this regard; see also ***Neethling's Law of Personality*** at 16-18; McQuoid-Mason at 196-197.

scattered throughout the files of government agencies. On account of the state's numerous activities and functions, the personal data processed covers a wide range of topics, for example information on civil servants as employees; conscripts in the defence force; pupils and students at educational institutions (such as schools, colleges, technikons and universities); suspects, accused persons and prisoners from the police and correctional services; taxpayers from the receiver of revenue; recipients of welfare from social services; and on all individuals in terms of census reports and registration of the population.

4.4.3 When collected , compiled and maintained over years and across jurisdictions, the records contain a complete reflection of the events, habits, and occupations of individuals and families. The effect of technology has been to strip away much of the privacy that used to exist because of the difficulty of finding and obtaining records.[80] With the growing use of computers in state departments (and especially with the introduction of the new e-government proposals), it is submitted that there is a need for legislation to regulate the collection, use and disclosure of information by government.[81]

4.4.4 Public records about individuals include a wide range of personal information. A public record can be identified as :[82]

a) a register, list, roll or compendium of personal data under the control or direction of a public body;

b) maintained pursuant to statute, regulation, rule, or administrative practice; and

c) open (in whole or in part) to public inspection, copying, distribution, or search under the specific law or policy.

4.4.5 There are, however, also categories of personal information maintained by government agencies that are not routinely available to the public. These include census records, income tax records, wage and personal property tax records, health records, school records (except directory information) juvenile criminal proceedings, adoption records, welfare and social service records,

---

80 Gellman R "Public Record Usage in the United States" Presentation at the 23rd International Conference of Data Protection Commissioners, Paris, 24-26 September 2001 (hereafter referred to as "Gellman") at 1.

81 McQuoid-Mason at 197.

82 Gellman at 1.

benefit records and library borrowing records.

4.4.6 The processing of this data is usually justified by its public importance[83] and the storage and use of the information are generally essential for the proper functioning of the state administration and effective state planning. Since individuals may be compelled by legislation[84] to furnish information on themselves to the state, the state controls this unique source of information directly[85]

4.4.7 To illustrate the danger which the processing of data by the state poses to the privacy of the individual, the Identification Act 72 of 1986[86] may be mentioned.[87] This statute[88] permits the Director-General of Internal Affairs to supply personal information (like that contained in the official identity document)[89] without the consent of the data subject to any other state department, local authority or statutory body for any of their objects, or even to any other person who makes application and pays the prescribed fees, if the director-general is of the opinion that such furnishing of information is in the interest of the person concerned or in the public interest.

---

83 In eg ***S v Bailey*** supra the court remarked regarding the compulsory furnishing of information in terms of the Statistics Act 66 of 1976: "one must assume... that this informration is reasonably required for the benefit of the community at large..."

84 See ***Neethling's Law of Personality*** at 301 on the requirement that legislation in this regard must be in accordance with fundamental human rights safeguarded by the Constitution.

85 See eg s 5(2) of the Statistics Act 66 of 1976: "Every person shall to the best of his knowledge and belief answer, when so required, all questions put to him orally or in writing under this Act by the Chief of the Central Statistical Services or his delegate and which are necessary for the collection of statistics, and shall furnish in the prescribed manner all such statistics as are required under this Act." Non-compliance with these provisions may entail criminal prosecution (s 13 Act 66 of 1976). See also s 75 of the Income Tax Act 58 of 1962; See Du Plessis at 378-379 382-383 on both these statutes. See generally Faul at 448-453.

86 See Du Plessis 379-381; cf McQuoid-Mason 159 197 on previous legislation.

87 See further, eg, also ***S v Bailey*** supra at 189-190, where the court referred to the effect on the individual's privacy of state action in regard to the compulsory furnishing of information in terms of the Statistics Act 66 of 1976 (190): "Speaking for myself, I have a measure of sympathy for the appellant. He was required to furnish an incredible mass of detail ranging across a very broad spectrum. These include personal details of his population group, age, qualifications, the nature of his professional work, status in the profession, average number of hours per week spent on work connected with the profession, attendance at refresher courses, whether he was contracted in or out under the Medical Schemes Act, the number of full time employees [etc]." Nevertheless the court held that the appellant's refusal to furnish the information on the grounds that "these are my private affairs" and are protected by his right to privacy, could not succeed in view of the statutory provisions.

88 S 17; See Du Plessis at 380-381.

89 See Du Plessis at 379-380; McQuoid-Mason at 159. Du Plessis at 381 concludes that this act violates the privacy of the individual and does not contain sufficient protective measures.

4.4.8 However, in view of the constitutionally protected fundamental right to privacy, in future it may happen that legislation of this nature is set aside or interpreted restrictively. A recent example of legislation of which the constitutionality may be in doubt is that of Chapter 3 of the Public Service Regulations[90] dealing with the financial disclosure of members of the Senior Management Structure. In terms of these regulations any such member is obliged to disclose details of certain specified registrable interests including any ownership or interest in land and property, whether inside or outside the Republic. The stated purposes of the regulations are to prevent conflict of interests and corruption since employees are entrusted with public funds, and as such need to maintain the highest standards of professional ethics. If the Public Service Commission is of the opinion that any of the disclosed interests conflicts or is likely to conflict with the execution of any official duty, steps will be taken.

4.4.9 The indiscriminate, blanket application of the regulations to all employees in a certain category irrespective of their job description, the fact that the regulations are not deemed to be effective and finally the fact that the object of the regulations can be obtained by less intrusive methods, are all arguments in favour of the viewpoint that the regulations are unconstitutional. Since South Africa has no independent agency or ombudsman to determine disputes of this kind, employees will have to take this matter to court should they wish to address it. Currently any person who does not supply the information may be charged with misconduct.

4.4.10 Since employees are warned that information supplied in terms of the regulations may be accessed in terms of sec 11 of the PAIA, it is also possible that an employee will not be protected against his or her personal information being disclosed to third parties, since sec 34(2)(b) of PAIA may exclude such protection.

4.4.11 A requester requesting access to the record of a public body furthermore does not have to indicate the purpose for which the record is requested. This suggests that even if access is requested for purposes other than the protection of a right of interest, the request is not invalid. In fact, section 11(3) provides that a requester's right of access to the record of a public body is not affected by the reasons given for the request, or the information officer's belief as to what the

---

90 Chapter 3 of the Public Service Regulations, 2001, promulgated in terms of the Public Service Act, 1994.

reasons are. A request may, however, be denied if it is manifestly frivolous or vexatious.[91]

4.4.12 The following lessons can be drawn about how governments may approach the privacy issue in the years ahead:[92]

a) Learn from experience elsewhere. In the world of privacy protection, no government is an island. The toolbox of privacy instruments is increasingly a global toolbox, containing instruments for privacy protection that any jurisdiction can apply should it so wish.

b) Beware of the perception of Big Brother. Some of the most controversial privacy scandals have arisen as a result of large-scale governmental plans to integrate personal data systems. Indeed, it was those very plans that initially forced the issue onto the agenda in many Western societies. The spectre of the "Big Brother" omniscient state is still a real fear.

c) Resist the temptation to identify citizens just for the sake of it. Governments need to reflect on the extent to which they actually need to identify their citizens. There is often an assumption that government has a core and unique function to identify citizens. Debates over proposals to develop national identification cards in the UK and Australia, for example, were characterised by strong opposition from all sides of the spectrum.

d) Anticipate, rather than react to , privacy events. History suggests that organisations get caught out when they fail to appreciate, or they underestimate the degree of public concern over the collection and use of personal information.

e) Be transparent. Historical examples suggest that organisations get into trouble when they are less than honest about their personal data processing practices. Privacy scandals emerge when outsiders' suspicions are raised about the hypothetical ways in which systems developed for legitimate purposes can change into more intrusive surveillance devices.

f) Enhance trust. There is no necessary incompatibility between privacy protection and other policy goals which require the collection of personal information.

---

91 Sec 45 of the Act. 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 (hereafter referred to as "Visser").

92 Bennett at 29.

g) Design privacy in. A shift of attitude is necessary about privacy within government. If it is part and parcel of decision-making from the very early conceptualisation of a project, then more profound questions may be asked about whether the same goals could be achieved without the collection and processing of identifiable personal information. The basic architecture of information systems can be designed to be privacy invasive or privacy friendly.

4.4.13 The Commission invites comment from all interested parties, but especially from government departments, in this regard.

CHAPTER 5: SPECIFIC AREAS OF CONCERN

5.1 Introduction

5.1.1 During the course of the investigation it became clear that there were some issues that needed closer attention. In this chapter some of these areas will be reviewed. **Readers are invited to draw the attention of the Commission to further issues in need of investigation**.

5.2 Access to information v privacy rights

5.2.1 The question has been raised whether the rights to access to information and data protection are conflicting principles or complementary rights.

5.2.2 Tilley states that one should be very concerned with any conflicts that arise that would limit access to information.[1] Marc Rotenberg,[2] 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]

5.2.3 Freedom of information and privacy/data protection should rather be seen as different, but complementary aspects making up the "wholeness" of human rights.[4] However, the perception

---

1 Tilley A "Data Protection in South Africa and the Right to Access to Information: An Inescapable Clash?" Submission to the SALRC dated 26 August 2002. She refers to a discussion with an official from the Ministry of Sweden who indicated that the EU Directive's provisions (protecting privacy) regarding the processing of data appear too comprehensive and complicated. The difficulties seem to be mostly associated with the fact that the provisions may impose on the commonplace processing of personal data in the form of sound and image data and in continuous text, for example in the use of e-mail or the Internet.

2 Director of Computer Professionals for Social Responsibility, Washington DC.

3 Piller at 6.

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

of the public is critical and it is true that two competing constitutional rights are at stake here. These rights are interactive and need to be balanced.

5.2.4 Sec 32 of the **Constitution** provides a right of access to information. [5] It reads as follows:

(1) Everyone has the right to 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.

5.2.5 **The Promotion of Access to Information Act**, 2002[6] ("PAIA") was enacted in accordance with sec 32(2). [7] The Act regulates both publicly and privately held[8] information and overrides other pieces of legislation in the matter of access to information.

5.2.6 It should, however, be made clear that PAIA is not to be regarded as a data protection or privacy statute.[9] It does 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. [10]

---

5 As stated above Sec 14 of the Constitution provides for the protection of the right to privacy, hence the two rights will have to be balanced.

6 Act 2 of 2000.

7 The right to freedom of expression converges with the right of access to information as the former right includes the freedom to receive information and ideas. Sec 16(1)(b) of the Constitution.

8 "Concerns Raised over Access to Information Act," ***Mail and Guardian***, May 10, 2001.

9 Klaaren J & Penfold G "Access to Information" in Chaskalson M, Kentridge J, Klaaren J, Marcus G, Spitz D & Woolman S (reds) ***Constitutional Law of South Africa*** 2ed Juta Kenwyn 2002 (hereafter referred to as "Klaaren in Chaskalson et al") at 62-9 states that data protection legislation performs three functions: it prevents unauthorised disclosure and use of private information; it allows for the correction of personal information held by another body; and it allows for access to one's own information. The focus of such legislation is on the protection of privacy and not on access to information; See further the discussion on data protection principles in Chapter 6 below.

10 Klaaren in Chaskalson et al at 62-9.

5.2.7 Nevertheless, the PAIA does not contain a general prohibition on the disclosure of certain categories of information. It merely provides for mandatory grounds of non-disclosure in relation to requests under the Act. The role of privacy in the PAIA is merely a restriction on the right of access to information. In this way it gives effect to the constitutionally protected right to privacy.[11]

5.2.8 A person who complies with the procedures set out in the Act is entitled to access to the records of both public and private bodies if there is no ground upon which access to that record can be refused in terms of the Act.[12] In so far as public bodies are concerned a requester is entitled to the information irrespective of his or her reasons for seeking it,[13] but in so far as private bodies are concerned, the record has to be required for the exercise or protection of any rights.

5.2.9 The fact that a requester requesting access to the record of a public body does not have to indicate the purpose for which the record is requested means that even if access is requested for purposes other than the protection of a right of interest, the request is not invalid. In fact, section 11(3) provides that a requester's right of access to the record of a public body is not affected by the reasons given for the request or the information officer's belief as to what the reasons are. A request may however, be denied if it is manifestly frivolous or vexatious.[14]

5.2.10 There are also other grounds upon which access to records must or may be refused, one of which is a request for information that would involve the unreasonable disclosure of personal information about a third party. [15] A list of exceptions is, however, included[16] to provide for

---

11 Klaaren in Chaskalson et al at 62-9.

12 Sec 11(1).

13 Sec 11(3).

14 Sec 45 of the Act; Visser at 254.

15 Sec 34(1) and 63(1) for public and private bodies respectively.
Sec 34(1) provides as follows:
34 Mandatory protection of privacy of third party who is natural person

(1) Subject to subsection (2), the information officer of a public body must refuse a request for access to a record of the body if its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.

Sec 63(1) provides as follows:
63 Mandatory protection of privacy of third party who is natural person

(1) Subject to subsection (2), the head of a private body must refuse a request for access to a record of the body if its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.

those instances in which these grounds of refusal will not apply. Personal information is defined in the Act. [17]

---

16 Sec 34 (2) and 63 (2) for private and public bodies respectively.
Section 34(2) provides as follows:

(2) A record may not be refused in terms of subsection (1) insofar as it consists of information-

(a) about an individual who has consented in terms of section 48 or otherwise in writing to its disclosure to the requester concerned;
(b) that was given to the public body by the individual to whom it relates and the individual was informed by or on behalf of the public body, before it is given, that the information belongs to a class of information that would or might be made available to the public;
(c) already publicly available;
(d) about an individual's physical or mental health, or well-being, who is under the care of the requester and who is-
  (i) under the age of 18 years; or
  (ii) incapable of understanding the nature of the request, and if giving access would be in the individual's best interests;
(e) about an individual who is deceased and the requester is-
  (i) the individual's next of kin; or
  (ii) making the request with the written consent of the individual's next of kin; or
(f) about an individual who is or was an official of a public body and which relates to the position or functions of the individual, including, but not limited to-
  (i) the fact that the individual is or was an official of that public body;
  (ii) the title, work address, work phone number and other similar particulars of the individual;
  (iii) the classification, salary scale, remuneration and responsibilities of the position held or services performed by the individual; and
  [Sub-para. (iii) substituted by s. 31 of Act 42 of 2001.]
  (iv) the name of the individual on a record prepared by the individual in the course of employment.

Sec 63 (2) provides as follows:
(2) A record may not be refused in terms of subsection (1) insofar as it consists of information-

(a) about an individual who has consented in terms of section 72 or otherwise in writing to its disclosure to the requester concerned;
(b) already publicly available;
(c) that was given to the private body by the individual to whom it relates and the individual was informed by or on behalf of the private body, before it is given, that the information belongs to a class of information that would or might be made available to the public;
(d) about an individual's physical or mental health, or well-being, who is under the care of the requester and who is-
  (i) under the age of 18 years; or
  (ii) incapable of understanding the nature of the request,

  and if giving access would be in the individual's best interests;
(e) about an individual who is deceased and the requester is-
  (i) the individual's next of kin; or
  (ii) making the request with the written consent of the individual's next of kin; or
(f) about an individual who is or was an official of a private body and which relates to the position or functions of the individual, including, but not limited to-
  (i) the fact that the individual is or was an official of that private body;
  (ii) the title, work address, work phone number and other similar particulars of the individual;
  (iii) the classification, salary scale or remuneration and responsibilities of the position held or services performed by the individual; and
  (iv) the name of the individual on a record prepared by the individual in the course of employment.

17 Sec 1 of Act 2 of 2002. See above in Ch 2.

5.2.11 This state of affairs may create a threat to the privacy of the individual and can be seen as motivation for the enactment of privacy legislation making provision for privacy protection principles. Privacy legislation, on the other hand, may in turn encroach on the right to access. A balance has to be found. Whether an infringement of a right can be justified is decided according to the criteria set out in sec 36 of the Constitution. Appropriate evidence must be led as to whether the infringement is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.[18]

5.2.12 It is important to note that the PAIA only prohibits the "unreasonable" disclosure of personal information. The crucial question in applying these provisions will therefore be whether, in the relevant circumstances, disclosure will be unreasonable.[19]

5.2.13 The disclosure of information of a third party will only amount to an infringement of the right to privacy where the third party can be said to have a legitimate or reasonable expectation of privacy in relation to the particular information.[20] In the next stage of the investigation (determining whether the disclosure is unreasonable) all the surrounding circumstances, including the strength of the third party's privacy interest, the nature of the particular record and the importance of the purpose for which it was requested will have to be examined.[21] Access to personal information of a third party should be granted only when "on balance , the public interest that the request should be granted outweighs the public interest that the right to privacy of the individual to whom the information relates should be upheld".

5.2.14 An interesting example of possible conflict between access and privacy is that of the new health care draft Bill (NHB).[22] Sec 14 of the Bill protects a patient's privacy/confidentiality to a far greater extent than the PAIA does. The PAIA has been interpreted to include parental access to a child's file under any circumstances while this is not permitted in terms of sec 16(1) of the NHB. PAIA also does not make provision for instances where there is a dispute between family members

---

18 See discussion in Ch 3 above.

19 Klaaren in Chaskalson et al at 62-20.

20 See the discussion on the right to privacy in Ch 3 above.

21 Klaaren in Chaskalson et al at 62-20.

22 National Health Bill dated 9 November 2001.

as to whether a file should be accessed or kept confidential.[23]

5.2.15 Like the right to access, the right to privacy must always be balanced against other interests. Many interests involved in balancing access and privacy are the same: national security, law enforcement, and the operational requirements of government. Interests in access and privacy are constantly balanced against each other.[24]

5.2.16 A solution to the conflict between the right to information and the right to privacy as expressed in data protection may also be reached by another route. One option may be a systemic solution to the problem in that the mechanism for enforcing the provision of the access regime and the data protection regime is one and the same. In the United Kingdom one would therefore find an Information and Data Commissioner dealing with both access to information and data protection.

5.2.17 Do readers regard the rights to access of information and data protection as conflicting principles or as complimentary rights? How should the data privacy legislation interact with the existing privacy sections in the Promotion of Access to Information Act?

5.3 Crossborder data transfers

5.3.1 Another imperative is that of transborder flow and data havens.[25] The ease with which electronic data flows across borders leads to a concern that data 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 data could then be processed in those countries, frequently called "data havens," without any limitations.

5.3.2 For this reason, most data protection laws include restrictions on the transfer of information to other countries unless the information is protected in the destination country. For example, Article 12 of the Council of Europe's 1981 Convention places restrictions on the transborder flows of

---

23 Klinck E Legal Adviser of the Human Rights, Law and Ethics Unit, SAMA, in a letter to the Department of Justice dated 26 November 2001.

24 At 22.

25 See discussion in EPIC Report 2002 at 14 and the references made therein.

personal data.[26] Similarly, 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.[27]

5.3.3 The European Union and all its trading partners are required to have adequate data protection regimes, conforming to the European Data Protection Directives, with effect from 24 October 1998. [28] This means that transfer of data from the EU to both private and governmental bodies will normally only be permissible with countries which have acceptable data protection legislation or selfregulation covering the principles outlined in Chapter 6.[29]

---

26 Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, 1981, available at <http://www.coe.fr/eng/legaltxt/108e.htm>.

27 See Bygrave 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.

28 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.

29 DMA Submission on Open Democracy Bill.

5.3.4 The following points should be noted:[30]

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 data transfer operation, including:

- the nature of the data;
- the purpose and duration of the data processing and transmission operation;
- the rules of law in force; and
- the professional rules and security measures established for the data.

5.3.5 Article 26 identifies the circumstances under which an EU member nation can authorise transfer in the absence of an adequate level of data protection, including:

a) the data subject has given consent to the transfer unambiguously. (It is not clear whether assent is required, or if notice with the opportunity to opt out is sufficient)

b) the company receiving the data establishes privacy rights through appropriate contractual clauses. [31]

5.3.6 On July 26, 2000 the European Commission ruled that both Switzerland and Hungary provide "adequate" protection for personal information and therefore that all transfers of personal data to these countries could continue.[32] In January 2002, the European Commission recognized that the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

---

30 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").

31 See further Bygrave 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.

32 See European Commission Press Release, "Data protection: Commission adopts decisions recognising adequacy of regimes in United States, Switzerland and Hungary," July 27, 2000, available at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm.

provides adequate protection for certain personal data transferred from the European Union to Canada. The Commission's decision of adequacy does not cover any personal data held by federal sector or provincial bodies or information held by personal organizations and used for non-commercial purposes, such as data handled by charities or collected in the context of an employment relationship.[33] The Commission is currently looking into the privacy protection schemes in several other non-European Union countries, including New Zealand, Australia, and Hong-Kong.[34]

5.3.7 Although the 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.

5.3.8 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.[35].

5.3.9 The United States strongly lobbied the European Union and its member countries to find the United States system adequate. In 1998, the United States began negotiating a "Safe Harbor" agreement with the European Union in order to ensure the continued transborder flows of personal data. 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 data 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.[36]

---

33 See EPIC Report 2002 at 17 and reference to Commission Decision of December 20, 2001, Official Journal of the European Communities L 2/13 available at http://www.europa.eu.int/comm/internal_market/dataprot/adequacy/canada-faq_en.htm

34 Safe Harbor List http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

35 See EPIC Report 2002 at 17 and reference to Schwartz PM and Reidenberg JR ***Data Privacy Law*** Michie 1996.

36 EPIC 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.

5.3.10 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 data from Europe.

5.3.11 On July 26, 2000, the Commission approved the agreement.[37] Over 200 companies have joined the Safe Harbor. [38]

5.3.12 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 choose (opt out of) the collection of data 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) to the collection.
- Organisations wishing to transfer data 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 data.
- 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.

---

37 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.

38 Safe Harbor List http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

5.3.13 Privacy advocates and consumer groups both in the United States and Europe are highly 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 data. The agreement rests on a self-regulatory system whereby companies merely promise not to violate their declared privacy practices. There is little enforcement or systematic review of compliance. The Safe Harbor status is granted at the time of self-certification. There is no individual right to appeal or right to compensation for privacy infringements. There is an open-ended grace period for United States signatory companies to implement the principles.[39]

5.3.14 In February 2002 the European Commission issued a report on the practical operation of the European Union-United States Safe Harbor Agreement.[40] 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. The Commission will issue a full evaluation of the agreement in 2003.

5.3.15 In July 2002, the Article 29 Data Protection Working Party issued a working paper on the functioning of the agreement. In it, the Working Party expressed its intention to study the agreement in further detail with particular regard to "possible gaps between the principles…and the implementing practices" and also "the transparency requirements to be met by organisations." The Working Party called on all authorities, organisations and companies concerned to enhance compliance and awareness of the Agreement.[41]

5.3.16 Another possible way to protect the privacy of information transferred to countries that do not provide "adequate protection" is to rely on a private contract containing standard data protection

---

39 EPIC Report 2002 at 18.

40 European Commission Staff Working Paper, February 2002, available at http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf>

41 "Working Document on the Functioning of the Safe Harbor Agreement," Article 29 Data Protection Working Party, 11194/02/EN, July 2, 2002, available at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp62_en.pdf

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 data transferred from the European Union, the contract would have to meet the standard "adequacy" test in order to satisfy the Data Protection Directive.[42]

5.3.17 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.[43]

5.3.18 The requirements set out in the EU Directive have resulted in growing pressure outside Europe for the passage of strong data protection laws. Multinational companies would be unable to function if their international data links were disrupted. 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 data.

5.3.19 It is also important to consider that the transfer of data 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.

5.3.20 Would it adversely affect the country's international trade if a data privacy model is adopted for South Africa that is not regarded as "adequate" in terms of Article 25 of the EU Directive? If so, how?

5.4 Consent: the opt-in, opt-out debate

42 EPIC Report 2002 at 16.

43 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.

.

5.4.1 It has been stated that data processing is lawful where the data subject has consented to it. Consent may be explicit, as when the data subject expressly consents to the use of his or her information as part of the data 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 data. [44] These two possibilities are sometimes explained in terms of the so-called opt-in and opt-out conditions.

5.4.2 One option is that in order to protect privacy, the government should prohibit the use of personal information unless consumers "opt in" by giving their explicit consent for each and every use. [45] Under the "opt out" regime personal information about an individual may be freely used within defined legal limits as long as the individual does not "opt out" of the use.

5.4.3 It has been argued[46] that the "opt in" option offers no greater privacy protection than allowing consumers to "opt out" of uses of information to which they object, yet it imposes significantly higher costs on consumers, businesses, and the economy as it restricts the flow of information on which we all depend. It should therefore rather be reserved for exceptional situations where the risk of those costs and consequences is justified.

5.4.4 Free-flowing information is an essential component of any economy. Many of the characteristics of the "New Economy" (e.g.,just-in-time-delivery, total quality management, electronic commerce), and virtually all sectors experiencing strong growth, depend on the speedy, efficient availability of reliable information. So, too, do nearly all social and professional interactions. As many scholars have stressed: "Information is the lifeblood that sustains political, social, and business decisions." [47]

5.4.5 The Federal Reserve Board reached a similar conclusion in its 1997 report to Congress regarding consumers' personal financial information: "[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society

---

44 See discussion on consent as an element of the collection limitation principle in Ch 6 below.

45 This may, however, be considered to be an unreasonable limitation of opposing rights.

46 Cate F H & Staten M E "Protecting Privacy in the New Millennium: The Fallacy of "opt-in" at 3 as referred to by Barnard F in a submission to the Commission dated 16/7/2001(hereafter referred to as"Cate").

47 Branscomb AW Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition, 36 Vanderbilt Law Review 985, 987(1983) as reffered to in "Cate".

and market economy."[48]

5.4.6 One of the most severe restrictions on information flows would be the adoption of laws prohibiting the use of information about an individual unless the individual "opts-in" to the use by expressing affirmative consent. Only in the narrowest of circumstances where privacy interests might legitimately thought to be at their highest (e.g., certain uses of medical information or the use of credit reports for employment purposes) is affirmative consumer consent required today for the use of personal information.

5.4.7 "Opt in" and "opt out" both give consumers the final say about whether his or her information is used.

5.4.8 The opposite argument is that it would be questionable whether implied consent could be inferred from a failure to opt out or from an individual's objection to a proposal. Failure to object does not imply consent in these circumstances because it will not be clear that the individual exercised an informed choice (for example, the individual may have thrown the form in the bin without reading it). It will also often not be clear that the individual's failure to respond was a positive decision. In many cases it will be likely that the individual did not respond because doing so involved cost or too much effort.[49]

5.4.9 Consent can only be inferred from an individual's failure to opt out if all of the following conditions are met (and even then, not in all circumstances):

- the organisation has a direct ongoing relationship with the individual;
- opting out is part of the contact that the organisation would be making anyway with the individual (for example, to pay a bill online);
- the individual fully understands the implications of opting out;
- opting in or opting out is freely available and not bundled with other purposes;
- there is no financial cost to the individual in receiving the chance to opt out and

---

48 Board of Governors of the Federal Reserve System, ***Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud*** 2 (1997).

49 Office of the Federal Privacy Commissioner ***Draft National Privacy Principles Guidelines*** A Consultation document Australia 7 May 2001 (hereafter referred to as "Federal Commission Guidelines") at 28 available at http://www.privacy.gov.au/publications/dnppg.html accessed on 2/4/2003..

involves little effort

- the consequences of failing to opt out are harmless (for example, the individual continues to receive offers, but disclosures to another party would not be harmless); and
- if the individual opts out late the individual is fully restored to the circumstances he or she would have been if the opting out had been exercised earlier.

5.4.10 It is, however, true that there is a stark difference between "opt in" and "opt out" in terms of cost. An "opt-out" system presumes that consumers do want the convenience, range of services, and lower costs that a free flow of personal information facilitates, and then allows people who are particularly concerned about privacy to block the use of their information. Put another way, the "opt-out" system sets the default rule to "free information flow" and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an "opt-in" system presumes that consumers do not want the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.

5.4.11 In other words, an "opt-in" system sets the default rule to "no information flow". Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must rebuild the pipeline by contacting one customer at a time to gain their permission to use information.

5.4.12 Consequently, an "opt-in" system for giving consumers control over information usage is always more expensive than an "opt-out" system. Opt in requires that every consumer be contacted to gain explicit permission. Under opt out, contact only occurs for those consumers who wish to withhold permission. Opt in is more costly precisely because it fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them

5.4.13 It is therefore argued that "opt in" impedes economic growth by raising the costs of providing services and consequently decreasing the range of products and services available to consumers.[50] While individual consumers may "opt out" of a specific information use without making

---

50 To illustrate the cost of setting a default rule that halts the free flow of information, consider the experience of U.S. West, one of the few U.S. companies to test an "opt-in" system. In obtaining permission to utilize information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.), the company found that an "opt-in" system was significantly more expensive to administer, costing almost $30 per customer contacted. To gain permission to

the overall provision of services based on that use economically untenable, it is far more difficult to create and market new services based on building up a base of consumers who have decided, when contacted, to "opt in" to the necessary information exchange.

5.4.14 An "opt-out" system allows individuals with privacy concerns to prohibit certain uses of their information, but it also permits people who are less concerned about the privacy of basic information, such as that used in most direct marketing, to learn about new services and products they might value. In an "opt-in" system, all consumers (not only those who are sensitive to their privacy protection) lose many opportunities to take advantage of information-dependent services, whether instant credit, targeted marketing, unified frequent travel programs, or personal shoppers.

5.4.15 In short, "opt-in" systems impose extra costs on everyone, regardless of privacy-sensitivity, as compared to "opt-out" systems. Restrictions on information flows inevitably restrict the range of opportunities to which consumers will be given the chance to consent in the first place. Businesses incur higher costs of finding new customers because they must rely on mass advertising, mailings and telephone calls rather than targeting their marketing efforts at consumers who are likely to be interested. In addition, the lack of readily available personal information denies firms a key tool used to prevent and detect fraud, putting further upward pressure on costs, and ultimately prices.

5.4.16 "Opt-in" systems are furthermore contrary to consumer expectations and behavior. The vast majority of the public does not object to the reasonable use of information about them if they know that they can "opt out" of such uses should they choose to.

5.4.17 It is, however, accepted that “opt in” should be reserved for situations where the risk of those costs and consequences is justified. One example might be in the collection of data from children on the Internet. Another might be in the release of medical records for a variety of purposes. Moreover, the indiscriminate use of "opt in" means that this exceptional privacy protection will no longer signal that a particularly significant privacy interest is at risk.

---

use such information for marketing, U.S. West determined that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. Consequently, many U.S. West customers received more calls than in an "opt-out" system, and one-third of their customers were denied opportunities to receive information about valuable new products and services.

5.4.18 In summary, legislators and policymakers should carefully consider the costs associated with an "opt-in" regime. Those costs are measured not only in economic terms (higher prices and lost opportunities), but also in additional burdens on consumers and businesses alike, and infringement upon the open flow of information.

5.4.19 In a submission to Parliament[51] the Edgars group[52] indicated that legislation dealing with the disclosure and usage of information held on private databases could impact significantly on their business in the context of individual consent to disclosure of information. The number of accounts held would make it extremely difficult, if not impossible, to obtain the express consent of each and every account holder for purposes as contemplated in legislation.

5.4.20 They accept and commit themselves in principle to the rights of individuals to object to the use of disclosure of their personal information to third parties unless they have consented to such use or disclosure, but must in this regard stress the enormous administration and cost burden on themselves if the Act intends to regulate the exact manner (prescribed from/prescribed manner) that such consented use, disclosure or denial thereof must be embodied in.

5.4.21 In framing the legislation the administrative and practical issues should be borne in mind. The administrative activities and costs associated with obtaining the express consent of customers would be enormous. It can be submitted that imposing on the database holder the obligation to give effect to the specific instructions of a customer (ie expressly to record their denial or consent) would be far more appropriate than imposing on the database holder the obligation to obtain the express consent of the customer.

5.4.22 In terms of the ECT Act advertisers must give consumers the option of being removed from their mailing lists. If they still bombard people with spam despite being asked not to, they will be guilty of a criminal offence and risk a fine or jail term. Spammers must also reveal where they

---

51 Submission made in response to the discussion of the Open Democracy Bill in Parliament.

52 NV Toerien, Group Secretary and Legal Council in letter dated 7 August 1998. The Edgars Group is a leading speciality retailer of clothing, footware and accessories. The group trades under the style Edgars, Sale House, Jet, Cuthberts and ABC throughout South Africa from some 600 trading outlets. Edgars Group of companies has a base in excess of 3,6 million customer account holders. Edgars Group relies heavily on these account holders for a substantial portion of merchandise sales. They use the postal services to communicate with these customers on a regular basis inter alia to send them monthly statements to inform them of any promotions, sales or general information which is relevant to them.

obtained details when asked so that recipients can contact the source and make them stop selling their personal details. Contravening the rules will constitute an offence punishable by a fine or up to a year's imprisonment.[53]

5.4.23 The Commission requires the guidance of our readers in this respect. Do you think that the opt-out approach can constitute valid consent? If so, why? If not, why not? What are the implications for consumers and organisations for allowing opt-out consent in the circumstances outlined above?

5.5 Data sharing

a) Private data users

5.5.1 Data can be shared, traded or rented. A company should, however, not share data with a third party unless the individual has given permission or unless it is for the furtherance of a legitimate private interest or public interest. Even with permission it should furthermore only be shared with carefully chosen, reputable and trustworthy third parties.[54]

---

53 Sec 45(1) (b) of the ECT Act reads:
Unsolicited goods, services or communications

45. (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) .....
(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribe in sec 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).

Sec 49 reads as follows:
Complaints to Consumer Affairs Committee

49. A consumer may lodge a complaint with the Consumer Affairs Committee in respect of any non-compliance with the provisions of this Chapter by a supplier.

54 Telegraph Privacy Policy.

5.5.2 The data user may also provide aggregate statistics on their customers, sales, traffic patterns and related site information to reputable third-party vendors, but these statistics will include no personally identifying information.[55]

5.5.3 The company or database owner that gathered the information in the first instance should be the curator of that particular information. At the time of gathering the information the holding company should have obtained the necessary permission from clients as to sharing, etc., of information.[56]

5.5.4 It is quite possible that different companies have almost the same information about numerous customers who conduct business in different environments. In each case the particular database owner has a vested interest in and becomes the curator of the clients' information.

5.5.5 The South African Insurance Association (SAIA)[57] has instituted a shared claims database on behalf of the industry. The purpose is the sharing of data to combat fraud. Insurance fraud is estimated world-wide to add between five and fifteen percent to the cost of insurance premiums. Honest consumers are therefore carrying the cost of this fraud.

5.5.6 The operation has been outsourced to Information Trust Corporation (ITC), the largest SA credit bureau and brokers will also be an integral part of the initiative. They have created a user-

friendly system that will make it easier to identify and eliminate fraudulent claims in the short-term industry.[58]

---

55 Telegraph.Privacy Policy.

56 Barnard F "Informal Notes from the DMA to the Law Commission re a Possible New Data Privacy Act for South Africa " 14 September 2001 at 3.

57 SAIA promotes the short-term insurance industry in order to create an awareness and understanding of the industry. It represents almost all of the short-term insurance companies and is authorised to negotiate on their behalf. SAIA members abide by a Code of Conduct.

58 In the test phase, historical data from two organisations has been run using the ID number to identify duplicate claims. From the 15 000 profiles, 181 duplicate claims were detected. These duplicate claims amounted to R1 447 902. On further investigation, 28% of these were multiple claims, and 70% of all duplicate claims were related to vehicle insurance. The South African Insurance Association ***Annual Review*** May 2000 - April 2001 (hereafter referred to as " SAIA Annual Review") at 19.

5.5.7 Future phases of the project have been identified as follows:[59]

(a) The use of the system for underwriting.

(b) An interface with the South African Fraud Prevention Service database, a database aimed at combating fraud within the broader financial services industry through the sharing of known attempts by consumers to commit fraud against the institution.

(c) An interface with data provided by the Vehicle Security Association (VESA), including a database of after-market vehicle security devices fitted to insured vehicles.

(d) An interface with the Department of Transport National Traffic Information System (NaTIS), giving access to vehicle and drivers licence data.

(e) The use of data on service providers and third parties involved in the claim process to detect fraud perpetrated by service providers.

(f) An interface to the Department of Home Affairs databases giving access to identity number information and cross-border movement of vehicles and persons.

(g) An interface to South African Police Service stolen and recovered vehicle data.

(h) An interface to details of claimants against the Road Accident Fund.

(i) Provision of lapsed policy information to the banks to allow banks to protect encumbered assets, in particular motor vehicles.

5.5.8 The first phase of the system became operational in May 2001.[60] The system targets three categories of fraud: consumers, service providers such as loss adjusters, doctors and lawyers and the insurance industry itself.

5.5.9 In an article in ***Business Day***, [61] different views regarding this new development were canvassed:

(a) Webber Wentzel Bowens constitutional lawyer Glenn Penfold is quoted as saying that insurance companies should obtain proper and informed consent from policy-

---

59 SAIA Annual Review at 9.

60 Ibid.

61 Temkin S "Insurers provoke fears with information-sharing" ***Business Day*** 3 August 2001 (hereafter referred to as "Business Day article").

holders. He says that although the companies could have defences, they could face legal action under common law for breach of privacy in the absence of proper consent.[62] According to the article some insurance companies sent policy-holders endorsements to their policies, stating that the database had been implemented and that their right to privacy had been waived to allow the sharing of information. These endorsements did not require direct authorisation by the policy-holders.

(b) Consumer Institute director John Bizos says that the endorsements have been incorporated into policy-holders' policies "contrary to any written instructions from clients". He fears that the industry may eventually extend the database " to more than just the sharing of claims information".

(c) Sanlam's head of marketing, Steve Zietsman, says that his company will respect existing policyholders's refusals to allow the waiving of their rights to privacy, but that potential policyholders would be turned down by Sanlam and possibly other short-term insurers to whom they may turn.

(d) Francois Barnard, director of the Direct Marketing Association, says that database owners should respect their client's right to privacy. He says that owners may reason that they have implied consent from their customers to use and share information. They may also argue that unless their customers have not specifically asked for their information not to be shared, they have "de facto" consent to share this information. Barnard says, however, that this would constitute "short-term folly with serious long-term implications".

5.5.10 In its comment on section 55 of the Open Democracy Bill the South African Chamber of Business (SACOB)[63] indicated that if personal information could not be exchanged between companies of the same group it will pose considerable and unnecessary costly administrative difficulties for certain companies engaged in retail credit operations. It was suggested that a sub-section be included so as to permit such access to a common database.

5.5.11 Amid all the debate about how to protect people's personal information as it's bandied about

---

62 Business Day article.

63 Submission on Open Democracy Bill dated 12 Augustus 1998; SACOB consists of 90 individual Chambers and 60 Association Members represents some 40 000 business, large and small throughout SA.

the Web, a new protocol is in the works that aims to give web-based businesses a means of trading this information online.[64]

5.5.12 Re-using and redistributing information and assets from one website to another is an ad hoc and expensive process. Before successfully transferring any data and managing the relationship, both ends must agree on a common protocol and management model. The Information Content & Exchange Protocol (ICE) will now provide businesses with a standardised method for exchanging users' personal information, preferences and other types of data related to online business. The protocol is also designed to automate the process of negotiating the terms and conditions of syndication for this information. Before ICE is able to accomplish this, it will however need to be integrated with other existing web protocols.

5.5.13 The W3C's Platform for Privacy Preferences (P3P) is a protocol that allows a website to reach an understanding with a user about what personal information will be shared and collected; that information, in turn will become a user's "profile" for that particular site. When ICE is combined with P3P, web-based organisations will not only be able to collect user's personal profiles, but will be able to exchange them, creating virtual trading cards of information. ICE can also be used to automate the distribution of the demographic information of a site, transforming its users' data into a new variety of syndicated content.

5.5.14 JavaSoft, Sun Microsystem's software division, is a member of the ad hoc ICE working group and both a syndicator of web content and an aggregator of other companies' information. It publishes content for use by its distributors and resellers, by various mirror sites. ICE aims to facilitate trade in profiles, but only with explicit consumer consent, as established during a P3P negotiation between a consumer and a website.

5.5.15 Should institutions be allowed to share data, and if so, in what circumstances? What should the consent requirements be in this regard? In sharing data, who is responsible for the accuracy and maintenance of the data? What are the views and experiences of consumers regarding the accuracy of data being collected?

---

64 Rein L "Your data as online commodity" ***Wired News*** June 2 1998 available at www.wired.com/news/technology/ accessed on 4/2/2002

b) Public data users (e-government)

5.5.16 E-government is a specific example of data-sharing.[65] It enables a world of joined up services and coordinated responses by government. The question is how do we decide when privacy risks outweigh service benefits.[66] Is e-government only doing what we already do in the same way as we have done it but only using electronic means, or is it recognising the new technology as a means of rethinking how government delivers services?[67]

5.5.17 Areas of government in which data sharing may be relevant are defence, immigration, foreign affairs, social security, telecommunications, taxation, justice (courts and police), education (schools and tertiary institutions), health (hospitals) infrastructure and investment (roads, transport, business), natural resources, local government (building regulation, sanitation, community health and recreation, animal and pest control).

5.5.18 E-government may be much more than the online interface of government. It may provide the opportunity for the complete transformation of government. The Department of Justice in Australia is , for example, implementing a system to enable a fully electronic flow of records and documents from initial contact with police through courts and corrections. There is also a major project planned to implement a fully electronic health record in Victoria to enable efficient and timely transfer of patient records between doctors and hospitals. This provides safety and economic benefits for patients - speeding diagnosis, minimising repeat testing risks and unnecessary costs.[68] South Africa has embarked on a similar project.

5.5.19 Benefits include improved efficiency, reduced time and cost for all parties, including the

---

65 Hodgkinson S "Whither Privacy with e-Governmen?t" Presentation at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002 (hereafter referred to as "Hodgkinson").

66 Hodgkinson at 1.

67 Frith R " Data Sharing - The Key to E-government" Presentation at the 24th International Conference of Privacy and Data Protection Officers, Cardiff, 9-11 September 2002 (hereafter referred to as "Frith").

68 Hodgkinson at 11.

private sector. It will eliminate multiple requests for the same information. Customers are tired of:

- having to visit or call many offices/ agencies for related services
- having to prove repeatedly who they are
- filling in endless forms
- repeating their story at each point of contact

Sharing of data can also detect fraud or, if used earlier, prevent fraud and deter future fraud.[69] Opportunity exists to enhance social planning by better sharing or existing data held by different parts of government.[70]

5.5.20 The question can, however, be asked whether seamless government and privacy could be regarded as friends or foes. [71] Challenges that should be addressed are the question of public trust, data accuracy and data security. These are, however, challenges to overcome rather than reasons not to proceed.[72]

5.5.21 The government needs public trust for the successful implementation of its e-government programme.[73] The government has special privacy obligations [74] arising from the fact that they are handling sensitive information (criminal, health, taxes etc). They furthermore have a special position of trust and there exists a huge power difference between government and citizen. The government is the monopoly service provider: customers are obliged to deal with government for many services and cannot necessarily choose to "opt in " or "opt out" of a new service when government is the only provider.

---

69 Frith at 4.

70 Frith at 5.

71 Findings from Focus Groups, Research done by Dr Perri 6, Director, The Policy Programme, Institute for Applied Health and Social Policy, King's College, London and Consultant to the Performance and Innovation Unit of behalf of the Unit in its Project on privacy and data sharing "Strategies for Reassurance: Public Concerns about Privacy and Data Sharing in Government" published at http://www.cabinetoffice.gov.uk/innovation/2002/privacy/report/papers/perri6.pdf. (hereafter referred to as "Perri Focus Groups ").

72 Frith at 6.

73 Perri 6 "Seamless Government and Privacy - Friends or Foes? Issues of Public Trust" Presentation at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002 (hereafter referred to as "Perri Public Trust").

74 Hodgkinson at 12.

5.5.22 Fragmented organisational structures and systems and a culture of respect for the privacy of personal information have traditionally protected privacy. The imperative is to ensure that joined-up e-Government models do not unacceptably reduce privacy.[75]

5.5.23 Results from an investigation done for the cabinet office in the United Kingdom[76] suggested that the public's perception of e-government is not really positive. In general, the key findings on benefit perception are that:

- the benefits perceived from data sharing are relatively few in number;
- at least without a great deal of thought, people cannot identify many ways in which they personally benefit;
- those things which they do see as personal benefits are not necessarily of overwhelming importance to them;
- those who attach greatest weight to the benefits to government are the ones who use public services least frequently;
- the possibility - let alone the benefits - of personalisation of public services has not yet reached the public consciousness

5.5.24 The following risks were identified:[77]

- errors in data handling;
- infection with inaccurate data;
- misidentification;
- rigidity in the data structure and handling, rigid services;
- malicious provision of data from anonymous sources;
- reversal of the presumption of innocence;
- unjust inference (eg jumping to conclusions, decisions to deny entitlement unfairly based on inferences from matched data, where each of the elements matched might have been correct in its original context but where the combination is misleading;
- "soft" data (eg professionals' opinions or assessments of individuals as clients);
- unauthorised access to personal information;

---

75 Hodgkinson at 12.

76 Perri Focus Groups at 26.

77 Perri Focus Groups at (x).

- unauthorised informal disclosure of personal information;
- arbitrary use of power;
- failure to identify criminals, people not entitled to services but claiming or using them etc; and
- being subject to unacceptable physical oversight (eg being seen in public to be a user of certain stigmatised public services).

5.5.25 The following challenges for government seem to be of particular importance and urgency in any programme of policy-making around data sharing:

– demonstrating that regulating authority exists and can effectively administer sanctions upon government departments and agencies which engage in data sharing in ways that violate privacy principles;
– offering the public concrete and clear reasons to believe that what they are shown, when they exercise their rights of subject access (rights to be told what information is held about them), is indeed the true and complete record, and communicating convincingly to the public that sanctions for the provision of misleading information are sufficient, credible and effective;
– providing convincing security support for on-line real-time subject access schemes (that is providing subject access through the Internet or a digital television to the immediate and current record about them , rather than a printout of something that is up to four weeks old;
– demonstrating to the public that refusals of consent will not be so interpreted as, automatically, to trigger investigation, and still less to lead to the reversal of the presumption of innocence - that is, that privacy concerns will be accepted as a valid reason for refusing consent, unless there is independent ground for suspicion about a person who is the subject of data;
– demonstrating to the public that levels of security and authorisation for staff access to personal information are managed effectively;
– designing multifunctional smart card schemes in ways that provide for the disabling of lost and stolen cards and for the reconstruction in any replacement card of the complete data set in the lost or stolen card as it was immediately prior to cancellation;
– convincing the public that data taken from reader devices on the uses of particular cards will not be put together to form profiles of particular individuals on any ascribed categorical

basis, but will be done only in individual cases where there is already independent reason for suspicion of crime;

– convincing the public that voluntary codes of practice for government departments and agencies will carry effective sanctions for violations that make those codes credible and worthwhile; and

– convincing the public that the power of parliamentary and media scrutiny over data sharing is sufficient, that legislators and the executive will take the issue of risks in data sharing seriously.

5.5.26 In Ireland government is trying to reconcile two central, but opposing principles :

– customer data is "owned" by the customer to the maximum extent possible

– customer data is stored and shared for re-use to the maximum extent possible

5.5.27 Smart card technology[78] is now found in multiple services and applications. It is used by the police, national security, banks, employment, hospitals, airports, tax authorities, phone companies, car registration, national insurance, utilities. The question is whether it is possible to provide secure and efficient identification methods for all these systems. Is it possible to ensure privacy for the persons relying on the systems?

5.5.28 What are the perceptions of the public regarding the benefits on the one hand and risks on the other to be derived from integrated data sharing in government? Do people recognise the available safeguards and trust them? In sharing data, who is responsible for the accuracy and maintenance of the data? Comments are invited.

5.6 Data profiling

78 Arrehed H & Chaudry D "The Role of Smart Card Technology in Identity and Privacy" Presentation at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September 2002.

5.6.1 It has already been established that the mere collecting and storing of data 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.

5.6.2 The fact that a subject purchases large quantities of halaal meat at times which relate to Muslim feast days may be unexeptionable. If that information is passed on to a security agency which has 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, it may draw inverse inferences which are entirely incorrect.[79]

5.6.3 In the advertising world, the practice exists of tracking Internet users and compile dossiers on them in order to target banner advertisements. A marketing profile is a record of an individual's characteristics created by acquiring personal information from multiple sources and then using it to target products and services.[80] Marketing profiles are created and used by the private sector to maintain old customers and to target new ones by identifying those persons warranting solicitation.[81]

5.6.4 There is no objection to the compiling of statistical data and profiles from personal information, provided that its is not possible to trace the personal information of any identifiable individual from such profiling. Profiling is a valuable marketing tool and should be allowed as long as it is not abused by making individualised personal information available.

5.6.5 One of the largest advertisers in the USA, DoubleClick, however, set off widespread public outrage when it began attaching personal information from a marketing firm it purchased to the estimated 100 million previously anonymous profiles it had collected.[82] The company backed down

---

79 Tilley at 3.

80 NTIA Privacy Report Appendix A: Marketing Profiles available at http://www.ntia.doc.gov/ntiahome/privwhitepaper.html (hereafter referred to as "NTIA Report") at 31.

81 At 32.

82 See EPIC DoubleClick Pages <http://www.epic.org/privacy/doubletrouble/>.

due to public opposition, a dramatic fall in its stock price and investigations from the FTC and several state attorneys-general.

5.6.6 In July 2000 the Federal Trade Commission in the USA reached an agreement with the Network Advertisers Initiative, a group consisting of the largest online advertisers including DoubleClick, which will allow for online profiling and any future merger of such databases to occur with only the opt-out consent. [83] In January 2001 the FTC dropped its investigation of DoubleClick. However, a number of private lawsuits were filed against DoubleClick. In January 2001 DoubleClick closed its online profiling division, and in May 2002 privacy class actions suits against the company were settled that resulted in little or no benefit to Internet users. [84]

5.6.7 Profiles can be construed as assets. When ICE and P3P become a part of the web's infrastructure, netizens might start to expect something back for the use of their data. Even now some websites offer personalised content to members as a benefit for providing a user profile. Incentives include free software upgrades, customised content, preferred pricing of merchandise, or even copies of the demographics report themselves. An end user may be asked if she/he was interested in an incentive such as free shipping, or a deep discount on her purchase in exchange for the privilege of selling her name and profile information to another site. With such permission obtained ICE would facilitate all the back-end details of selling and renting the user profiles to other companies for database marketing.

5.6.8 Without question, public records, internal records, and external records are being accessed and matched into marketing profiles. Profiles have furthermore shown much ingenuity. For example, one way for a merchandiser to acquire more telling internal records is to issue a merchandiser credit card that is co-branded with a national credit card chain such as Mastercard or Visa. As provider of the credit card, the merchandiser has complete access to the credit card holder's transaction history, including the individual's shopping history at competing stores. By issuing such cards merchandisers get a tantalising glimpse at what its shoppers buy from rivals.

---

83 For a detailed history and critical analysis of this agreement, see Electronic Privacy Information Center (EPIC) and Junkbusters, "Network Advertising Initiative: Principles not Privacy," July 2000 at <http://www.epic.org/privacy/internet/NAI_analysis.html>.

84 Privacy advocates debate merits of DoubleClick settlement, Computerworld, May 22, 2002, at <http://www.computerworld.com/printthis/2002/0,4814,71382,00.html>.

This information is then used to market the card holder for the merchandiser's own products.[85]

5.6.9 Intel announced in May 2000 that it was dropping the incorporation of unique identifiers in its next-generation computer processors following a consumer boycott. [86] Several industry spokespeople, including Intel's Chairman Andrew Grove, have been supportive of federal Internet privacy legislation in order to stave off the states' recent efforts to enact such protections on their own. [87]

5.6.10 Do readers see data profiling as a natural element of marketing practice or is it an unacceptable infringement of the individual's privacy?. What should the consent requirements be?

5.7 Health

5.7.1 It is well known that nothing affects man as closely as his own health. And as much as we depend on support from others and new techniques, we want to determine for ourselves who has knowledge of what, and in what circumstances, about our health problems. Technical progress can therefore not only be a source of hope, but also of concern. [88]

5.7.2 It is therefore important, when using data relative to health, to give high priority to the right of the people concerned to self-determination in this essential and private domain.[89]

5.7.3 A person may indeed be harmed by the use of his or her health information outside the core health care arena. The following examples have been noted:[90]

– an employee was fired from a job days after being diagnosed with a genetic disorder

---

85 NTIA Report at 37.

86 See <http://www.bigbrotherinside.org>.

87 "Gates, Grove Differ on Net Privacy Laws," ***Industry Standard***, June 6, 2000.

88 Jacob J "Health at the Heart of Files" Presentation at the 23rd International Conference of Data Protection Commissioners, Paris, 24-26 September 2001 (hereafter referred to as "Jacob").

89 Jacob at 2.

90 Goldman at 2.

that required expensive treatment. The employer, who is self-insured, fired her to avoid the projected expenses.

- a woman's photograph and medical records was posted on the Internet by anti-abortion activists without her permission after receiving treatment at a hospital for complications from an abortion.
- Several thousand patient records inadvertently lingered on public Internet sites for two months due to a mistake made at a Medical Centre.
- An employee was automatically enrolled in a "depression program" by her employer after her prescription drugs management company reported that she was using anti-depressants.
- A drug company inadvertently revealed 600 patient e-mail addresses of persons using Prozac when an e-mail was sent to all the participants instead of to individual users.

5.7.4 Genetic engineering without bioethics would furthermore risk breaking various protective taboos. Thus, decoding the genome[91] in order to evaluate the human being and his worth to society would risk flouting every man's right to his intrinsic value and to the recognition of his dignity, which cannot be calculated from hereditary biological factors. It is therefore the fear that the usefulness of a human being may be evaluated based on recordings of the state of his health and that this might determine, for example, whether he gets or keeps a job, his creditworthiness, even possibly his life and death when measured against the costs needed for the necessary treatment.[92]

5.7.5 The situation has therefore developed where billions of dollars have been spent mapping the human genome and yet people are afraid to get a genetic test. The Internet can zip medical information and services from doctor's offices into your home, and yet people are afraid to go online. The fear and reticence that cause people to withdraw from full participation in their own care should be the common cause around which to unite.[93]

---

91 It was announced on CNN on 12 April 2003 that scientists working together in six countries have finalised their work in decoding the genome.

92 Jacob at 1.

93 Goldman at 7.

5.7.6 In South Africa there is, at present, little consistency in approaches to patient confidentiality and no national standards or policies on patient confidentiality, apart from specific rules and the general constitutional provisions that are not aimed at the specifics of doctor-patient-medical relationship.

5.7.7 Certain scenarios furthermore exist where the patient's right to self determination cannot be fully applied. That is the case with the archives of the general practitioner, who notes in writing his conclusions, his decisions and provisions, not only in the interest of the patient, but also in his own interest. The patient has the right to be informed of what has been noted in writing and the practitioner can only disclose the data to a third party if he follows a rule of law or if he has the consent of the patient.[94]

5.7.8 One may have to take notice of conflicting rights of others in this regard. Insurance companies, or other persons having to pay the costs, may demand certain information necessary for controlling their expenses. Another conflict exists between the patient's right to privacy and the important interests of others in the fight against contagious diseases.[95]

5.7.9 The National Health Bill of November 2001 provides that every patient is entitled to confidentiality of all health information, including health status, treatment or stay in a private or public establishment. This information is only to be disclosed if the user consents in writing or if a law or a court order authorises the disclosure. Mechanisms for the protection of health records held by any private or public health establishment are found in section 19 of the Draft Bill. [96]

---

94 Jacob at 2.

95 Jacob at 3.

96 It lists some nine types of conduct that would constitute an offence. Included are:

… (g) without authority, connects the personal identification elements of a ***use***r's record with any element of that record that concerns the ***use***r's condition, treatment or history;
(h) gains or attempts to gain, unauthorised access to a record or record-keeping system, by any means, including intercepting information being transmitted from one person, or one part of a record-keeping system, to another;
(i) without authority, connects any part of a computer or other electronic system on which records are kept to -
(i) any other computer or other electronic system;
(ii) any terminal or other installation connected to or forming part of any other computer or other electronic system; or
(iii) attempts or actually does modify or impair the operation of -
(aa) any part of the operating system of a computer or other electronic system on which a ***user's*** records are kept; or
(bb) any part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a ***user's*** records are kept.

5.7.10 This means that any person other than the doctor or facility who wants that information has to get the patient's consent in writing or do so in accordance with a law or court order.

5.7.11 From this it is clear that decoding of systems of de-identification is prohibited, as is the connecting of systems "without authority". It can be assumed that in view of the provisions of section 14, that authority must include consent or authorisation by law or court order. Administrative staff may have access to records for "any legitimate purpose within the ordinary course of their duties" (section 17), e.g. for submitting accounts to medical schemes.[97]

5.7.12 International sources on this issue include the following:

a) The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data binds European signatories. The regulation of data and privacy protection is supplemented by a number of Recommendations issued by the Committee of Ministers, most notably the Recommendation on the Protection of Medical Data (1997).[98]

b) The EU Directive sets out the circumstances under which personal data may be processed[99] as well as the exceptions to the processing of the data. Subsection 3 indicates that where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional *subject under national law or rules* established by national competent bodies subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy..

---

97 Klinck at 5.

98 Recommendation No R (97) 5 on the protection of medical data defines "personal data", "genetic data" and "medical data". Data may only be collected by health care professionals, or those working on behalf of the professionals (who should be subject to the same rules of confidentiality). Non-professionals controlling files are subject to rules of confidentiality comparable to those binding the professional. The Recommendation also deals with genetic data. It also provides for the withdrawal of consent at any stage by a person. Consent has to be free, express and informed. Many of the aspects already alluded to above in connection with control over the data, the right to know who has what on one and what its used for, etc. are addressed as well.

99 See discussion on EU Directive in Ch 6 below.

c) The World Medical Association (WMA)[100] passed a statement on ethical considerations regarding Health Databases, which sets the tone for medical associations world-wide.

5.7.13 During 2000, Commonwealth and State governments in Australia announced plans to move towards unique patient identifiers in the health sector, likely to be centered around a health smart card.[101] The Commonwealth's proposal, HealthConnect, is intended as a voluntary national health information network under which health-related information about an individual would be collected in a standard, electronic format at the point of care.[102] [103] In July 2001 the Department of Health announced that all negotiations on the implementation of this system and the introduction of the enabling legislation had been postponed due to "technical difficulties." [104] In the interim the Department is consulting with the Privacy Commissioner in order to ensure standards for patient privacy.[105]

5.7.14 In December 2001 the National Health and Medical Research Council (NHMRC) issued guidelines (under section 95A of the Privacy Act 1988) on privacy in medical research. Genetic privacy is currently under joint review by the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council. The group was scheduled to issue its final report by June 2002 but has recently extended the deadline by nine months until March 2003.

---

100 The World Medical Association ***Declaration on Ethical Considerations Regarding Health Databases*** adopted by the WMA General Assembly, Washington 2002 (hereafter referred to as "WMA Declaration"). See Ch 4 above.

101 Health services are primarily delivered by the public sector in Australia, with only around a third of the population having private health insurance. The responsibility for delivery of health services is shared between the Commonwealth Government, which is responsible for much of the funding of the health system, and the States, which operate hospitals and community health services.

102 For details see <http://www.health.gov.au/healthonline/connect.htm>.

103 As a first phase of this system the Department of Health and Aged Care drafted the Better Medication Management System Bill that would establish individual electronic medication records in order to improve access to information about drugs for doctors and patients. The system was widely criticized by consumers and doctors groups concerned about patient confidentiality and professional liability. "Medicos Oppose Data Bill," Karen Dearne, ***Australian IT*** July 24, 2001.

104 'Medical E-Files 'Delayed For Poll' by John Kerin, ***Australian IT***, July 30 2001.

105 "Your Health On The Line" ***Australian Financial Review*** May 25 2002.

5.7.15 The British Medical Association has struggled to obtain political will for the formulation of proper *medical* data-protection/confidentiality legislation so as to settle the variety of issues in this regard. It is the BMA's view that anonymous data may be used freely. Administrative and clinical information should be separate, and assurances as to real anonymity have to be provided. Dates of birth, postal codes etc., especially in combination, can identify a person. In the UK case of ***Source Informatics Ltd***[106] it was stated that the anonymisation of information does not remove the duty of confidentiality. For research, medical advancement and proper administration of the NHS, consent may be construed as implied where doctors and the Health Service use anonymised information for these purposes.

5.7.16 The American Medical Association[107] keeps to the US Constitution and ethical duties so as to provide guidance to doctors in patient confidentiality. According to the AMA a breach of confidentiality is a disclosure to a third party, without patient consent or court order, of private information that the physician has learned within the patient-physician relationship. Disclosure can be oral or written, by telephone or fax, or electronically, for example, via e-mail or health information networks. The medium is irrelevant, although special security requirements may apply to the electronic transfer of information. The general rule regarding release of a patient's medical record is that information contained in a patient's medical record may be released to third parties only if the patient has consented to such disclosure.

5.7.17 The Canadian Medical Association affirms that in terms of the CMA Code of Ethics (1996), medical records are confidential documents. Although the records are the property of the physician or health care institution that compiled them, patients have a right to examine their records and to obtain a copy of the information contained in them. Physicians should provide an explanation of the medical record to the patient when requested to do so. Unless the law requires otherwise, or if the maintenance of confidentiality would result in a significant risk of substantial harm to others or to the patient if the patient is incompetent, patient authorisation is necessary for the disclosure of information contained in medical records to third parties.

---

106 (1999) LTL 2/6/99, quoted in ***Confidentiality and Disclosure of Health Information*** 1999 at http://www.bma.org.uk/public.

107 http://www.ama-assn.org/ama/pub/category/4610.html.

5.7.18 The Canadian Medical Association (CMA) has adopted a Health Information Privacy Code[108] to protect the privacy of its patients, the confidentiality and security of its health information and the trust and integrity of the therapeutic relationship. The Code is based on the Canadian Standards Association's Model Code for the Protection of Personal Information ("CSA Code") as a sectoral code of the CSA Code. The Code provides instruction and guidance respecting health information collection, use, disclosure and access.

5.7.19 It is clear that people must maintain some degree of control over their own lives, and in this case, over the information they share about themselves in order to get health care and benefits. No right is absolute, and privacy is no exception. But the power of health privacy is that it benefits individuals, improves access to care and quality of care, enhances the reliability of data downstream and is a boost for health care organisations.[109]

5.7.20 The Commission invites comment on all of the above issues, and more specifically with regard to the following areas:

* **genetic engineering;**
* **special considerations about the needs of minors;**
* **information provided to spouses, dependants, and other next of kin;**
* **public health reporting; and**
* **fraud and abuse investigations.**

5.8 Security

5.8.1 The concepts of privacy and security are so closely related that they are often a source of confusion for many. The two are not separate, and for purposes of protecting individual information cannot be separated. Without strong security, personal information cannot be properly secured from misuse or abuse. There is also a close relationship between security technologies and privacy

108 http://www.cma.ca/cma/common/displayPage.do?pageId=/staticContent/HTML/N0/l2/where_we_stand/1998/09-16.htm.

109 Goldman at 7.

technologies. At the same time, however, they are not interchangeable technological concepts.[110]

5.8.2 Security solutions, products and services typically seek to prevent the introduction of viruses, eliminate network vulnerabilities, limit access by unauthorised users and authenticate data, messages or users. [111]

5.8.3 However, beyond the requirement that personal data be protected by reasonable or adequate security safeguards, privacy protection includes limits of a "legal" nature to the collection, handling, storage or transmission or personally identifiable or aggregates data collected from individual users.[112] In this section we will, however, only be dealing with aspects of security.

5.8.4 Computers 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.[113]

5.8.5 The number and nature of infrastructure access devices have 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.[114]

5.8.6 However, the speed and accessibility that create the enormous benefits of the computer age may, if not properly controlled, allow individuals and organisations to eavesdrop inexpensively on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.[115]

---

110 OECD Hall Report at 17.

111 Ibid.

112 Ibid.

113 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.

114 OECD Security Guidelines at 7.

115 OECD Security Guidelines at 7.

5.8.7 Dramatic increases in computer interconnectivity, especially in the use of the Internet, have furthermore increased the risks to computer systems.[116] The potential danger if computers performing these functions are interfered with is very serious.[117]

5.8.8 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.[118]

5.8.9 In addition, the disgruntled organisation insider is a significant threat. 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.[119]

5.8.10 As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. [120]

---

116 United States General Accounting Office (GAO) "Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk" Statement 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; 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 Discussion Paper") at 3.

117 SALC Discussion Paper at 3.

118 GAO testimony at 3.

119 GAO testimony at 4.

120 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")at 10.

5.8.11 There is a multitude of methods by means of which information can be obtained from a computer or its functioning be interfered with. Such methods can include the duplication of information on a computer, the removal of information on a computer, the alteration of information stored on a computer and the alteration of the functioning of a computer.[121]

5.8.12 Security specialists have found it useful to place potential security violations in three categories:[122]

a) Unauthorised information release: An unathorised 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.

c) Unauthorised denial of use: An intruder can prevent an authorised user from referring to or modifying information. This may cause a system to crash.

5.8.13 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.[123]

5.8.14 Examples of resources that may be at risk are payments and collections that could be lost or stolen and sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime. Targets also include telephone customer records

---

121 SALC 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.

122 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.

123 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 consumer credit report information. Critical operations, such as those supporting national defence and emergency services, could be disrupted.[124]

5.8.15 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. [125]

5.8.16 Problems regarding the security of data have been acknowledged and addressed worldwide since the early eighties. Both the EU Directive and the OECD Guidelines make provision for security issues.[126] Article 17 of the EU Directive[127] stipulates that member states shall provide that the controller has to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

5.8.17 It provides further that such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

5.8.18 Principle 5 of the OECD Guidelines provides that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

5.8.19 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

---

124 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.

125 CCIPS at 10.

126 See discussion on Principle 9 at 196 below.

127 As set out in Section VIII - Confidentiality and Security of Processing of Directive 95/46/EC.

OECD governments have now drawn up new guidelines entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"[128] to deal specifically with cyber terrorism, computer viruses, hacking and other threats.[129] The Security Guidelines should be read in conjunction with the abovementioned Guidelines.

5.8.20 The Guidelines suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".[130]

5.8.21 They urge all users of information technology, including government, business and individual users, to adhere to and implement nine basic principles covering such areas as security awareness and responsibility and respect for ethical and democratic values.[131]

5.8.22 The nine principles are complementary and should be read as a whole. [132]The Principles are as follows:

(a) Awareness:[133] Participants should be aware of the need for security of information

---

128 See fn 113 above.

129 Organisation for Economic Co-operation and Devlopment (OECD) "OECD Governments Launch Drive to Improve Security of Onlline Networks" News release dated August 7, 2002 (hereafter referred to as "OECD news release") at 1.

130 OECD Security Guidelines at 7.

131 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.

132 OECD Security Guidelines at 9.

133 OECD Security Guidelines at 10.

systems and networks and what they can do to enhance security.[134]

(b) Responsibility: [135] All participants are responsible for the security of information systems and networks. [136]

(c) Response:[137] Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents. [138]

(d) Ethics: [139] Participants should respect the legitimate interests of others. [140]

(e) Democracy:[141] The security of information systems and networks should be compatible with essential values of a democratic society.[142]

(f) Risk assessment:[143] Participants should conduct risk assessments.[144]

---

134 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.

135 OECD Security Guidelines at 10.

136 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.

137 OECD Security Guidelines at 10.

138 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.

139 OECD Security Guidelines at 11.

140 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.

141 OECD Security Guidelines at 11.

142 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.

143 OECD Security Guidelines at 11.

144 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

(g) Security design and implementation:[145] Participants should incorporate security as an essential element of information systems and networks.[146]

(h) Security management: [147] Participants should adopt a comprehensive approach to security management. [148]

(i) Reassessment:[149] Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. [150]

5.8.23 The OECD recommends that member countries establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the Guidelines by adopting and promoting a culture of security as set out in the Guidelines.[151]

5.8.24 In practice six major areas of security design and management have been identified.[152] These six areas of general controls are:

a) security program management, which provides the framework for ensuring that risks

---

assessment should include consideration of the potential harm that may originate from others or be caused to others.

145 OECD Security Guidelines at 12.

146 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.

147 OECD Security Guidelines at 12.

148 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.

149 OECD Security Guidelines at 12.

150 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.

151 OECD Security Guidelines at 15.

152 GAO testimony at 10.

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 data;

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.

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

5.8.26 Some examples of security technologies[153] 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 interception to a very high degree.

5.8.27 Proxies 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.[154] Many technologies can be used in many different ways. It is therefore crucial to recognise the context in which any given technology is used. [155]

---

153 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.

154 OECD Hall Report at 16 and 23.

155 OECD Hall Report Introduction at 4.

5.8.28 There are clear advantages to incorporating the principles set out in the OECD Security Guidelines in any future policy guidelines that may be drawn up in South Africa in this regard. An important question to be considered is , however, whether specific provision should be made in the envisaged privacy legislation for the implementation of these principles.

5.8.29 In South Africa the legislator has already created certain offences in sections 85 to 89[156] of the Electronic Communications and Transactions Act [157] to deal with unauthorised access to, interception of or interference with data and with computer-related extortion, fraud and forgery.[158] Chapter V of the Act furthermore provides for the registration of cryptography providers.[159] 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.

5.8.30 Comments are invited as to 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. Comment is also welcomed regarding the practical issues surrounding identity theft, a practice which seems to have become a major problem for financial institutions and their customers.

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

157 Act 25 of 2002.

158 See also para 6.2.115 below for the provisions in the Open Democracy Bill.

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

CHAPTER 6: PRINCIPLES OF DATA PROTECTION

6.1 Origins of data protection principles

a) Introduction

6.1.1 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] The widespread adoption of the Internet is also making people far more conscious of, and concerned about, privacy of information.

6.1.2 In response to these developments, countries have started to develop data protection laws in 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

---

1 This use of the computer has far-reaching consequences. McQuoid-Mason 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*** 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 at 8 on so-called "financial privacy".

3 Tilley at 3.

4 Piller at 2.

5 Victorian Law Reform Commission at 5.

(1977), and France (1978).[6]

6.1.3 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 Data[7] (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]

6.1.4 These instruments set out specific rules covering the handling of electronic data. The rules describe personal information as data that is afforded protection at every step from collection to storage and dissemination.

6.1.5 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.

6.1.6 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)

6.1.7 The Convention is so far the sole international treaty to deal specifically with data protection.

---

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 available at http://www.coe.fr/eng/legaltxt/108e.htm..

8 OECD Guidelines.

9 Bennett at 10.

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]

6.1.8 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]

6.1.9 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 at 32.

13 Bygrave 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]

6.1.10 An additional Protocol to the Convention was adopted on 23 May 2001[21] 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)

6.1.11 In late 1980, the Organisation for Economic Cooperation and Development (OECD) issued

---

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.

a set of Guidelines concerning the privacy of personal records. Although broad, the OECD guidelines set up important standards for future governmental privacy rules. These guidelines underpin most current international agreements, national laws, and self-regulatory policies. Although the guidelines were voluntary, roughly half of OECD member-nations had already passed or proposed privacy-protecting legislation by 1980. By 1983, 182 American companies claimed to have adopted the guidelines, although very few ever implemented practices that directly matched the standards.

6.1.12 The OECD Guidelines have been highly influential on the enactment and content of data 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 data 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]

6.1.13 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 data privacy principles.[23]

6.1.14 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

22 Bygrave at 33 and references therein.

23 Victorian Law Reform Commission at 23.

rights.[24]

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

- Collection Limitation Principle [25]
- Data Quality Principle[26]
- Purpose Specification Principle [27]
- Use Limitation Principle[28]
- Security Safeguards Principle [29]
- Openness Principle[30]
- Individual Participation Principle[31]

---

24 As referred to in Strathclyde "Notes for Information Security Theme Two: Data protection" at 4.

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 the 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.

– Accountability Principle[32]

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]

6.1.16 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]

6.1.17 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]

6.1.18 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.

6.1.19 The directive sets a baseline common level of data privacy protection that not only reinforces

---

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.

33 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.

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 at 5.

36 The UK objected to the measure as extending the scope and cost of legislation and ultimately abstained form the final vote in the Council of Ministers. Germany was concerned that the protection afforded its citizens by its national Act, may be weakened. The Unites States thought the transborder data flows were being driven by considerations of economic protectionism and constituting a thinly veiled attack on the US data processing industry.

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]

6.1.20 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]

6.1.21 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.

6.1.22 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 the future, the commercial and government use of such information will generally require "explicit and unambiguous" consent of the data subject.

6.1.23 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

---

37 Art 3 of the EU Directive. See also para 1.3.4 in Ch1.

38 As referred to in Strathclyde 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.

39 Recital 11 of the EU Directive.

40 Fisher excerpt. See especially paras (a) -(e) of Art 6 of the EU Directive.

under which each individual is given the option of whether to provide the information requested or not, through a type of notice and opt-out procedure.

- Individuals must also be provided with an opportunity to learn the identity of organisations intending to process data about them and the main purpose for which that information is being collected or will be used.
- The Data Protection Directive also requires all data processing to have a proper legal basis and identifies the following legal grounds for the collection and use of data:
  - consent;
  - contract;
  - legal obligations;
  - vital interests of the data subject; and
  - the balance between the legitimate interest of the people collecting or using the data and the people to whom the data relates.
- 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 “adequate level” of data protection.[41]

6.1.24 This requirement has resulted in growing pressure outside Europe for the passage of data

41 Article 25 of the EU Directive.

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]

6.1.25 In 1997 the European Union supplemented the 1995 directive by introducing the Telecommunications Privacy Directive.[43] This directive established specific protections covering telephone, digital television, mobile networks and other telecommunications systems.[44]

6.1.26 On June 25, 2002 the European Union Council adopted the new Electronic Communications Privacy Directive as voted in the Parliament. [45] 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

---

42 See the discussion on crossborder transfers in Ch5.

43 EU Directive.

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

45 2439th Council meeting, Luxembourg, June 25, 2002. EPIC Report 2002 at 11 explains as follows: 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.

In July 2001, the European Parliament’s Civil Liberties Committee approved the draft directive without data retention stating: The Civil Liberties Committee (“LIBE Committee”) expressed itself in favour of a strict regulation of law enforcement authorities' access to personal data of citizens, such as communication traffic and location data. This decision is fundamental because in this way the EP blocks European Union States' efforts underway in the Council to put their citizens under generalised and pervasive surveillance, following the Echelon model.

Following the events of September 11, however, the political climate changed and the Parliament came under increasing pressure from member states to adopt the Council’s proposal for data retention. The United Kingdom and the Netherlands, in particular, questioned whether the proposed privacy rules still struck “the right balance between privacy and the needs of the law enforcement agencies in the light of the battle against terrorism.”

The Parliament stood firm and up to a few weeks before the final vote on May 30, 2002, the majority of MEPs opposed any form of data retention. Finally, after much pressure by the European Council and European Union governments, and well organized lobbying by two Spanish MEPs, the two main political parties (PPE and PSE, the center-left and center-right parties) reached a deal to vote in favor of the Council’s position.

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 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.[46]

6.1.27 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 data 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.

6.1.28 Another possible way to protect the privacy of information transferred to countries that do not provide "adequate protection" is to rely on a private contract containing standard data 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 data transferred from the European Union, the contract would have to meet the standard "adequacy" test in order to satisfy the Data Protection Directive.[47]

e) United Nations Guidelines

---

46 EPIC Report 2002 at (iii).

47 EPIC 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.

6.1.29 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 data 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 data regimes than the other instruments.[49]

f) Commonwealth Guidelines

6.1.30 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.

6 .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.

6.1.32 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

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

49 Bygrave at 33.

administered by small and developing countries without the need to create significant new structures.

6.1.33 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.

6.1.34 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.

6.1.35 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.

6.1.36 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 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.

6.2 Discussion of Data Principles

a) Introduction

6.2.1 It is common for privacy or data protection acts worldwide to contain sets of principles. The information privacy principles lie at the heart of any Data Privacy Act. They have 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 data protection laws. The principles can, however, be found in all types of policy and legal instruments.[51]

6.2.2 Except to the extent that any data controller is able to claim an exemption from any of the principles (whether on a transitional or outright basis) the principles apply to all personal data processed by data controllers.

6.2.3 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). In our case the principles will also be compared with other modern sets of privacy principles developed in other jurisdictions in recent years.

6.2.4 One should remember that these codes are guidelines only which ought to be interpreted by countries to suite 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.

6.2.5 For example in the UK the data principles originally derived from the CoE Convention which in turn were given substance and amplificaton by recital 11 of the EU Directive. In New Zealand,

---

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 at 3.

on the other hand, the information privacy principles do not directly repeat the OECD principles but 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]

6.2.6 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 data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole.

b) Principles of Data Protection

6.2.7 What follows is a discussion of the various data principles (sometimes called "good information handling") with which data agencies are required to comply. 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 data 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, data protection authorities in the exercise of their discretionary powers. The principles may also help to shape the drafting of new data protection laws.[53]

6.2.8 The data protection principles that will be discussed are the following:

- Principle 1: Fair and lawful processing
- Principle 2: Openness
- Principle 3: Collection Limitation
- Principle 4: Use/Purpose Specification
- Principle 5: Disclosure Limitation

52 New Zealand Discussion Paper at 1.

53 Bygrave at 57.

- •• Principle 6: Individual participation
- •• Principle 7: Data Quality
- •• Principle 8: Finality
- •• Principle 9: Security Safeguards
- •• Principle 10: Accountability
- •• Principle 11: Sensitivity

(i) Principle 1: Fair and lawful processing

6.2.9 It is sometimes argued that the primary principle of data protection laws is that personal data shall be processed fairly and lawfully.[54] This principle is primary because it embraces and generates the other core principles of data 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 data[55] or not specifically mentioned at all.[56]

6.2.10 The notion of "lawfulness" is relatively self-explanatory. The bulk of data protection instruments comprehend legitimacy prima facie in terms of procedural norms hinging on a criterion of lawfulness (eg that the purposes for which personal data are processed should be compatible

---

54 See Bygrave at 58 and the references made there-in;

Art 5(a) of the CoE Convention states:
Personal data undergoing automatic processing shall be:
a). obtained and processed fairly and lawfully;...

Article 6 (1)(a) of the EU Directive stipulates that Member States shall provide that personal data must be processed fairly and lawfully.

Principle 1 in the UK's Data Protection Act of 1998 provides:
Personal data shall be processed fairly and lawfully and , in particular, shall not be processed unless-
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive data, at least one of the conditions in Schedule 3 is also met.
Schedule 2 is based on Art 7 of the EU Directive and follows the Directive fairly closely. The conditions deal with the consent to processing as well as other lawful reasons why the data controller needs to process data of the subject.
Schedule 3 derives from Art 8 of the EU Directive which allows the processing of sensitive data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs etc only in specific cases.

55 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.

56 Bygrave at 58 and the reference therein to the Norwegian PDA.

with the ordinary, lawful ambit of the particular data controller's activities).[57] The determination of what is fair may be a more difficult task.[58]

6.2.11 At a general level the notion of fairness[59] undoubtably means that, in striving to achieve their data-processing goals, data controllers 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.[60]

6.2.12 In determining whether processing is fair, regard is to be had to the method by which the data was obtained. [61] Fairness implies that a person is not unduly pressured into supplying data on him/herself to a data controller. From this, it arguably follows that fairness implies a certain protection from abuse by data controllers of their monopoly position. While very few data 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."[62]

6.2.13 Fairness further implies that the processing of data be transparent for the data subject.[63] Fairness militates against secretive collection and processing and also against deception of the data subject as to the nature of, and purposes for, the data processing. Another requirement that may flow from this argument is that data should be collected from the data subject, not from third parties. [64] This requirement is expressly laid down in some, but not the majority of data protection

---

57 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.

58 Strathclyde at 16.

59 See discussion in Ch 3 on 55 on criterion of reasonableness or boni mores.

60 Bygrave at 58.

61 Bainbridge D ***Data protection*** CLT Professional Publishing Welwyn Garden City 2000 (hereafter referred to as "Bainbridge") at 58.

62 Bygrave at 59. See discussion in Ch 5.

63 Bainbridge at 59.

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

instruments.[65]

6.2.14 Since fairness implies that data controllers must take some account of the reasonable expectations of data subjects, this has direct consequences for the purposes for which data may be processed.[66] It helps to ground rules embracing the purpose specification principle. It sets limits on the secondary purposes to which personal data may be put. When personal data obtained for one purpose is subsequently used for another purpose, which the data subject would not reasonably anticipate, the data controller may have to obtain the data subject's consent to the new use.[67] Where a person was deceived or misled as to the purposes of the processing the processing will be unfair. The subject should also be informed as to the non-obvious uses to which the controller intends to put the data.[68]

6.2.15 Even though a data user may be able to show that information was obtained and personal data 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 the fair processing principle. [69]

6.2.16 Where a data user 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.[70]

---

65 Bygrave at 59 and the references made therein.

66 The Commonwealth Bill for private users states:
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.

67 Bygrave at 59.

68 Bainbridge at 58. See Part II of the proposed Commonwealth Privacy Act dealing with the collection, use, disclosure and retention of personal information by public agencies.

69 Information Commissioner ***Chapter 3: The Data Protection Principles of the IC's Legal Guidance*** Version 1 Nov 2001 (hereafter referred to as "Information Commissioner") at 12.

70 Information Commissioner at 18.

6.2.17 Where personal data 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 unfair.

(ii) Principle 2: Openness

6.2.18 The principle of openness flows from the notion of fairness and transparency set out above. 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/she has to have knowledge of the fact that personal information about him/her is being kept by a specific body.[71]

6.2.19 It is clear that even the most comprehensive measures for protecting data are worthless if the individual does not have such knowledge. Without this knowledge he remains completely unaware that his privacy is threatened or even actually infringed. Therefore the data medium should have a legal duty to notify persons concerning whom data are collected of this fact (unless, of course, they are in some other way already aware of it).[72] Obviously allowance must be made for exceptions to this principle, for example where personal information is processed for the purposes of national security.[73]

6.2.20 The most important of these rules are those which require data controllers to orient data subjects directly about their data-processing operations. Secondly, are the category of rules requiring data controllers to provide basic details of their processing of personal data to data protection authorities, coupled with a requirement that the latter store this information in a publicly accessible register.[74]

---

71 Roos at 499.

72 ***Neethling's Law of Personality*** 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." There is usually an agreement between the credit bureau and the user of data that the latter will not inform an individual of the identity of the credit bureau (see further McQuoid-Mason at 198).

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

74 Bygrave at 63.

6.2.21 Principle 6 of the OECD Guidelines[75] stipulates that there should be a general policy of openness about developments, practices and policies with respect to personal data.[76] 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.

6.2.22 Articles 10-11 of the EU Directive[77] require 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. 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

---

75 Para 9 Part II Basic Principles of National Application of OECD Guidelines; Roos at 503.

76 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.

77 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.

(art 21(1)) and to ensure that there is a register of processing operations open to public inspection (art 21(2).

6.2.23 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".

6.2.24 This means that the following facts should be publicly known:[78]

a) the existence of record-keeping systems, registers and data banks that contain personal data;

b) nature of the data being processed;

c) a description of the main purpose and uses of the data; and

d) identity and usual residence of the data controller.

6.2.25 An example of the principle in national legislation is that of Principle 3 of the New Zealand Privacy Act. [79] Underlying the principle is the idea of openness: that collection of personal

---

78 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.

79 **PRINCIPLE 3**

Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of -

(a) The fact that the information is being collected; and
(b) The purpose for which the information is being collected; and
(c) The intended recipients of the information; and
(d) The name and address of -

(i) The agency that is collecting the information; and
(ii) The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law -

(i) The particular law by or under which the collection of the information is so authorised or required; and
(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and

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 there should generally be transparency about information collection policy and individual participation in that process.[80]

6.2.26 In South Africa PAIA partly complies with this principle as far as the public sector is concerned, with the requirements in sections 14 and 15 that an index of records must be kept.[81] A similar provision is found in section 51 which applies to private bodies. PAIA does not, however, specifically deal with the collection of data.

iii) Principle 3: Collection Limitation

6.2.27 This principle envisages that there should be limits to the collection of data. "Fishing expeditions" should not be allowed, and personal information should be collected for a clearly specified purpose only.[82] Data should be collected by lawful and fair means, and, where appropriate, with the knowledge and consent of the data subject.

Data collected for a specific purpose

6.2.28 The principle is prominent in all the main international data protection instruments as well as in national legislation.[83]

(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.

80 New Zealand Discussion Paper at 3.

81 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.

82 Roos at 499 and the references made therein.

83 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;

6.2.29 Article 6(1)(c) of the EU Directive stipulates that Member States shall provide that personal data must be:

> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; [84]

6.2.30 The minimality principle is also manifested in Arts 7 and 8 of the Directive [85] which deal with

---

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.

84 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.

85 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 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

this question extensively, by setting out circumstances which will be reasonable, and what is not reasonable processing. Of crucial importance for the extent to which data processing may occur, is the interpretation of the criterion "necessary" in paras (b)-(f) of Art 7 and paras (b), (c) and (e) of Art 8(2).

6.2.31 The necessity criterion should probably be construed as embracing two overlapping requirements :[86]

a) that the processing corresponds to a pressing (and legitimate) social, political or commercial need;

b) that the processing is proportionate to the aim involved.

The stringency of the above two requirements will undoubtedly vary from case to case depending, inter alia, on the sensitivity of the data involved and the context in which the processing occurs.[87]

6.2.32 Principle 1 of the OECD Guidelines reads as follows:[88]

> Collection Limitation Principle
>
> 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.

6.2.33 The amount of personal data collected should be limited to what is necessary to achieve 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

86 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 folllws from the criterion "not excessive" in Art 6(1)(c) of the Directive.

87 Bygrave at 343.

88 CDT's Guide to Online Privacy/OECD available at http:/www.cdt.org/privacy/guide/basic/oecdguidelines. html.

purpose for which the data are gathered.[89] The principle is 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".[90]

Knowledge and consent of data subject

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

a) rules requiring data controllers to collect data directly from data subjects in certain circumstances;

b) rules prohibiting the processing of personal data without the consent of the data subject. [91]

Directly

6.2.35 Rules requiring that data may only be collected from the subject directly, are found only in a minority of data protection instruments.[92] However, such rules could and should be read into the more common and general requirement that personal data be processed fairly. In New Zealand the principle is set out in Principle 2 of their Act.[93]

---

89 Sec 7(1)b) of the Commonwealth Privacy Bill states that the collection of the information must be necessary for, or directly related to, that purpose.

90 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".

91 See discussion in Ch 5.

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

Consent

6.2.36 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.

6.2.37 Even where a positive action is taken to give authorisation there sometimes remains a problem of specificity. Some agencies ask customers to sign authorisations, unlimited in time and subject matter, essentially purporting to authorise the agency to collect anything from anyone at any time and to use and disclose the information for any purpose to any person. Some might see this as attempting to contract out of some of the limitations imposed by the information privacy principles.

6.2.38 Some privacy laws have grappled with these issues. For example, the EU Directive provides that the personal data may only be processed if the individual concerned "has unambiguously given

---

(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.

his consent".[94]

6.2.39 Some instruments make no mention of a consent requirement[95] while others often stipulate consent in fairly narrow contexts, eg as a precondition for disclosure of data to third parties.[96]

6.2.40 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 EC Directive. [97] The alternative prerequisites are often formulated broadly, thereby reducing significantly the extent to which data controllers are hostage to the consent requirement in practice.[98] With regard to Art 7 of the EC Directive, for example, most instances of processing will be able to be justified under the criteria in paras (b) - (f) of the provision.[99]

6.2.41 From these sections we can see that the primary concern of the directive is to ensure that the data subject agrees to whatever use the data 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 data which is

---

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 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 at 66.

processed. The consent may also be implicit, such as where a contract entered into requires the automatic processing of the data subject's data. [100]

6.2.42 A specific right to object is also laid down in some data protection laws. The EC 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, however, the ILO Code of Practice on Protection of Workers' Personal Data). Nor have they existed in the bulk of national laws though this situation no longer pertains in Europe as a result of the adoption of the Directive.[101]

6.2.43 There are, however, also examples of exemptions to the request of consent:

a) The data controller may be required by law to process the data. A South African example would be where banks are required to supply the department of Trade and Industry with statistics in relation to their lending patterns in order to prevent red-lining.

b) The processing may be necessary to protect the vital interests of the data subject. Information about notifiable diseases is one such example.

c) There is also the legitimate interest exemption, where the data processor has some legitimate interest in processing data; or third parties in receiving the data (eg customers of credit bureaux). Local authority processing the data of its electricity users in order to establish what the year-on-year increase in electricity use is going to be would be one such example.

---

100 See discussion on consent, and more specifically the difference between opt-in and opt-out options in Ch 5 above.

101 Bygrave at 66.

6.2.44 Sec 51 (1) of the Electronic Communications and Transactions Act[102] suggests a similar regime, whereby the consent of the data subject is needed, unless the data controller is required or permitted by law to process the data.

(iv) Principle 4: Purpose specification

6.2.45 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.

6.2.46 This principle is furthermore set out in Article 6(1)(b)and (c) of the EU Directive.[103] See also the basic regulatory premise - embodied in arts 7 and 8 of the EC Directive - which is that the processing of data is prohibited unless it is necessary for the achievement of specific goals.

Purpose specified at time of collection

6.2.47 Many data 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 data 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

---

102 **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.

103 Article 6(1)(b) and (c) 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.
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

and legal authority for collection of personal information.

6.2.48 If an obligation were to be imposed on agencies 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 agency? Explaining the purpose of collection is seen as of greatest importance, but should any other explanations be required, such as an indication as to whether collection is mandatory or voluntary?

6.2.49 One issue raised regarding the New Zealand principle is whether it effectively "limits ... the collection of personal data" since it may be open to agencies to proclaim their functions or activities on a very broad basis. It may be relatively easy for an agency to claim that it had broader purposes in mind than were fully understood by the individual from whom information was collected. The problem is how to be sure as to what an agency's function or activities were at the time of collection. [104]

6.2.50 This task is theoretically more straightforward in jurisdictions having a registration process. In those jurisdictions agencies are required to register a list of their functions or activities and the purposes for which they collect information. They are not permitted to use the information for an unregistered purpose. [105]

6.2.51 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.[106]

---

104 New Zealand Discussion Paper at 3.

105 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.

106 New Zealand Discussion Paper at 2.

6.2.52 For example, it might be possible for agencies to have on their own file a statement of their functions and activities and their purposes for collecting information. The suggestion is that this could be verified in some way, such as by having a dated copy open for inspection at the agency or published from time to time, for example in an agency's annual report.

6.2.53 Another approach might place an onus on the agency to prove these matters in the event of a complaint. Naturally an agency 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 agency would be obliged to make out a case where there are doubts as to the matter.

6.2.54 A third suggestion would be to oblige agencies to give notice to the regulatory agency in certain exceptional cases where a high degree of sensitivity exists in respect of the purpose of the information. [107]

Used only for specified purpose

6.2.55 Data should be used only for purposes specified at the time of collection. In New Zealand this principle is set out in Principle 10:Limits on use of personal information [108] and in the UK it is set out in Principles 2 and 3.[109]

6.2.56 Principle 10 gives effect to the OECD "purpose specification principle" and "use limitation principle". 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) lie at the heart

---

107 New Zealand Discussion Paper at 2.

108 New Zealand Discussion Paper at 7.

109 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 furtehr processed in any manner incompatible with that purpose or those purposes.
The third principle reads as follows:
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

of any data protection law.[110]

6.2.57 The Commonwealth Model Law for the Public sector makes provision for this principle in section 9.[111] The Commonwealth Model Law for the private sector also makes provision in sections 12, 14 and 15.[112]

---

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

111 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
  (ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned;
(e) the authority believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety; or
(f) use of the information for that other purpose is necessary -
  (i) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law;
  (ii) for the enforcement of a law imposing a pecuniary penalty;
  (iii) for the protection of public revenue;
  (iv) for the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
  (v) in the interests of national security.

112 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

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

6.2.59 The Commissioner had to form a view on the meaning of the term in a Principle 8 case where an agency 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. In this case the inaccurate information was simply deleted.

6.2.60 Data controllers should continually monitor compliance with this principle. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate, [113] and use thereof unfair?

(v) Principle 5: Disclosure Limitation

---

14. An organisation shall only use or disclose personal information under section 12 or section 13, where such use or disclosure would not amount to an unreasonable invasion of privacy of the individual concerned, taking into account the specific nature of the personal information and the specific purpose for which it is to be so used or disclosed.

Use of personal information outside *[name of country]*

15.(1) An organisation shall not use, outside *[name of country]* personal information collected in *[name of country]* unless the organisation -
(a) would be permitted under this Act to make the same use of that information in *[name of country];* and
(b) takes appropriate steps to preserve the confidentiality of the information and to protect the privacy of individuals.
(2) Nothing in this section affects the use of personal information that is required or authorised to be made under another Act.

113 Information Commissioner at 18.

6.2.61 The principles of collection limitation, purpose specification and use limitation are closely related and require that, once personal data 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. The notion of "relevance" underlies all these principles, since the data may be used or disclosed only for purposes specified at the time of collection.[114] Information gathered to determine income tax liability, for example, may not be used to evaluate eligibility for social assistance. If data are disclosed for other purposes, the consent of the individual must first be obtained.[115]

6.2.62 In practice, disclosure limitation therefore means that there should be limits to the use and disclosure of personal data: personal data should not be (used or) disclosed ...except with the consent of the data subject; or by the authority of law.[116]

6.2.63 This principle is not always expressed in data protection instruments in the manner formulated above. Moreover, neither the CoE Convention nor the EC Directive specifically addresses the issue of disclosure limitation but treat it as part of the broader issue of the conditions for processing data. 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.

6.2.64 The OECD Guidelines incorporate the principle of disclosure limitation within a broader principle termed the "Use Limitation Principle", [117] while the UN Guidelines specifically address the issue of disclosure under the principle of purpose specification.[118]

---

114 See purpose principle above.

115 Roos at 505.

116 Para 10 of the OECD Guidelines; 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.

117 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.

118 Bygrave at 67.

6.2.65 Disclosure limitation can, however, be singled out as a separate principle in its own right because it tends to play a distinct and significant role in shaping data protection laws. 6.2.62 Concomitantly, numerous national statutes expressly delineate it as a separate principle or set of rules.[119]

6.2.66 In New Zealand this principle is set out in Principle 11[120]: Limits on disclosure of personal information[121] In the Commonwealth Model Law for the Public sector makes provision for this principle in sections 11 and 12[122] and in the Model Law for the private sector in sections 13 and

---

119 Bygrave at 67.

120 **PRINCIPLE 11**

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds -

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
(b) That the source of the information is a publicly available publication; or
(c) That the disclosure is to the individual concerned; or
(d) That the disclosure is authorised by the individual concerned; or
(e) That non-compliance is necessary -

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
(ii) For the enforcement of a law imposing a pecuniary penalty; or
(iii) For the protection of the public revenue; or
(iv) For the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to:

(i) Public health or public safety; or
(ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or
(h) That the information -

(i) Is to be used in a form in which the individual concerned is not identified; or
(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

121 New Zealand Discussion Paper at 7.

122 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;

16.[123]

(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.

123 Limits on disclosure of personal information

13.(1) Where an organisation holds personal information, it shall not disclose the information to another person, body or agency (other than the individual concerned), unless –
(a) the individual concerned has expressly or impliedly consented to the disclosure;
(b) the disclosure of the information is required or authorised by or under law;
(c) the disclosure of the information is one of the purposes in connection with which the information was collected, or is directly connected to that purpose;
(d) the individual concerned is reasonably likely to have been aware or made aware under section 10(2)(c) that information of that kind is usually passed on to that person, body or agency;
(e) the information is to be disclosed -
(i) in a form in which the individual concerned is not identified; or
(ii) for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(f) the organisation believes on reasonable grounds that disclosure of the information is necessary –
(i) to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or other person, or to public health or safety;
(ii) for the prevention, detection, investigation, prosecution or punishment of any offence or breach of law; or
(iii) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.
(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.

(vi) Principle 6: Individual Participation (Data subject participation and control)

6.2.67 This principle provides that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or oganisations. The expectation is that individuals themselves can do much to mitigate any problems arising from the wrong people using the wrong data for the wrong purposes.[124]

6.2.68 Data 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 data processing activities generally. (See above: openness)

Access to data held

6.2.69 There are furthermore rules which grant persons the right to gain access to data kept on them by other persons and organisations. This right is known as "the right to access" Most, if not all, data protection instruments make provision for such a right. An influential formulation of the right is given in Art 12 of the EU Directive.[125]

6.2.70 Principle 7 of the OECD Guidelines[126] deals with individual participation.

---

124 Roos at 504 and references made therein.

125 Article 12 of the EU Directive deals with the right to access.
This provides persons with a right to access not just to data relating directly to them but also to information about the way in which the data are used, including the purpose of the processing, the recipients and sources of the data, and the "logic involved in any automated processing of data concerning the data subject.

126 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

6.2.71 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 data protection instruments. See Art 8 of the CoE Convention[127], paras 12-13 of the OECD Guideline and Principle 4 of the UN Guidelines. None of the latter, with the exception of the UN Guidelines, specifically mentions the right to be informed of the recipients of data.

6.2.72 The Directive is also broader than PAIA, in that one is entitled to more than the record, but also the information relating to the processing itself. This seems to indicate that access provisions for the individual can be broadened by data protection legislation, and access to more information than is possible under PAIA is required.[128]

6.2.73 On his request the data user must allow the individual concerned reasonable access to his data record. This power (or entitlement) of access[129] is necessary for effective and equitable control

---

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.

127 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 hin 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.

128 Individuals may have access to their personal information without paying the request fee (sec 22 and 54).

129 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).

of data,[130] for only thus will such 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. Of course, there may be exceptions to the right of access to data in particular circumstances.[131]

6.2.74 In addition to the right of access to his data record, an individual must also have the right to require from the data medium information as to the identity of all persons who have had access to his data 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 data user must be legally obliged, at the request of the individual, to give him information concerning whom and when the data were made available. Obviously provision must be made for exceptions in situations where it will not be justifiable to disclose such information.[132]

6.2.75 In New Zealand this principle is set out in Principle 6.[133] This right to access is subject to many exemptions, but this is not unusual when one compares it to legislation in other jurisdictions. It remains to be seen whether in practice these exemptions will result in the right of access being unduly curtailed.[134]

Objection to collection of data

---

130 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 at 166-170.

131 ***Neethling's Law of Personality*** at 304 and the references made therein.

132 Ibid.

133 **PRINCIPLE 6**

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled -

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and
(b) To have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.
(3) The application of this principle is subject to the provisions of Parts IV and V of this Act.

134 Roos at 504.

6.2.76 This principle also allows persons to object to others' processing of data on themselves and to demand that these data be rectified or erased insofar as the data are invalid, irrelevant, illegally held, etc. The ability to object is linked primarily to rules prohibiting various types of data processing without the consent of the data subjects. Such rules are especially prominent in the EC Directive, relative to older data protection instruments.[135]

Correction

6.2.77 With respect to rectification rights, most data protection instruments have provisions which give persons the right to demand that incorrect, misleading, irrelevant or obsolescent data relating to them be rectified or deleted by those in control of the data and or require that data controllers rectify or delete such data.[136]

6.2.78 Detailed provision was made for correction in clauses 51, 52 and 53 of the Open Democracy Bill, but only section 88 of PAIA survived. [137]

6.2.79 Section 88 of PAIA does not deal with correction sufficiently. Therefore it should be dealt with comprehensively in a data protection Act. 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 data. [138]

6.2.80 In this regard, the individual must have the power to procure a correction of misleading or

---

135 Bygrave at 65.

136 Bygrave at 66.

137 **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)

138 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.

incomplete data, or the deletion of data which are false or obsolete, or data obtained in an unlawful manner, or data 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.[139]

6.2.81 In New Zealand this principle is set out in Principle 7[140]

6.2.82 In terms of the Open Democracy Bill public bodies must inform all other governmental bodies or persons to whom inaccurate information has been supplied of a subsequent correction in such information; private bodies are, however, not under a similar obligation. A data privacy Act should be improved to ensure that it does not fall short on this point.[141]

6.2.83 In the Commonwealth Model Law for the public sector the principle manifested in section 15.[142]

---

139 These powers are recognised to a greater or lesser extent by all foreign legislation dealing with data protection (see Neethling ***Huldigingsbundel WA Joubert*** at 124 fn 128).

140 **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.

141 Roos at 504.

142 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),

6.2.84 From the foregoing it appears that a person must be given active control over his own data records if he is to be properly protected by law.

(vii) Principle 7: Data Quality

6.2.85 Principle 2 of the OECD Guidelines reads as follows:[143]

> 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.

6.2.86 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.

6.2.87 All data protection laws contain rules directly embodying the principle, but they vary considerably in their wording, scope and stringency. Data protection laws use a variety of terms to describe the stipulated data quality. Art 5(d) of the CoE Convention and Art 6(1)(d) of the EC Directive

---

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
(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.

143 CDT's Guide to Online Privacy/OECD available at http:/www.cdt.org/privacy/guide/basic/oecdguidelines.html.

refer to "accurate" and "up to date" data. See also Data Protection Principle 4 in Part 1 of Schedule 1 to the UK Act.[144] Other laws refer to "accuracy or correctness" or "completeness" (OECD Guidelines).[145]

6.2.88 Variation exists in terms of the stringency with which data protection instruments require checks on the validity of personal data. The standard set by the EC Directive, for example, is in terms of "every reasonable step must be taken" (art 6(1)(d)). By contrast the UN Guidelines emphasis a duty to carry out "regular checks" (principle 2).[146] In the UK it is not enough for a data controller 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 data at the time. They have to go further and take reasonable steps to ensure the accuracy of the data themselves and mark the data with any objections. The extent to which such steps are necessary will depend on the (negative) consequences of the inaccuracy for the data subject. [147]

6.2.89 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.[148]

6.2.90 In the Commonwealth Model Law for the public sector this principle is manifested in art 9.[149] In the Model Law for the private sector it can be found in art 17.[150]

---

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

145 Bygrave at 62.

146 Bygrave at 63.

147 Information Commissioner at 19.

148 Bygrave at 13.

149 **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.

150 **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;

6.2.91 In New Zealand the principle manifests itself in Principle 8 stipulating that the accuracy, etc, of personal information has to be checked before use. [151]

(viii) Principle 8: Finality

6.2.92 The finality principle refers to these provisions that require that personal data should be erased or anonymised once they are no longer required for the purpose for which they have been kept.

6.2.93 A privacy risk exists where such personal data is retained since:

- 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.

6.2.94 To comply with this principle data users will need to review their personal data regularly and to delete the information which is no longer required for their purposes.[152]

(b) take all reasonable steps to minimise the possibility that an organisation will use inaccurate personal information to make a decision about the individual.

(2) The organisation shall not update a record of personal information about an individual unless–
(a) doing so is necessary to fulfil the purpose for which the organisation collec ted the information;
(b) the individual consents to the updating; or
(c) this Act or another law permits the updating.

151 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.

152 Information Commissioner at 20.

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

6.2.96 See also art 5(e) of the CoE Convention.[153] The Commonwealth Model Law for private sector sets out the finality of records in art 20 (2) and (3).[154]

6.2.97 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 other provisions such as those setting out the principle of "purpose specification". Many, but not all,[155] national laws make specific provision for the erasure etc of personal information once the data are no longer required.[156]

6.2.98 For examples in national laws see Data Protection Principle 5 in the UK Data Protection Act[157]

---

153 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.

154 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).

155 US federal Privacy Act being an example.

156 Bygrave at 60.

157 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.

and Principle 9 of the New Zealand Privacy Act. [158] Similar provisions are found in several other jurisdictions. See for example, principle 2(2) of the Hong Kong Personal Data (Privacy) Ordinance[159] and the 1993 Quebec Act respecting the Protection of Personal Information in the Private Sector (section 12).[160]

6.2.99 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 Archives Act and Local Government Act require the retention of certain archives.[161]

6.2.100 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 data user and able to be used both lawfully and in accordance with the information privacy principles. It may also be possible, for example, for the data user to return documents to the individual concerned or disclose the information to another data user that does have a further lawful use for the information.

6.2.101 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);

---

158 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.

159 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.

160 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.

161 New Zealand Discussion Paper at 6.

- 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).

6.2.102 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.

6.2.103 In the Commonwealth Model Bill for the public sector this principle is set out in art 14.[162] In the Model Law for the private sector it is set out in art 20.[163]

(ix) Principle 9: Security safeguards

6.2.104 This means that personal data should be protected by reasonable security safeguards

---

162 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 theinformation, if necessary.
(2) Subject to subsection (1) and this Act, the Minister shall prescribe by regulation, guidelines for the retention and disposal of personal information held by a public authority.

163 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).

against the risks such as loss, unauthorised access, destruction, use, modification or disclosure.[164]

6.2.105 The principle manifests itself in Principle 5 of The OECD Guidelines.[165] A representative provision is also found in Art 7 of the CoE Convention.[166]

6.2.106 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".[167] Further, the measures taken pursuant to Art 17(1) and (3) shall be documented. (Art 17(4)).

6.2.107 In the Commonwealth Model Law for the public sector it is set out in art 13[168] and in the Model

---

164 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; See Bygrave at 67.

165 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.

166 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."

167 Bygrave at 68.

168 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.

Law for the private sector in art 18.[169]

6.2.108 An example of national legislation is Data Protection Principle 7 of the UK Data Protection Act[170] and Principle 5 of the New Zealand Act, which is closely modeled on a principle in the Australian Privacy Act.

6.2.109 In 1992 the OECD released its Guidelines for the Security of Information Systems ("the 1992 guidelines"). This built upon the security safeguards principle in the earlier OECD guidelines. The 1992 Guidelines developed eight principles on the security of information systems. These Guidelines were in turn followed up by the OECD Guidelines for the Security of Information Systems and Networks of 2002.[171]

6.2.110 The other OECD development in relation to security safeguards-related principles concerns work in relation to cryptography. In 1996 the OECD released Guidelines for Cryptography Policy which included within them a set of principles.

6.2.111 Cryptography has become central to the debate over security of personal information.

6.2.112 In the USA the principles in relation to the national information infrastructure took a novel

---

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

170 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.

171 See discussion in para 5.8 above especially fn 113.

approach to security. They emphasised the empowerment of individuals to utilise technology to safeguard their own data. One part of the "empowerment principle" stated:

> "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."

6.2.113 The empowerment principle also says 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.

6.2.114 In South Africa this principle was also reflected in the Open Democracy Bill, but only in regard to public bodies. Ideally, private bodies should also be under a specific obligation to nominate a person to be responsible for the security of personal information.[172]

(x) Principle 10: Accountability

6.2.115 Principle 8 of the OECD Guidelines reads as follows:[173]

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

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

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

6.2.117 Data Protection Principle of the UK Data Protection Act is an example of national legislation

---

172 Roos at 505.

173 CDT's Guide to Online Privacy/OECD available at http:/www.cdt.org/privacy/guide/basic/oecdguidelines.html.

in this regard.[174]

(xi) Principle 11: Sensitivity

6.2.118 The principle of sensitivity holds that the processing of certain types of data which are regarded as especially sensitive for data subjects should be subject to more stringent controls than other personal data. The principle primarily manifests in rules that place special limits on the processing of predefined categories of data.

6.2.119 The most influential list of these data categories is provided for in Art 8(1) of the EC Directive[175] : it embraces data on a person's "racial or ethnic origin", "political opinions", "religious or philosophical beliefs", "trade union membership", "health" and "sexual life". Further, Art 8(5) makes special provision for data on criminal records and the like.[176]

6.2.120 Similar lists are found in numerous other data protection instruments at both international and national level,[177] 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).

---

174 Sixth Principle
Personal data shall be processed in accordance with the rights of data subjects under this Act.
A person will contravene this principle if he fails to supply information pursuant to a subject access request or fail to comply with a notice given in terms of the Act.

175 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.

176 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.

177 The UK Data Protection Act, 1998 sets out conditions for the processing of sensitive data as part of its First Principle (data to be processed fairly and lawfully) and includes **explici**t consent to processing.

6.2.121 The lists in some national laws also include, or have previously included, data revealing a person to be in receipt of social welfare benefits. References to this sort of data, however, have to be dropped from the lists in the data protection laws of EU and EEA Member States as the list of data categories in Art 8(1) of the Directive is intended to be exhaustive.

6.2.122 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 data deserve special protection, and partly to a belief that the sensitivity of personal data is not an a priori given but dependent on the context in which the data are used. The previous or current absence of extra protection for designated categories of especially sensitive data in some national data protection laws would appear to be due to much the same considerations, along with uncertainty over what the possible extra protection should involve.[178]

6.2.123 Another provision of the Directive which, it is suggested, would improve the Bill should a similar provision be included, is that no individual may be subjected to a decision which significantly affects him/her (eg evaluation of performance at work, creditworthiness) where such decision is based solely on the automated processing of data. This provision therefore requires human intervention whenever important decisions are made about an individual. [179]

6.2.124 Views are sought as to whether all or some of the eleven principles set out above should be incorporated in a Data Privacy Act and if so, how this should be done. Since the inaccuracy of information collected and stored is a major problem for consumers, specific feedback is requested regarding Principle 7: data quality (see 191 above) and Principle 6: individual participation (see 185 above).

178 Bygrave 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.

179 Roos at 505.

CHAPTER 7: REGULATION /IMPLEMENTATION OF PRINCIPLES

7.1 Introduction

7.1.1. An essential aspect of any privacy protection regime is oversight. The effectiveness of data protection provisions in protecting an individual's personality rights will depend largely on how they are applied and interpreted in practice.[1]

7.1.2 It has been argued[2] that the rules for data protection come from three distinct perspectives, namely political, economic and technological:

a) In Europe, data 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 protections for consumers. Data protection is a question of economic power rather than political right.

c) Across these two policy models of data protection, technological rules and defaults define information practices for network interactions.

7.1.3 Four models for privacy protection can therefore be identified in this regard.[3] 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 privacy protection. 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. There is now a range of different tools within the toolbox all of which are necessary,

---

1 Roos 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 at the 23rd International Conference of Data Protection Commissioners, Paris, 24-26 September 2001(hereafter referred to as "Reidenberg") at 2 and the references made therein.

3 EPIC Report 2002 at 3.

and none sufficient. [4]The models are as follows:

a) Comprehensive laws

7.1.4 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 data protection laws have established special authorities (data protection authorities) to oversee specifically the implementation of these laws.[5] A variation of these laws, which is described as a co-regulatory model, was adopted in Canada, Australia and the Netherlands. Under this approach, industry develops rules for the protection of privacy that are enforced by the industry and overseen by the private oversight agency.[6]

b) Sectoral laws

7.1.5 Some countries, such as the United States, have avoided enacting general data 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 - 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 many countries, sectoral laws are used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.[7]

---

4 Bennett at 28.

5 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 at 70. 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 fn 277 and the references made therein.

6 EPIC Report 2002 at 4.

7 Ibid.

c) Selfregulation

7.1.6 Data protection can also be achieved - at least in theory - through various forms of selfregulation, 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 protections and lack enforcement. This is currently the policy promoted by the governments of the United States and Singapore.[8]

d) Technologies of privacy

7.1.7 With the recent development of commercially available technology-based systems, privacy protection has also moved into the hands of individual users. Users of the Internet and of 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.[9] Users should be aware that not all tools are effective of protecting privacy. Some are poorly designed while others may be designed to facilitate law enforcement access. [10]

7.2 Models of Privacy Protection

a) Comprehensive laws

7.2.1 The rules found in data protection laws usually belong to two main categories:[11]

a) rules concerned directly with regulating the processing of personal data (so-called

---

8 Ibid.

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

10 EPIC Report 2002 at 5.

11 Bygrave at 84.

Data Protection Principles)[12]; and

b) rules concerned primarily with monitoring and enforcing the first set of rules.

7.2.2 The first category of rules can in turn be sub-divided into two main sub-categories:

a) Rules regulating the manner and purposes of data processing . These rules ensure that the processing of data occurs with the participation of the data subject. Data processing should therefore be authorised, publicised and rectifiable.

b) Rules relating to the quality of personal data.

7.2.3 The second main category of rules can also be broken down into two main sub-categories:

a) Rules that facilitate monitoring and enforcement functions.

b) Rules directly concerned with monitoring and enforcement functions.

7.2.4 Data protection laws attempt to secure a balance between, on the one hand, the privacy, integrity and autonomy interests of data subjects and, on the other hand, the economic, social and political interests of data controllers in being able to process data. This does not, however, mean the existence of an equal weighting of the two sets of interests . For instance, the drafters of the OECD Guidelines and the EU Directive appear to have been primarily interested in ensuring minimal interference of transborder data flows, with data protection being seen essentially as a means of realising this interest. Other data protection laws have been enacted largely in order to create acceptance for data-processing activities of the data users.[13]

7.2.5 As seen above, most countries with an omnibus data protection or privacy act, have an official or agency that oversees enforcement of the act. 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.

7.2.6 The most detailed treatment of the competence and functions of data 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

---

12 See discussion of Data Protection Principles in Chapter 6.

13 Bygrave at 86.

provisions adopted by the Members States pursuant to the Directive. [14]

7.2.7 In contrast to the EU Directive, the OECD Guidelines have little to say about the need for, and competence of, national data protection authorities. Indeed, they do not require such authorities to be established. A similar situation has pertained up until recently with the CoE Convention. However, an additional Protocol to the Convention was adopted on 23 May 2001[15] by the CoE Committee of Ministers replicating in Art 1 the basic thrust of Art 28 of the Directive.[16].

7.2.8 The UN Guidelines specifically address the need to establish national data protection authorities that are "impartial", "independent" and "technically competent".[17]

7.2.9 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 to deal with allegations of damage caused by breach of the privacy law.[18]

7.2.10 It should also be noted that data protection authorities are not alone in monitoring, encouraging and enforcing the implementation of data 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 data protection instruments.[19]

7.2.11 On the international plane, notable examples of relevant bodies are the expert committees on data 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

---

14 Bygrave at 71.

15 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.

16 Bygrave at 73.

17 Bygrave at 73 referring to para 8.

18 Commonwealth Secretariat ***Draft Model Law on the Protection of Personal Information*** LMM(02) 8 October 2002 (hereafter referred to as "Commonwealth Model Law for Private Bodies") at 2.

19 Bygrave at 73.

setting of data protection standards. These include the World Trade Organisation (WTO), World Intelectual Property Organisation (WIPO) and the World Wide Web Consortium (W3C). Many of these bodies will approach data protection from a market-oriented rather than a human rights perspective.[20]

7.2.12 At a national level, obvious examples of relevant bodies are those charged with hearing appeals from the decisions of data protection authorities. Other examples are parliamentary committees, ombudsmen and national auditing offices. Some countries' laws make specific provision for industries, professions, etc to draw up sectoral codes of conduct/practice on data protection in co-operation with data protection authorities.[21] An increasing number of schemes for the development of such codes is likely, given that the EC 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.[22]

7.2.13 These authorities must act with complete independence in exercising the functions entrusted to them. 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 a data 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).[23]

7.2.14 This criterion of independence boils down to the capacity for a data 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

---

20 Bygrave at 74.

21 See eg Parts VI-VII of the New Zealand Act; s 51(3)-(4) of the United Kingdom Act; Part IIIAA of the Australian Act; and Art 25 of the Netherlands' Act.

22 Bygrave at 74 referring to Art 27.

23 Bygrave at 71.

usually be subject to political and legal review. Moreover, decision making by an authority will be steered at a more general level by laws and regulations laid down by other bodies.[24]

7.2.15 The Directive contains several provisions which will stimulate an internationalisation, at least within the EU, of supervisory and monitoring regimes in the field of data protection.[25] 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, but 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.[26]

7.2.16 At the 23rd International Conference of Data Protection Commissioners[27] an accreditation procedure (for recognising the credentials of data protection authorities for the purposes of the International Conference) was established.[28] The following rules were set: The data 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. [29]

7.2.17 Most data protection laws lay down special rules to enhance the ability of data protection authorities to monitor the practices of data controllers. While data protection laws expound similar core principles, there are numerous differences between them in terms of the monitoring and

---

24 Bygrave at 70.

25 See Art 28(6) in this regard.

26 Bygrave at 73.

27 Held in Paris, France 24-26 September 2001.

28 Accredited members would have a legitimately full share in the resolutions which may be adopted.

29 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.

supervisory regimes they establish:

a) One category requires data controllers simply to **notify** data protection authorities of certain planned processing of personal information.[30] Upon notification, processing is usually allowed to begin. [31] Most data protection laws, including the EU Directive (the other three main international data 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.[32]

b) Occasionally, the notification requirement is formalised as a system for **registration**. [33] Under this sort of system, data controllers must as a general rule apply to be registered with the data protection authority, registration being a necessary precondition for their processing of personal data. Once application for registration is lodged, the controller is legally able to begin processing.[34] The UK is an example of the registration model.

c) Another category of control/oversight requires that data controllers must apply for and receive specific authorisation (in the form of a **licence)** from the relevant data protection authority prior to establishing a personal register or engaging in a particular data -processing activity. Only a minority of data 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

---

30 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.

31 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 porcessing.

32 Bygrave at 75.

33 Repealed sections 4-9 of the UK Act of 1984.

34 Bygrave at 75.

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 data or for the matching of data.[35] Sweden is and example of the licencing model.

7.2.18 Apart from monitoring the practices of data controllers, agencies may also have other duties. Some examples are as follows:[36]

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.

b) The bodies have the power to conduct **investigations** and have a right 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.

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 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: ombudsman, public prosecutor, universities, autonomic data 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

---

35 Bygrave at 76.

36 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 (hereafter referred to as "Lopez").

Freedom of **Information Act**. These include Hungary,[37] Estonia, Thailand, Ireland[38], and the United Kingdom 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 data protection and freedom of information.

7.2.19 The contemporary role of the Data Protection Authority is therefore that of ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer and international ambassador**.**[39]

7.2.20 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 practice and encouraging industry associations to adopt them. They also can use their annual reports to point out problems.

7.2.21 Problems experienced by agencies in giving effect to data legislation are as follows:

a) A major problem with many agencies around the world is a **lack of resources** to adequately conduct oversight and enforcement. Many 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.[40]

---

37 The Hungarian Data Protection and Freedom of Information Commission have created 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. The Hungarian Data Protection Act is unique in Europe in that it is not really an act of "data protection", as it is habitually referred to, but rather a law on rights to freedom of information. The Commissioner is constantly driven by this very dual function to seek the balance or, to put it more accurately, the often narrow path between these two freedom rights, which at times seem fundamentally contradictory and are always of a mutually limiting force.

38 The Irish Commission has also 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.

39 Bennett CJ "The Data Protection Authority: Regulator, Ombudsman, Regulator or Campaigner?" Presentation at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, 9-11 September, 2002.(hereafter referred to as " Bennett Conference Paper").

40 Task Group on Open Democracy ***Open Democracy Act for South Africa : Policy Proposals,*** 1995 on 18. The proposals were compiled on the basis of preliminary consultations undertaken by the Task Group late in 1994. They identified principles, rather than details to serve as the basis for further consultations early in 1995. In so far as costs and

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. In Japan and Thailand, the oversight agency is under the control of the Prime Ministers Office. In Thailand, the director was transferred in 2000 after conflicts with the Prime Ministers' Office. In 2001, Slovenia amended its Data Protection Act in order to establish an independent supervisory authority and thereby ensure compliance with the Data Protection Directive. This was previously the responsibility of the Ministry of Justice. 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.

7.2.22 On the other hand, the enactment of comprehensive legislation may have the following negative implications for data users:

a) The database owners may face additional costs in having to comply with whatever legislation is passed;[41]

b) Data users 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.[42]

---

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.

41 The USA is currently debating the merits of privacy legislation and a major part of the debate concerns the costs to business. See above in fn 53 at 11 the studies being conducted in this regard.

42 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.

7.2.23 All data protection Acts stipulate a variety of sanctions and remedies for breach of their provisions. Provision is usually made for a combination of penalties (fines and imprisonment), compensatory damages and where applicable, revocation of licences and deregistration.

7.2.24 The topic of sanctions and remedies is dealt with only in very general terms by the CoE Convention, OECD Guidelines and UN Guidelines. The EC 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.[43] It also stipulates that decisions by a data protection authority which give rise to complaints "may be appealed against through the courts".[44]

7.2.25 In many jurisdictions, the enforcement of data protection laws seems rarely to involve meting out penalties in the form of fines or imprisonment. Data protection authorities appear generally reluctant to punitively strike out at illegal activity with a "big stick". 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, data 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.[45]

7.2.26 Examples of the work done by Privacy Commissioners in other countries are as follows:

a) In Canada both the Privacy Act and PIPEDA are overseen by the independent Privacy Commissioner of Canada:

   – Under the Privacy Act[46] the Commissioner has:

---

43 Art 22.

44 Art 28(3).

45 Bygrave at 79 and references therein.

46 EPIC Report 2002 at 133: 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. 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

- •• the power to investigate, mediate, and make recommendations, but cannot issue orders or impose penalties.
- •• During the course of an investigation the Commissioner may subpoena witnesses and compel testimony, and enter premises in order to obtain documents and conduct interviews.
- •• The Commissioner is also charged with conducting periodic audits of federal institutions to determine compliance with the Privacy Act, and to recommend changes where necessary.
- •• The Commissioner can initiate a Federal Court review in limited circumstances relating to denial of access to records.

– The Commissioner's powers under PIPEDA [47]are very similar to those under the Privacy Act.

- •• The Commissioner has powers of recommendation only with regard to complaints submitted under the Act. Once a complaint is received, the Commissioner assigns an investigator to look into the matter. The investigator then submits his findings to the Commissioner who then considers the case and issues a report with recommendations.
- •• He can also request the organisation in question to submit, with a specified period of time, notice of any action taken or proposed to be taken to implement these recommendations.[48]
- •• However, if the Commissioner is satisfied that there are reasonable grounds

---

more than 8,047 requests for information concerning the Privacy Act.

47 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.requests for information concerning PIPEDA, 95 formal complaints (half of which involved banks) and initiated 198 investigations.Office of the Privacy Commissioner, Canada ***Annual Report to Parliament* 2000-2001, Part Two–** ***Report on the Personal Information Protection and Electronic Documents Act***, December 200. The Commissioner's office completed and issued findings and recommendations on 27 complaints.

48 See generally Office of the Privacy Commissioner, Canada ***Your Privacy Responsibilities: A Guide for Business and Organizations*** December 2000.

to investigate a matter under the Act, he may initiate his own complaint.[49]

- Under PIPEDA the Commissioner is also authorised to conduct broad research into privacy issues and promote awareness and understanding of privacy issues among Canadians.

b) In the UK[50] the Data 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;
- assessing processing with the consent of data controllers;
- laying reports and codes of practice before each House of Parliament;
- assisting individuals where processing is for special purposes; and
- participating in international co-operation.

7.2.27 The Data Protection Act 1998 furthermore follows a twin track approach (as it did with the 1984 Act) by giving the Commissioner powers of enforcement whilst also providing for a number of criminal offences under the Act. The Commissioner therefore has powers and functions pertaining to notification, enforcement, prosecution of offenders and powers of entry and inspection all set out in the relevant sections of the act.

---

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

50 Bainbridge at 217 and 143.

7.2.28 The act also makes provision for the Data Protection Tribunal. The purpose of the Tribunal is primarily to hear appeals from data controllers in respect of notices served by the commissioner or determinations made by the Commissioner as to whether processing is for special purposes. A data subject, however, does not have a right to appeal to the Tribunal against a decision of the Commissioner.

7.2.29 An important question in the privacy debate in South Africa would be whether a Data Privacy Act should in fact make provision for a data protection agency. In parallel debates during consultations on the Open Democracy Act about the necessity of a regulating agency to ensure enforcement of this Act (which of course included privacy provisions at that stage),[51] the following interesting viewpoints were held:

(i) The **Human Rights Commission**[52] noted that the ODB did not establish a data 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 sets out the High Court as the forum for relief. The Commission believed the High Court to be an inappropriate forum. It is inaccessible, 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. Thus is particularly relevant to access to information, where there is no existing precedent, and a body of jurisprudence needs to be developed from scratch. The Commission 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 at all. These included the creation of a tribunal system, or the use of an ombudsman or Information Commissioner to resolve disputes. These options need careful consideration, with emphasis on the

---

51 The Bill subsequently became known as the Promotion of Access to Information Ac 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.

52 Submission to the Open Democracy Bill.

short-term cost implications of setting up new bureaucracies, and the long term cost implications of clogging up the court system even further.

(ii) The **Open Democracy Lobby Group**[53] 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.

(iii) 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 would be to dispose of complaints lodged in terms of the Promotion of Access to Information Act in a procedurally fair, economical and expeditious manner. [54]

7.2.30 As stated above the newly proposed Commonwealth legislation also makes provision for the establishment of an independent Privacy Commissioner with a range of functions and powers, but on an optional basis. Accordingly it could be omitted in the case of a country having an insufficient resource base to allow the creation of an additional public officer, thereby making it necessary for the enacting country to designate a person to perform certain critical functions relating to the protection of personal privacy. It is the view of the Commonwealth Secretariat that

---

53 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).

54 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.

provided such person has, in the exercise of his or her duties under the Act, adequate independence, the integrity of the legislation would not be jeopardized.

7.2.31 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[55] as may be specified in the instrument of appointment.

7.2.32 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

---

55 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 Minster 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.

powers to carry out an investigation in this regard.[56]

7.2.33 With regard to private bodies the Privacy Commissioner shall have similar powers and duties.[57]

7.2.34 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.

7.2.35 Whether or not South African privacy legislation should make provision for a statutory regulatory authority is one of the main questions that will have to be answered

---

56 The [Commissioner] will have, in relation to carrying out of the investigation of any complaint under this Act, power -

(a) to summon and enforce the appearance of persons before the *[Commissioner*] and compel them to give oral or written evidence on oath and to produce such documents and things as the *[Commissioner*] deems requisite to the full investigation and consideration of the complaint, in the same manner and to the same extent as a superior court of record;

(b) to administer oaths;

(c) to receive and accept such evidence and other information, whether on oath or by affidavit or otherwise, as the *[Commissioner*] sees fit, whether or not the evidence or information is or would be admissible in a court of law;

(d) to enter any premises occupied by any public authority on satisfying any security requirements of the authority relating to the premises;

(e) to converse in private with any person in any premises entered pursuant to paragraph(d) and otherwise carry out therein such inquiries within the power of the *[Commissioner*] under this Act as the *[Commissioner*] sees fit; and

(f) to examine or obtain copies of or extracts from books or other records found in any premises entered pursuant to paragraph(d) containing any matter relevant to the investigation.

57 Art 34 of the Commonwealth Model Law for Private Bodies.

during this investigation. We therefore require the guidance of our readers in this regard. What should the level of this authority be? Where should it be housed?

7.2.36 As seen above, 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.[58]

b) Sectoral laws

7.2.37 The United States is a good example of a country where industries 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. [59]

7.2.38 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.[60]

7.2.39 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. [61]

---

58 Bennett Paper.

59 Reidenberg at 2.

60 Ibid.

61 NTIA Privacy Report at 11.

7.2.40 For instance, in the USA, Congress has created specific statutory rights to privacy for oral and electronic communications;[62] financial, educational and credit information;[63] criminal history,[64] and even video rental records.[65] All of these laws were passed following collaboration among civil liberties, consumer, and industry groups.[66]

7.2.41 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, medical records and marketing information.[67] 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.[68]

7.2.42 This statutory gap-filling approach also leaves many areas of information processing untouched and runs counter to the cross-sectoral nature of modern data processing[69].

7.2.43 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

---

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

63 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).

64 Privacy Act of 1974, 5 U.S.C. 552a(2)(a) (1974); Freedom of Information Act, 5 U.S.C. 552 (1966).

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

66 Goldman at 2 and references therein to the abovementioned legislation.

67 Gellman RM "Data Privacy Law (book review)" ***Government Information Quarterly*** vol 14 no 2 1997 at 215-217. Review of the book by Scwartz PM and Reidenberg JR ***A Study of United States Data Protection*** Charlottesville, VA Michie 1996.

68 Reidenberg at 2.

69 Reidenberg at 5.

have no recourse at all. Also, foreign governments have nowhere to bring concerns about disparate privacy regulation.[70]

c) Self regulation

7.2.44 In the USA there is general distrust of State control of economic and social matters, accompanied by scepticism towards legislative regulation of the private sector except where there are proven to exist flagrant imbalances of power between private parties which cannot be corrected otherwise than by legislative intervention. Industries have therefore been encouraged to self-regulate. [71]

7.2.45 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.[72]

7.2.46 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.[73]

7.2.47 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

---

70 Gellman supra.

71 Froomkin AM "The Death of Privacy?" ***Stanford Law Review*** Vol 52:1461 May 2000 (hereafter referred to as " Froomkin") at 1525.

72 Hustinx PJ "Co-regulation or self-regulation by public and private bodies - the case of data protection" Published in Freudendesgabe fur Alfred Bullesbach 2002 Umbruch von Regelungssystemen in der Informationgesellschaft (hereafter referred to as "Hustinx") at 2 as referred to by EPIC Report 2002.

73 Bennett at 23; 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 (hereafter referred to as "Raab").

serious proposals for self-regulation among market participants rely on the threat of government regulation if the data collectors fail to regulate themselves sufficiently.[74]

7.2.48 In a more positive sense, self-regulation is often advanced as a means of experimenting and to prepare for regulation in a positive way. Another option that self-regulation 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.[75]

7.2.49 In order for institutions to regulate themselves four interrelated policy instruments may play a role[76] namely privacy statements, privacy codes, privacy standards and privacy seals.

i) Privacy commitments/ statements

7.2.50 Privacy commitments perform no other function than to indicate to clients, consumers and regulators that the orgnisation has considered privacy protection at some level, and 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 data. Many examples can be found in the privacy statements to be found on contemporary public and private sector websites.[77] 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.[78]

---

74 Froomkin at 1525.

75 Hustinx at 2.

76 Raab at 1.

77 Bennett Conference Paper at 17.

78 Bennett Conference Paper at 18.

ii) Codes of conduct

7.2.51 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.[79]

7.2.52 The successful implementation of privacy policy is inextricably linked to the ways in which that policy is developed. Before any codification takes place, a central question should be posed: Should the policy merely reflect existing business approaches, or should it reflect goals for which the organisation might strive in future. The correct answer is that it should reflect a thorough understanding of existing practices, as well as a commitment to improve.[80]

7.2.53 In short, the organisation should be prepared to implement any policy it codifies. The term “code of practice” should be reserved for codified policies that not only state commitments to the outside world, but also bind employees to these obligations.

7.2.54 Many codes are developed in the absence of a regulatory framework in order to avoid or anticipate further regulatory intervention. 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

---

79 Bennett Voluntary Codes Project at 4.

80 Bennett Voluntary Codes Project at 16.

range of incentives and sanctions are continuously at work.[81]

7.2.55 Countries where privacy codes perform crucial functions within the framework of statutory data protection regimes are The Netherlands, New Zealand, Ireland and the UK. Art 27 of the European Directive furthermore requires member states to "encourage the drawing up of codes of conduct intended to contribute to the proper implementation of ....national provisions... taking account of the specific features of various sectors." [82]

7.2.56 Codes of practice do however offer some clear advantages even within a legislated data protection regime. The process of negotiating codes enhances the understanding of the privacy problem within different sectors. It also allows the data protection authority to gain a better appreciation of the relevant privacy issues and directly to influence the self-regulatory mechanisms. Codes are flexible instruments and can be adapted to changing economic and technological developments. [83]

7.2.57 Five kinds of privacy code can be identified[84] according to scope of application: organisational code[85], the sectoral code,[86] the functional code[87], the professional code[88] and the

---

81 Bennett Voluntary Codes Project at 21.

82 Bennett Conference Paper at 4.

83 Ibid.

84 Raab at 9-11 identifies five types of privacy code: organisational codes, sectoral codes, functional codes, technological codes and professional codes.

85 This applies to one agency that is bound by a clear organisational structure.

86 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.

87 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.

88 Codes developed for those directly involved in information processing activities eg market researchers, and health professionals.

technological code[89].

7.2.58 In South Africa the Direct Marketing Association stressed the fact that all members of the Association are bound by a stringent Code of Practice based on international norms, and which was developed in conjunction with the Consumer Affairs Committee of the Department of Trade and Industry.[90].

iii) Privacy standards

7.2.59 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 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.[91]

7.2.60 The idea of a more general privacy standard[92] that could incorporate the entire range of privacy protection principles has been negotiated in Canada.[93] 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, have recently

---

89 As new potentially intrusive technologies have entered society, codes have developed to deal with their specific application.

90 Barnard F "Informal Notes from the DMA to the Law Commission re a Possible New Data Privacy Act for SA" 14 September 2001 at 1.

91 Bennett Conference Paper at 22. See in this regard the British Standard, BS7799.

92 Bennett Conference Paper at 23.

93 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.

been negotiated in Australia and Japan.[94]

7.2.61 The Centre Europeanne de Normalisations (CEN), responsible for the negotiation of standards within Europe, has begun to study the feasibility of an international privacy standard, supported by the Article 29 Working Party. This would comprise a general data protection standard which would set out practical operational steps to be taken by an organisation in order to comply with relevant data protection legislation, a series of sector specific initiatives in key areas such as health information and human resource management and task specific initiatives mainly related to the online environment. [95]

iv) Privacy seals

7.2.62 One logical corollary of any standard is a commonly understood mark, symbol or cachet that can be awarded to any organisation that is successfully certified or registered. The development of a specific "mark" or "seal" for privacy protection has, however, proliferated on the Internet. These programmes are built on the premise that consumers should be able to have consistent disclosure of privacy practices from all sites with which they interact.

7.2.63 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.[96]

7.2.64 What is needed therefore is a granting organisation responsible for examining private

---

94 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 has been overtaken by a more general legislative approach.

95 Bennett Conference Paper at 24.

96 Bennett Conference Paper and references therein.

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.[97]

7.2.65 Current seal programmes have not inspired great confidence.[98] Furthermore, the more privacy seal programmes in existence, the more the consumer will be confused, and the more difficult it will be for any one system to achieve a reputation as the methodology by which privacy protective practices can be claimed and assured. [99]

7.2.66 Ideally these four instruments (commitments, codes, standards and seals) should be cumulative. The self-regulatory process should involve:[100]

a) an agreement and statement of organisational policy;

b) a codification of that policy throughout the oganisation or sector;

c) a verification of those practices through some external and independent conformity assessment process; and

d) the assignment of a "seal of good housekeeping".

7.2.67 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

---

97 Bennett Conference Paper at 25.

98 See discussion in Froomkin at 1525 as to the actions of the trustmarkholder TRUSTe. It became clear that firms licence the trustmark and some corporate sponsors contribute huge soums 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 that are better off without the trustmark and the attendant hassle.

99 Bennett Conference Paper at 26.

100 Ibid.

in privacy self-regulation in this cumulative and logical manner are very few.[101]

7.2.68 A more generic problem with self-regulatory schemes is that they regulate only those motivated or principled enough to take part in them. [102]

7.2.69 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.[103] In this document it was stressed that to implement meaningful, consumer-friendly, self-regulatory regimes to protect privacy, self-regulation must do more than articulate broad policies or guidelines. Effective self-regulation also involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from non-compliance.

7.2.70 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

---

101 Ibid.

102 Froomkin at 1528.

103 National Telecommunications and Information Administration, Department of Commerce ***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 "Commerce Report") at 1.

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.

d) Technology

7.2.71 While technology has made our personal lives more transparent, privacy and technology are not inherently antagonistic. [104]

7.2.72 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.[105]

7.2.73 Technology by itself is therefore neither a privacy enhancer nor a privacy threat. This is to be determined by its uses.[106] Technology will become a privacy enhancer if appropriate awareness, education, management processes/business models are developed.[107] Some argue that new technologies may prove to be one of the most potent forces driving the right to

---

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

105 Valeri at 3..

106 Valeri at 8.

107 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

informational self-determination.[108]

7.2.74 Technology can also solve or at least alleviate privacy problems. Identity management systems and intelligent tools for blocking, filtering and customisation will help individuals to limit the amount of personal information released to what is really necessary and intended. These mechanisms range the technological gamut from cryptography to cookie cutters, and from anonymisers to an industry-proposed consumer "choice" approach called "Platform for Privacy Preferences" or P3P.[109]

7.2.75 The proposals originate from technologists, consumers, or industry, all of whom profess an interest in "protecting" users ' privacy in cyberspace. Some of these self-help technologies spring from a mindset of self-defense. Surveillance technologists compete to defeat the privacy technologists, who in turn find some way around data collectors. Other technologies arise from industry representatives, who believe that for net commerce to thrive, industry as a whole must "compromise" with consumer groups in restricting the type of private information that is collected, and the use to which it is put and that some self-restrictions are required.[110]

7.2.76 Privacy Enhancing Technologies (PETs) have been defined as [111]

> 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.

7.2.77 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

---

108 Piller at 7.

109 Berkman Center for Internet and Society (Berkman Online Lectures and Discussions) Harvard Law School ***Privacy in Cyberspace 2002*** Module VI: Self-help Mechanisms: Cryptography, Privacy-enhancing Technologies, and P3P available at http://eon.law.harvard.edu/privacy/module6.html (hereafter referred to as "***Privacy in Cyberspace***") at 1.

110 ***Privacy in Cyberspace*** at 1.

111 Reference to the definition of Herbert Burkert in fn 288 in Froomkin at 1529.

seeks to reduce the transaction cost of determining how much personal data should be surrendered in a given transaction.[112]

7.2.78 The P3P project provides a standard way for websites 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 websites can refer to in their privacy policies and a protocol requesting and transmitting website privacy policies. P3P enabled websites 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.

7.2.79 System designers can organise a system to withhold (or never gather) data about the person, the object of the transaction, the action performed, or even the system itself. Most electronic road-pricing schemes currently deployed identify the vehicle or an attached token.[113]

7.2.80 For matters involving electronic communications or data storage, encryption is the major PET. Governments , however, sometimes try to retard the spread of consumer cryptography that might be used to protect e-mails, stored data, faxes etc from eavesdroppers and intruders, ostensibly because these same technologies also enable the targets of investigations to shield their communications from investigators.[114]

7.2.81 Critics of the technology model argue that it suffers from the absence of a representative public policy debate and from the commercial pressure toward technical structures that maximise data collection and data veillance. Commercial pressures push developers and implementers toward products that collect as much information about users as is possible. Typically, these "data creep" functions are either non-transparent to the user or incomprehensible. These technical

---

112 Froomkin at 1529.

113 Froomkin at 1530.

114 Froomkin at 1532.

decisions hide important policy issues for privacy.[115]

7.3 Conclusion

7.3.1 In comparing different data protection laws, cross-national regulatory trends[116] can be identified.[117] Some of these are as follows:

a) Increasing regulatory density, therefore more detailed discriminating provisions and requirements;

b) Increasing concern to lay down procedural mechanisms for enforcing compliance with the data principles;

c) A shift in regulatory focus, for instance the encouragement of sectoral codes of practice;

d) A trend away from comprehensive licencing regimes to requirements for mere notification/registration of data-processing operations; and

e) Enhancement of opportunities for participatory control.

7.3.2 The Commission agrees in principle with the argument that the different models referred to above are neither self-sufficient not complete alternatives to one another.[118] Though conceived as distinct rule sets, the legal, technological and market models of fair information practices are in fact interdependent as tools for effective data protection. The different models need to be channelled in the same direction so that the rules support each other rather than frustrate each other.

---

115 Reidenberg at 4.

116 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 at 88.

117 Bygrave at 88.

118 Reidenberg at 3.

7.3.3 The following guiding principles can be identified:

a) Legislation will be necessary to establish the public policy objectives.

b) These principles will have to be implemented by some form of statutory regulatory authority working in conjunction with industry.

c) In a democratic society, rule-making through technology will be shaped by public policy goals and debate.

d) Legal liability will be an essential instrumental device for the development of privacy products.

The Commission invites comment on all these issues.

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 directly the experiences of other countries 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]

8.1.2 Even taking into account these influences, it is clear that there has been a harmonisation

---

1 The information reflected in this chapter is based on extracts from Parts 2 and 3 (Country Reports) of the ***Privacy and Human Rights Report 2002*** published by the Electronic Privacy Information Center *(*EPIC) and Privacy International and the references therein, unless otherwise indicated . This annual report by EPIC and Privacy International reviews the state of privacy in over fifty countries around the world. It outlines legal protections for privacy, new challenges, and summarises important issues and events relating to privacy and surveillance. It is available at http://www.privacyinternational.org/survey/phr2002/ .

2 Performance and Innovation Unit of the UK Cabinet Office ***Privacy and Data-Sharing: The Way Forward for the Public Services*** Ann B, International Comparisons April 2002 (hereafter referred to as " 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.

in the implementation of data protection principles and that the international nature of these principles has already, and will also in future, promote the development of global standards.

8.2 International Directives[7]

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 are 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 Data;[10] 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 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

---

7 See discussion in Chapters 1and 6 above.

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

9 Bygrave at 30.

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

11 OECD Guidelines.

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

13 Art 23.

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 Directive[16] 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 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 the future, the commercial and government use of such information will generally require "explicit and unambiguous" consent of the data subject. The

---

14 Bygrave at 32.

15 Bygrave at 34.

16 EU Directive.

17 For further discussion see Ch5 above.

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 proved 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 data 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 data 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 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

---

18 See Ch 1 above.

19 As referred to in Strathclyde 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 at 33.

by small and developing countries without the need to create significant new structures.[22]

8.2.14 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.

8.3 United States of America[23]

8.3.1 The United States Constitution does not explicitly mentions a right to privacy. The Supreme Court has ruled that there is a limited constitutional right of privacy based on a number of provisions in the Bill of Rights and subsequent amendements.[24] This includes a right to privacy from government surveillance into an area where a person has a "reasonable expectation of privacy" [25] and also in matters relating to marriage, procreation, contraception, family relationships, child rearing and education. [26]

---

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 EPIC at 382 and the references made therein.

24 Such as the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments.

25 ***Katz v United States*** 389 U.S. 347, 19 Led 2d 576,88 Sct 507.

26 See e.g., ***Griswold v Connecticut***, 381 U.S. 479, 14 Led 2d 510, 85 Sct 1678; ***Whalen v Roe*** 429 U.S. 589 (1977); ***Paul v Davis*** 424 U.S. 714 (1976).

8.3.2 These rights are said to be substantive privacy rights distinguishable from informational privacy rights. Therefore, records held by third parties, such as financial records or telephone calling records are generally not protected unless a specific federal law applies.

8.3.3 The Privacy Act of 1974 protects records held by United States Government agencies and requires agencies to apply basic fair information practices. [27] 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.

8.3.4 The United States has no comprehensive privacy protection law for the private sector. A patchwork of federal laws covers some specific categories of personal information.[28] These include financial records,[29] credit reports, [30] video rentals, [31] cable television, [32] children's (under age 13) online activities, [33] educational records,[34] motor vehicle registrations, [35] and telemarketing. [36]

8.3.5 There is no independent privacy oversight agency in the United States:

– The Office of Management and Budget 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

---

27 Privacy Act, Pub. L. No. 93-579 (1974), codified at 5 USC § 552a,.

28 See Marc Rotenberg, ***The Privacy Law Sourcebook****:* United States Law, International Law, and Recent Developments (EPIC 2001).

29 Right to Financial Privacy Act, Pub. L. No. 95-630 (1978).

30 Fair Credit Reporting Act, Pub. L. No. 91-508 (1970), amended by PL 104-208 (1996).

31 Video Privacy Protection Act**,** Pub. L. No. 100-618 (1988).

32 Cable Privacy Protection Act, Pub. L. No. 98-549 (1984).

33 See Center for Media Education, A Parent's Guide to Online Privacy.

34 Family Educational Rights and Privacy Act, Public Law 93-380, 1974.

35 Drivers Privacy Protection Act, PL 103-322, 1994.

36 Telephone Consumer Protection Act, PL 102-243, 1991.

Management and Budget to coordinate federal stances towards privacy. The Counselor had only a limited advisory capacity. The new 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. [37] 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 Internet Privacy. [38] Instead, FTC has focused on enforcing existing law in the areas of telemarketing, spam, pretexting, and children's privacy. [39] 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. [40]

8.3.6 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 weak protections on financial information that is likely to be shared among merged

---

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

38 Protecting Consumers' Privacy: 2002 and Beyond, Remarks of FTC Chairman Timothy J. Muris, October 2001.

39 See FTC Privacy Initiatives.

40 The Proposed National "DO NOT CALL" Registry, Amendment to the Telemarketing Sales Rule, January 2002.

institutions. In spite of the low level of protections conferred, the effective date of the privacy provisions were pushed back from November 2000 until July 2001.

8.3.7 In October 1998 US Congress enacted the Children's Online Privacy Protection Act (COPPA), requiring commercial website operators to provide clear notice of their information gathering practices and to obtain parental consent before information is collected from children under the age of 13. The Act, which went into effect in April 2000, allows parents to access and check the information which has been collected and curtail its use. [41]

8.3.8 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.[42]

8.3.9 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.

---

41 FTC Privacy Pages .

42 EPIC Report 2002 385 referring to the 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.

[43] A number of court cases have dealt with the protection of right to privacy and data.[44]

8.3.10 There has been significant debate in the United States in recent years about the development of privacy laws covering the private sector:

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.[45]

c) There is also **substantial activity in the states**. In recent years, Massachusetts and Hawaii have considered comprehensive privacy bills for the private sector. California passed a Social Security Number bill that will prevent the printing of the identifier on forms, invoices, and identification badges. The bill also gives individuals greater power to control their credit report once fraud is suspected. Minnesota enacted a bill that requires ISPs to give notice and obtain user authorisation before using personal information for secondary purposes. In a statewide referendum, North

---

43 See ***Lake v WalMart Stores, Inc***., 582 N.W.2d 231 (Minn. 1998), for a review of state adoption of common law privacy torts.

44 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 Bibl*e, the Court invalidated a law that required registration with the government before individuals could engage in door-to-door solicitation. The Court held that a pre-registration requirement violated the First Amendment and individuals' right to anonymity. ***Watchtower Bible & Tract Soc'y of N.Y. v. Village of Stratton***, 122 S. Ct. 2080 (2002). In ***United States v 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 *Earl*s, the Court held that random, suspicionless drug testing of students involved in non-athletic extracurricular activities was justified under the "special needs" exception to the Fourth Amendment.Bd. of ***Educ. v Earls***, 122 S. Ct. 2559 (2002). In *Falv*o, the Court held that both peer grading and the reporting aloud of peer grades did not violate the Family Educational Rights and Privacy Act of 1974 (FERPA).***Owasso Indep. Sch. Dist. No. I-011 v Falvo***, 534 U.S. 426 (2001). In *Gonzag*a, the Court held that the FERPA does not give individuals a right to sue for violations of privacy ***Gonzaga Univ. v Doe***, 122 S. Ct. 2268 (2002).

45 See EPIC Bill Track.

Dakota residents established opt-in protections for financial information. Additionally, Georgia enacted a privacy law that prohibits private businesses from discarding documents or computer components that contain personal information[46].

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. [47] A series of companies, including Intel and Microsoft, were discovered to have released products that secretly track the activities of Internet users. [48] 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[49]** has been created and private-sector corporations are collaborating to use commercial marketing data for terrorism profiling. [50]

f) The past year has seen a new trend towards the increased use of **video surveillance** cameras linked with facial recognition software in public places. [51]

g) There have been a number of proposals to create a **National ID** in the wake of the

---

46 EPIC Report 2002 at 386.

47 Hoofnagle CJ ***Consumer Privacy In the E-Commerce Marketplace 2002*** Third Annual Institute on Privacy Law Practicing Law Institute G0-00W2 (June 2002).

48 See Big Brother Inside Campaign .

49 H.R. 5005, Homeland Security Act of 2002.

50 See Letter from the Center for Information Policy Leadership to Interested Parties, 2002.

51 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.

September terrorist attacks. [52] Most of these efforts have sought the creation of a national identification system through the standardisation of state driver's licenses.[53] [54]

8.4 United Kingdom of Great Britain and Northern Ireland[55]

8.4.1 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 establishes an enforceable right of privacy. [56] 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. [57]

8.4.2 The Parliament approved the Data Protection Act in July 1998. [58] The legislation, which came into force on March 1, 2000, updates the 1984 Data Protection Act in accordance with the requirements of the European Union's Data Protection Directive. [59] The Act covers records held by government agencies and private entities. It sets rules for processing personal information and applies to some paper records as well as those held on computer. It provides for limitations on the use of personal information, access to and correction of records and requires that entities that maintain records register with the Information Commissioner.

---

52 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.

53 ***Your Papers Please: From A State Driver's License to a System of National Identification***, EPIC Report, February 2002.

54 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.

55 EPIC at 375 and the references made therein.

56 Human Rights Bill, CM 3782, October 1997.

57 See "Developments in Jurisprudence", Appendix, Information Commissioner – Annual report and accounts for the year ending March 31 2002, June 2002 .

58 Data Protection Act 1998c. 29.

59 Data Protection Act 1984 (c. 35).

8.4.3 The Office of the Information Commissioner (formerly known as the Data Protection Commissioner and the Data Protection Registrar), is an independent supervisory authority that maintains the register and enforces the Act. [60] Statistics are published in the Annual Report.[61] In October 2000, the Commissioner issued a draft code of guidance for employer/employee relationships.[62]

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. [63]

8.4.5 There are also a number of other laws containing privacy components, most notably those governing medical records[64] and consumer credit information.[65] 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 may be 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.[66]

8.4.6 The privacy picture in the United Kingdom is mixed. There is, at some levels, a strong

---

60 Home page of the Information Commissioner, <http://www.dataprotection.gov.uk/>

61 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.

62 Data Protection Commissioner, Employment: (Draft COP), October 2000.

63 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.

64 Access to Medical Reports Act 1988, Access to Health Records Act 1990, The Health and Social Care Act 2001.

65 Consumer Credit Act, 1974.

66 Crime & Disorder Act 1998: Data protection implications for information-sharing.

public recognition and defence of privacy. Proposals to establish a national identity card, for example, have routinely failed 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.[67]

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.[68] The cards would be mandatory for all persons over 16 years old and would be required to obtain heath care, jobs and other services. [69]

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)[70] and the European Convention for the Protection of Human Rights and Fundamental Freedoms.[71] In November 2001, the United Kingdom signed the Council of Europe Convention on Cybercrime.[72] 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.

8.5 Kingdom of the Netherlands[73]

---

67 See Criminal Justice and Public Order Act 1994

68 See Privacy International ID Cards Page.

69 The proposal has already been widely criticised by politicians and major media across the political spectrum and is not expected to be approved. Blunkett first proposed the card shortly after September 11 but was forced to back away after it was also severely criticised.

70 Signed May 14, 1981; Ratified August 26, 1987; Entered into Force December 1, 1987.

71 Signed November 11, 1950; Ratified March 8, 1951; Entered into Force September 3, 1953

72 Signed November 23, 2001.

73 EPIC at 271 and the references made therein.

8.5.1 The Constitution[74] grants citizens an explicit right to privacy. [75]

8.5.2 In terms of the Data Protection Act of 1988 (now repealed) provision was made for the possibility to develop a code of conduct as means of implementation of the data principles and to request the Data Protection Authority for its approval of the code. 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.

8.5.3 In June 2000 a new act, the Personal Data Protection Act of 2000 was approved by the Parliament.[76]. This bill is a revised and expanded version of the 1988 Data Registration Act and replaced it. Its purpose is to bring Dutch law in line with the European Data Protection Directive and to regulate the disclosure of personal data to countries outside of the European Union. The new law

---

74 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."

75 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. 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."

76 Personal Data Protection Act, Staatsblad 2000 302, July 6, 2000, unofficial translation.

went into effect in September 2001. The sectoral codes of conduct still enjoy a considerable degree of popularity and are currently under revision for adaptation to the new legislation.

8.5.4 The College Bescherming Persoonsgegevens (CBP) serves as the Data Protection Authority and exercises supervision of the operation of personal data files in accordance with the Act.[77] 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.[78]

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) project which was established to develop privacy enhancing techniques to protect user information in electronic transactions[79].[80]

8.5.6 In its annual report for the year 2000, issued in May 2001, the Chamber drew attention to the increasing use of video surveillance cameras in public spaces, threats to privacy in the health sector, and the need for further privacy protection on the Internet.

8.5.7 Two decrees have been issued under the Data Registration Act. The Decree on Sensitive Data [81] 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

---

77 Homepage <www.cbpweb.nl>.

78 In 2001 the CBP received approximately 9,000 requests, a large increase over previous years. This increase is attributed to the increased public attention surrounding the passage of the new law. The CBP received approximately 300 complaints and requests for mediation, of which many related to requests for access to police records. The CBP issued a number of public education reports during 2001 and a policy framework for the transfer of data to third countries.

79 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.

80 College Bescherming Persoonsgegevens, Annual Report for the Year 2001, July 2002.

81 Decree on Sensitive Data, March 5, 1993.

in a personal data file. The Decree on Regulated Exemption[82] exempts certain organisations from the registration requirements of the Data Registration Act.

8.5.8 In May 2000, Dutch Internet providers canceled a deal with the Justice Department to provide names and addresses of Internet users under criminal investigation without a court order if the case involves a serious crime. Dutch privacy law gives the holder of a data registry the right to give out personal data to third parties in "pressing cases." The agreement between the providers and the Justice Department had to be halted nevertheless after a court ruled that the Justice Department was requesting information without a clear urgency.

8.5.9 In February 2002 privacy and civil liberties organisation, Bits of Freedom, organised the first Dutch Big Brother Awards (awards for most egregious privacy violations given each year by Privacy International and affiliate NGOs around the world). [83] [84]

8.5.10 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).[85] 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.[86] 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 Federal Republic of Germany[87]

---

82 Decree on Regulated Exemption, July 6, 1993.

83 The awards were granted to: the Health Institute RIVM for archiving over one million blood samples of children, without any legal basis or permission from the children's parents; the Mevis Committee for its 2001 report (above); the Organisation for Applied Scientific Research (TNO) for the development of the Automatic Aggression Detection video processing software; and to the State Secretary of Transport, Public Works and Water Management Monique de Vries for re-introducing proposals for data retention.

84 Dutch Big Brother Awards 2002.

85 Signed May 7, 1982; Ratified May 28, 1993; Entered into Force September 1, 1993.

86 Signed November 23, 2001.

87 EPIC at 182 and the references made therein.

8.6.1 The German Basic Law does not in express terms extend a general right to privacy although isolated aspects of privacy are protected in, for example, art 4 (freedom of belief), art 13 (inviolability of home), and art 10 (protection of postal communications).

8.6.2 The protection of a general right to privacy has been developed by the Federal Constitutional Court (FCC) on a case by case basis. It has been held that the constitutional obligation to respect the sphere of intimacy of individuals is based on the right to the unfettered development of personality embodied in art 2(1) of the Basic Law and in determining the context and ambit of this fundamental right, regard must be had to the inviolability of dignity in terms of art 1(1).

8.6.3 In a 1983 case against a government census law, the Federal Constitutional Court formally acknowledged an individual's "right of informational self-determination" which is limited by the "predominant public interest." The central part of the verdict stated: "Who can not certainly overlook which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be essentially hindered in his capability to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens could not know any longer who what and when in what situations knows about them."[88] This landmark court decision derived the "right of informational self-determination" directly from Articles 1(1) and 2(1) of the Basic Law, which declare the personal right (Persönlichkeitsrecht) to freedom to be inviolable.

8.6.4 Attempts to amend the Basic Law to include a right to data protection were discussed after reunification, when the Constitution was revised, and were successfully opposed by the then-conservative political majority.

8.6.5 Prior to the terrorist attacks in the United States in September 2001, Germany had the strictest data protection laws of any European Union state. [89] The world's first data protection law was passed in the German Land of Hessen in 1970. In 1977, a Federal Data Protection Law

---

88 BverfGE 65,1.

89 "Terrorism Reaches Germany Amid Warnings on Extremists," ***Deutsche Presse-Agentur***, April 17, 2002.

(BDSG) followed, which was reviewed in 1990, amended in 1994 and 1997. The general purpose of this law is “to protect the individual against violations of his personal right (Persönlichkeitsrecht) by handling person-related data.” The law covers collection, processing and use of personal data collected by public federal and state authorities (as long as there is no state regulation), and by non-public offices, if they process and use data for commercial or professional aims.

8.6.6 Germany was slow to update its law to make it consistent with the European Union Data Protection Directive. Under the terms of the directive Germany should have harmonised its law by October 1998. The European Commission announced in January 2000 that it was going to take Germany to court for failure to implement the directive. An amending bill was approved by the Government on June 14, 2000 and finally passed into law in May 2001.

8.6.7 The 2001 revisions to the BDSG include regulations on transmitting personal data abroad, video surveillance, anonymisation and pseudonymisation, smart cards, and sensitive data collection (relating to race/ethnic origin, political opinions, religious or philosophical convictions, union membership, health, and sexual orientation). It grants data subjects greater rights of objection. It also states that companies must now appoint a data protection officer if they collect, process, or use personal information; that databases collecting such information must be registered with Germany; and that consent from the individual whose data is collected is required after full disclosure of data collection and its consequences. [90]

8.6.8 In an effort to improve investigative measures to target sexual abuse of children, the German Bundesrat approved a proposal in May 2002 to make the current maximum allowed time for data retention the new minimum required time, effectively permitting limitless data retention.

8.6.9 The Federal Data Protection Commission (Bundesbeauftragte für den Datenschutz) is responsible for supervision of the Data Protection Act.[91] Its chief duties include receiving and investigating complaints, as well as submitting recommendations to Parliament and other

---

90 According to the Data Protection Commission, secondary legislation will need to be introduced on the auditing requirements and a more general revision of German data protection law may be outlined by the end of 2002.

91 Home Page <http://www.bfd.bund.de/>.

governmental bodies.[92]

8.6.10 All of the 16 Länder have their own specific data protection regulations that cover the public sector of the Länder administrations. [93] Each Land also has a commission to enforce the Länder data protection acts. Supervision, however, is carried out for the private sector by the Land authority designated by the Land data protection law (usually the Land Data Protection Commissioner).

8.6.11 Wherever they deal with the handling of personal information on natural persons, either directly or by amendments, nearly all German laws contain references to the respective data protection law or carry special sections on the handling of personal data that reflect the right to privacy.

8.6.12 Germany 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 later signed an Additional Protocol to this convention.[95] It has also signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms. In November 2002 Germany signed the Convention on Cybercrime[96]. 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.

---

92 In 2001 there were between 10,000 and 20,000 data controllers registered by the agency. Fax from Ulrich Dammann, Bundesbeauftragte für den Datenschutz, to Sarah Andrews, Research Director, the Electronic Privacy Information Center, July 27, 2000 (on file with the Electronic Privacy Information Center). However, the number of controllers is steadily decreasing as federal agencies, in compliance with the 2001 changes to the Act, appoint in-house data protection officers office,(as an alternative to registration under the Act).E-mail from Helmut Heil, Federal Data Protection Commission, to Marcia Hoffman, IPIOP Clerk, the Electronic Privacy Information Center, June 7, 2002 (on file with the Electronic Privacy Information Center). The Commission, which has 70 persons on staff, handles about 4,500 written and oral complaints and carries out around 45 investigations each year.Id.

93 Thirteen of the Länder (Brandenburg, Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, Schleswig-Holstein)Schleswig-Holstein, Berlin, Hamburg, Niederschsen, Saarland, Sachsen-Anhalt, Thüringen, and Mecklenburg-Vorpommern 786) have adopted new data protection laws pursuant to the European Union Directive.

94 Council of Europe, Legal Affairs, Treaty Office.

95 Council of Europe, Additional Protocol to the Convention For the Protection of Individuals With Regard to the Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows.

96 Signed November 23, 2001.

8.7 Canada[97]

8.7.1 The Canadian Charter of Rights and Freedoms does not specifically provide for the protection of personal privacy.[98] 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.[99]

8.7.2 Privacy is regulated at both the federal and provincial level. At the federal level, privacy is protected by two acts:

d) the 1982 federal Privacy Act; and
e) the 2001 Personal Information and Electronic Documents Act (PIPEDA).

8.7.3 The federal Privacy Act of 1982 regulates the confidentiality, collection, correction, disclosure, retention and use of personal information held by the federal sector. It provides individuals with a right to access and to correct personal information held by federal government organisations, subject to some exceptions.[100] 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.[101] 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.[102]

---

97 EPIC at 133 and the references made therein.

98 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).

99 ***Hunter v Southam***, 2 S.C.R. 145, 159-60 (1984).

100 Privacy Act, c. P-21.

101 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.

102 Privacy and Data Sharing Report fn 2 at 20.

8.7.4 In April 2000 the Personal Information Protection and Electronic Documents Act (PIPEDA) was approved by Parliament.[103] 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 Part 1 of the PIPEDA establishes the parameters 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.

8.7.6 Part 2 deals with the use of electronic transactions and documents to facilitate electronic commerce and electronic communication within judicial proceedings.

8.7.7 PIPEDA has a tiered implementation schedule:

a) In January 2001 the law took effect for personal information, excluding health information, held by federally regulated private sector entities, such as telecommunications and broadcasting businesses, banks and airlines, or businesses and organisations that disclose personal information across provincial or national borders. Health information was excluded for one year as a last minute concession to a powerful health sector lobby.

b) As of January 1, 2002, personal health information processed by the organisations outlined above is covered by the Act.

c) In January 2004, the Act will finally extend to every organisation that collects, uses, or discloses personal information in the course of a commercial activity, whether or not the organisation is federally regulated. It will cover all commercial activity in provincially regulated sectors unless the province enacts "substantially similar" laws, such as those of Québec.

---

103 Bill C-6, Personal Information Protection and Electronic Documents Act.

8.7.8 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 data transferred from the European Union to Canada.[104] This will allow certain personal data 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.

8.7.9 However, the Commission's decision of adequacy does not cover any personal data 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.[105] 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 data.

8.7.10 Both the Privacy Act and PIPEDA are overseen by the independent Privacy Commissioner of Canada who has the power to investigate, mediate, and make recommendations, but cannot issue orders or impose penalties. He also conducts periodic audits of federal institutions to determine compliance with the Privacy Act, and to recommend changes where necessary.[106]

8.7.11 The Commissioner's powers under PIPEDA [107]are very similar to those under the Privacy Act.

8.7.12 The Privacy Commissioner of Canada has been very active in a number of high profile

---

104 European Union Article 29 Data Protection Working Group, Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, January 26, 2001.

105 Commission Decision of December 20, 2001, Official Journal of the European Communities L 2/13.

106 Between April 1, 2000, and March 31, 2001, the office received a total of 1,713 complaints under the Privacy Act, an almost ten percent increase from the previous year. 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. Id. Since November 2001, the office has received more than 8,047 requests for information concerning the Privacy Act.

107 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 Email 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. Privacy Commissioner of Canada Annual Report to Parliament 2000-2001, ***Part Two–Report on the Personal Information Protection and Electronic Documents Act***, December 2001. The Commissioner's office completed and issued findings and recommendations on 27 complaints.

cases.[108] Under PIPEDA the Commissioner has investigated:

a) Air Canada for sharing its customers' personal and financial information with its partners.[109]

b) U.S-based international marketing firm that was disclosing personal information by gathering and selling data on physicians' prescribing patterns.[110]

c) A Canadian bank's refusal to grant a customer's request for access to their credit score.[111]

8.7.13 Miscellaneous statutes also contain a range of other privacy-related measures.[112] Most provinces also have some form of legislation protecting consumer credit information.

8.7.14 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

---

108 For example under the Privacy Act he has investigated:
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 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.

109 Letter from Privacy Commissioner George Radwanski to Air Canada, July 18, 2001.

110 Federal Privacy Commissioner George Radwanski Findings-September 21, 2001.

111 Office of the Privacy Commissioner, News Release, February 27, 2002.

112 The Bank Act , Insurance Companies Act, and Trust and Loan Companies Act 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." There are sectoral laws for pensions, video surveillance, immigration, and Social Security. The Young Offenders Act regulates the information that can be disclosed about offenders under the age of 18 while the Corrections and Conditional Release Act speaks to the information that can be disclosed to victims and their families.

Act of 1982. [113] 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.[114]

8.8 Commonwealth of Australia[115]

8.8.1 Neither the Australian Federal Constitution[116] 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 so far challenged. 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,[117] 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 Privacy Act, 1988 (Commonwealth)[118] is the primary domestic legislation on information

---

113 Perrin S et al.

114 Council of Europe. Cybercrime Convention.

115 EPIC at 102 and the references made therein.

116 The Commonwealth of Australia Constitution Act.

117 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. See further New Zealand Law Commission “Protecting Personal Information from Disclosure” Preliminary Paper 49 Wellington Feb 2002 at 10.

118 Privacy Act 1988 (Cth).

privacy protection in Australia.

8.8.5 Areas of coverage:

a) It creates a set of 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, applies to all private and public sector organisations.

c) The third area of coverage is the use of the government issued Tax File Number (TFN), where 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.[119]

8.8.7 The Privacy Act was recently extended by the Privacy Amendment (Private Sector) Act 2000(Commonwealth) to cover private sector organisations.

8.8.8 The amended Act began operating in December 2001. The law puts in place 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. 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 widely criticised as failing to meet international standards of privacy protection. [120]

8.8.9 The NPPs impose a lower standard of protection in several areas than the European Union

---

119 The Data-matching program (Assistance and Tax) Act 1990.

120 See Roger Clarke's Homepage <http://www.anu.edu.au/people/Roger.Clarke/>.

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).

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 In March 2001 the Article 29 Data Protecting Working Party of the European Commission expressed many reservations about the Act, suggesting that it would not, as currently written, satisfy the adequacy test in Articles 25 and 26 of the European Union directive for data to flow to third countries.[121] The group recommended the introduction of additional safeguards to address these concerns.

---

121 European Union Article 29 Data Protection Working Group, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000.

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." [122]

8.8.13 The Office of Privacy Commissioner,[123] [124] which enforces 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. [125]

---

122 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.

123 Homepage <http://www.privacy.gov.au/>.

124 In the period of 2000-2001, the Commissioners Office received 8177 telephone and 884 email inquiries. Of the 8177 calls, 46 percent (3831) related to matters falling within the Commissioner's jurisdiction. Of these 3831 calls, 1353 (35 percent) related to credit reporting; 896 (23 percent) to information handling practices under the Information Privacy Principles (IPPs); 112 (2.9 percent) to Tax File Numbers 157; 96 (2.5 percent) to spent convictions, 19(0.5 percent) to data-matching. The remaining inquiries were requests for general information or publications. Some 464 written inquiries were received (under the Privacy Act a complaint alleging interference with privacy must be lodged in writing). Of these, 20 (15 percent) were declined and 270 (58.2 percent) fell outside the Commissioners jurisdiction. The remaining were formally investigated as complaints. Federal Office of the Privacy Commissioner, The Operation of the Privacy Act, Annual Report 1 July 2000 – 30 June 2001.

125 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, 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.

c) 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 Commission, "Regulators Co-Operate to Improve Privacy Compliance," Media Release, 12 March 2002.

8.8.15 The federal Privacy Commissioner is also the supervisory and complaint handling agency of Part VIIC of the Crimes Act enacted in 1989[126] and the Data-matching Program (Assistance and Tax) Act 1990.[127]

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.[128] 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 indicate overwhelming support for privacy protection. [129] The Privacy Commissioner says that the results of the survey will be used in setting out a future work plan for the office including informing the marketing and communications strategy, and providing information for other areas of responsibility such as the development of industry codes and guidelines.

8.8.18 Public sector privacy issues continue to raise concerns. An example is the reform to the Australian tax system.[130] At the same time, the Government was forced into another backdown after

---

126 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).

127 That provides detailed procedural controls over the operation of a major program of information matching between federal tax and benefit agencies.

128 Office of the Federal Privacy Commissioner ***The Results of Research into Community, Business and Government attitudes towards Privacy in Australia*** July 31 2001.

129 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.***

130 As part of reforms to the Australian tax system from July 2000, the Australian Taxation Office required all enterprises to obtain an Australian Business Number. The ATO collected registration details including address and email contact, and planned to make this available to the public through the Australian Business Register and through selling it to database companies. A storm of protest occurred in June 2000 when it was realised that the register would include the home address and other details of almost 2 million individuals, who were sole traders, contractors or even had just a minor income from a hobby or some other activity. The Government agreed to amend the legislation, limit the content of the Australian Business Register and allow individuals to suppress their details.

receiving legal advice that the Australian Electoral Commission had illegally disclosed information on around 10 million registered Australian voters, after the Prime Minister had asked for this information in order to conduct a targeted direct mailing campaign outlining the benefits of the tax reform package.

8.8.19 All of the Australian States and Territories, with the exception of the Northern Territory, also have freedom of information laws.

8.9 Kingdom of Sweden[131]

8.9.1 Sweden's Constitution, which consists of several different legal documents, contains several provisions that are relevant to data protection:

a) Section 2 of the Instrument of Government Act of 1974[132] provides for the protection of individual privacy.

b) Section 13 of Chapter 2 of the same instrument states also that freedom of expression and information – which are constitutionally protected pursuant to the Freedom of the Press Act of 1949[133] – can be limited with respect to the "sanctity of private life."

c) Moreover, Section 3 of the same chapter provides for a right to protection of personal integrity in relation to automatic data processing. The same article also prohibits non-consensual registration of persons purely on the basis of their political opinion.

8.9.2 The European Convention on Human Rights has been incorporated into Swedish law in 1994. The ECHR is not formally part of the Swedish Constitution but has, in effect, similar status.

8.9.3 Sweden enacted the Personal Data Act (PDA) of 1998 to bring Swedish law into conformity with the requirements of the EU Directive on data protection.[134] The PDA essentially adopts the

---

131 EPIC at 342 and the references made therein.

132 Regeringsformen, SFS 1974:152.

133 Tryckfrihetsförordningen, SFS 1949:105.

134 Personuppgiftslagen, SFS 1998:204

European Union Data Protection Directive into Swedish law. It regulates the establishment and use, in both public and private sectors, of automated data files on physical/natural persons. The Act replaced the Data Act of 1973, which was the first comprehensive national act on privacy in the world.[135] [136]

8.9.4 Section 33 of the Act was amended in 1999 to adopt the European Union Directive standards on the transfer of personal data to a third country. According to the Data Inspection Board, the amendment will facilitate transfer of data through international communication networks, such as the Internet.[137]

8.9.5 The Data Inspection Board (Datainspektionen) is an independent board that oversees the enforcement of the Data Act. [138] One of their most publicised cases was against SABRE, the airline reservation system, for transferring medical information of passengers without adequate controls.[139]

8.9.6 The Act provides liberal exemptions for freedom of expression. It specifically states that in the case of a conflict the existing protections for freedom of the press (Freedom of the Press Act 1949) and freedom of speech (Freedom of Speech Act) will prevail.[140] The DIB has also proposed

---

135 Datalagen, SFS 1973:289.

136 The 1973 Act continued to apply until October 2001 with respect to processing of personal data initiated prior to October 24, 1998. An extended transition period, up to 2007, is allowed for pre-existing manual files.

137 Depending on the other circumstances, there may be situations where a third country - despite not having any data protection rules at all - still can be considered having an adequate level of protection. It is also possible that the level of protection in a third country may be assessed as adequate in some areas but not in others. The amendment entered into force in January 2000.

138 In 2001, the board received 341 complaints. 69 of these were related to the previous Act, which was still in force transitionally until October 1, 2001. The remaining 272 complaints were processed under the new Act. The Board received 475 inquiries relating to the PDA which required in depth examination. The Board also answered 15, 000 telephone inquiries and 2,500 emails. There are 2016 notified processing operations registered with the Board. 4726 controllers have personal data representatives and as such are exempted from the notification requirements. Email from Elisabeth Walinn, Data Inspection Board, to Sarah Andrews, Electronic Privacy Information Center, June 20, 2002 (on file with the Electronic Privacy Information Center). As of August 2000, the Board had 39 employees.

139 The Supreme Administrative Court recently declined to hear the case following decisions by lower courts upholding the Board's ruling.

140 In July 2001, the Swedish Supreme Court ruled that the operator of a web site dedicated to the criticism of a number of Swedish banks and bank officials did not violate data protection act as he was protected by the free expression exemptions. The Supreme Court thereby reversed the decision of the court of appeals that had imposed criminal fines on the web site operator for permitting the transfer of personal information outside the country without the approval of the Data Inspection Board (DIB). "Web Publication of Defamatory Text Shielded by Swedish Privacy Law's News Media Clause," by Stephen Joyce, BNA Daily Report for Executives, July 24, 2001. A number of other cases on the freedom of expression exemptions have been decided by the DIB itself, often in favour of the speaker. For a review of these cases

an amendment to the Act to cover "harmless data."[141]

8.9.7 There are a number of so called 'register laws' in Sweden which supplement the PDA rules on files containing personal data.[142] In 2001 additional laws were adopted to cover the processing of personal data for taxation purposes and social services. A bill to amend the Credit Reporting Act and bring it into[143] line with the European Union Data Directive and the Swedish PDA was approved by the Finance Committee in April, 2001.[144]

8.9.8 National identification numbers have been in use in Sweden for years. During the 1990s the 1973 Data Act was amended to introduce restrictions on their use. These restrictions were reproduced in the new PDA. Under section 22 of this Act information about personal identity numbers or classification numbers may only be processed without consent, if the processing is clearly justified having regard to the purpose of the processing, the importance of secure identification, or some other substantial reason.[145]

8.9.9 In 1999 the Swedish government established a Committee to study workplace privacy issues. The Committee is chaired by former Justice Minister Reidunn Lauren and includes a member of the Data Inspection Board. In March 2002 the Committee issued a proposal recommending specific legislation to protect the personal information of current employees, former employees and employment applicants in both the private and public sectors. According to the Committee Chair a bill will likely not be introduced on this issue until Spring 2003. [146]

---

see, Peter Blume et al, Nordic Data Protection 132-137 (DJOF Publishing 2001).

141 KlosekJ ***Data Privacy in the Information Age*** 106 Quorum Books 2000.

142 Some examples include the Health Care Register Act of 1998 SFS 1998:544 , the Police Data Act of 1998 SFS 1998:622, the Land Register Act of 2000, SFS2000:224 and the Schengen Information System Act of 2000. SFS 2000:344 Other statutes with provisions relating to data protection include the Secrecy Act of 1980, Sekretesslagen, SFS 1980:100. For information on the background to the new Act, see the report, Integritet-Offentlighet- nformationsteknikIntegrity-Publicity–Information Technology, SOU 1997:39. the Credit Information Act of 1973, Kreditupplysningslag, SFS 1973:1173,. the Debt Recovery Act of 1974, Inkassolag, SFS 1974:182,. and the Administrative Procedure Act of 1986 Förvaltningslagen, SFS 1986:223.

143 E-mail from Elisabeth Walinn, supra .

144 Baker & McKenzie, Global E-Commerce, What's New, April 9, 2001.

145 Ministry of Justice Sweden ***Information on the Personal Data Act.***

146 "Sweden Concerns Over Employer Monitoring," ***BNA World Data Protection Report*** Vo 2 Issue 4 April 2002.

8.9.10 In April 1999 a new law on Police Data was introduced and specifically prohibits security police filing of individuals solely on the grounds of "ethnical background, political opinion, religious or philosophical conviction, trade union membership, health details, or sexual preferences."[147]

8.9.11 Previously, it was also discovered that the Swedish statistical agency, Statistika, was monitoring 15,000 Stockholm residents born in 1953 in intimate detail. The information included statistics on drinking habits, religious beliefs, and sexual orientation. The DIB subsequently ordered the destruction of the master tape containing the data.[148]

8.9.12 Sweden 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).[149] It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.[150] In November 2001 it signed the Council of Europe Convention Cybercrime (ETS No. 185).[151] 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.

---

147 Act on Police Data (Polisdatalag 1998: 622) section 5.

148 Madsen W ***Handbook of Personal Data Protection*** New York: Stockton Press 1992.

149 Signed January 28, 1981; Ratified September 29, 1982; Entered into Force October 1, 1985.

150 Signed November 28, 1950; Ratified February 4, 1952; Entered into Force September 3, 1953.

151 Signed November 23, 2001.

CHAPTER 9: CONCLUSION AND PROPOSALS FOR DISCUSSION

9.1 In the preceding chapters we have endeavoured to set out the various problem areas regarding privacy and data protection. As set out above, the South African Law Reform Commission is of the opinion that the position regarding the regulation of data processing in South Africa should be formalised in a Bill. The text and content of such a Bill will be the subject of the discussion paper that will follow this issue paper. Respondents will be provided with ample opportunity, after publication of the Bill for information and comment, to evaluate and discuss the various sections of the Bill in detail.

9.2 The object of this issue paper has been, however, to provide background information and to develop the basic principles that will form the basis of the forthcoming legislation. Questions in this regard have been posed throughout the document and readers are once again encouraged to provide feedback on all the different issues.

9.3 Owing to the multifaceted nature of the data industry, it seems that it would be impossible to adopt only a single generally valid statutory measure regarding the protection of data. A differentiated approach seems to be necessary, depending on the nature of the entity compiling information (for example, the state or private individuals such as employers, the insurance industry, etc), the type of personal data collected and the purpose for which it is to be used.

9.4. In terms of this approach it will be necessary to develop (ethical) codes of conduct enforced by legal sanctions for the data activities of each sector of the data industry. However, this method is likely to be cumbersome and too extensive,[1] and may also prove to be too rigid.

9.5 Consequently, a more flexible approach seems to be required through which general principles for the protection of data may be developed.[2] See the discussion of the data protection

---

1 Cf eg the extensive provisions of the American Fair Credit Reporting Act 15 U.S.C. 1681(1970) which applies only to credit bureaux and similar institutions; cf also Klopper 286 who makes recommendations on the processing of credit information in South African law.

2 Such an approach is followed in the English Data Protection Act.

principles in Chapter 6. [3] These principles may then be applied *mutatis mutandis* to every segment of the data industry.[4]

9.6 It is submitted that effective data protection, based on general principles, can be achieved only through a two-pronged approach: the protection of personal information held by government on the one hand and private bodies on the other.

9.7 A very important question to be answered is whether the proposed privacy legislation should make provision for a statutory regulatory authority, and if so, what form this authority should take. See the discussion in Chapter 7 in this regard.

9.8 The preliminary proposals of the Commission can be summarised as follows:

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.

The Commission is seeking feedback regarding all these proposals. Comments will be appreciated and taken into account in drafting the Data Privacy Bill.

9.9 In conclusion it should be noted that , should these proposals be adopted, the protection of data privacy in South Africa will be brought into line with international requirements and developments.

---

3 See generally Neethling ***Privaatheid*** at 358; 1980 ***THRHR*** at 146.

4 The creation of general principles for the protection of data obviously does not prevent bodies which represent data media (such as the Institute for Chartered Accountants or the board dealing with the use of computers) from working out, in due time, detailed codes of conduct for their members in order to ensure that they adhere to the general principles of data protection.

SUMMARY OF PROPOSALS AND QUESTIONNAIRE

Privacy is a valuable aspect of personality. Data 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 data 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 data available to nearly anyone at a price.

The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. The question could no longer be whether information could 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 data protection statutes at national or federal level and the number of such countries is steadily growing. The investigation into the possible development of data 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 data 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 data 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 data 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 the 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.

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" (the so-called safe-harbour principles).

Privacy is therefore an important trade issue, as data 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" data protection by international standards.

The effectiveness of data protection provisions in protecting an individual's personality rights will, however, depend largely on how they are applied and interpreted in practice. In this regard it has been argued that the rules for data protection come from three distinct perspectives, namely political, economic and technological:

a) In Europe, data 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 protections for consumers. Data protection is a question of economic power rather than political right.
c) Across these two policy models of data protection, technological rules and defaults define information practices for network interactions.

Four models aimed at the protection of personal information can be identified. Depending on their application, these models can be complementary or contradictory. In most countries several are used simultaneously.

First of all, 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 data protecting laws and was adopted by the European Union to ensure compliance with its data protection regime.

Secondly, some countries have avoided enacting general data 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. There is also the problem of a lack of an oversight agency.

Thirdly, data protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. This is currently the policy promoted by the governments of the United States and Singapore.

Finally, with the recent development of commercially available technology-based systems, data protection has also moved into the hands of individual users. It is possible to employ a range of programs and systems that provide varying degrees of privacy and security of communications.

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. On the other hand, business interests may be enhanced by a statutory data protection regime. Many countries, especially in Asia, have developed or are currently developing data protection laws in an effort to promote electronic commerce. These countries recognise that consumers are uneasy with the increased availability of their personal data, particularly with new means of identification and forms of transactions, and therefore that their personal information is being utilised worldwide. Data 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.

It should be noted that the promulgation of data 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 and the Electronic Communications and Transactions Act 25 of 2002. Both these Acts contain interim provisions regarding data protection in South Africa.

The preliminary proposals of the Commission can be summarised as follows:

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.

The Commission is seeking feedback regarding all these proposals. Comments will be appreciated and taken into account in drafting the Data Privacy Bill.

Questionnaire:

In order to facilitate discussion, various questions have been posed throughout the document and readers are encouraged to provide feedback on all these different issues. Please note that readers do not have to limit their comments to these issues. For ease of reference a list of the questions are repeated here:

1) What should the scope of this inquiry be? Should the investigation include:

   a) automatic and manual files?
   b) information pertaining to both natural and juristic persons?
   c) information kept by both the public and the private sector?
   d) sound and image data?.
   e) critical data?
   f) personal information kept in the course of a purely personal or household activity? [Para 1.3.12]

2) What are the duties of the legislature insofar as the protection of privacy in general and informational privacy in particular are concerned? [Para 3.4.4]

3) What is the relationship between the Constitution and the common law of privacy? Does the Constitution's conception of privacy differ from that of the common law?[Para 3.4.4]

4) Should a distinction be drawn between the public and the private sector in drafting privacy legislation and if so, what should these differences be. [Para 4.1.4]

5) Do you think that existing legal remedies provide adequate protection to consumers against the collection and sharing of information by credit bureaux that may be misleading or incorrect? What are the views of the credit bureaux regarding the principles to be embodied in the proposed legislation? [Para 4.3.14]

6) The Commission is interested in the views of both consumers and marketing agencies regarding direct marketing practices. Does practice indeed match theory? [Para 4.3.22]

7) Do patients feel comfortable in providing personal medical information to physicians, hospitals and medical aid schemes? The Commission invites comment from health authorities with regard to the following areas:

   * genetic engineering
   * special considerations about the needs of minors;

* information provided to spouses, dependants, and other next of kin;
* public health reporting;
* fraud and abuse investigations. [Para 5.7.20]

8) Is there a need for statutory regulation in so far as financial privacy is concerned? If so, what should the nature of such regulation be ? [Para 4.3.52]

9) The Commission has noted that in-depth studies dealing specifically with privacy in the workplace are currently being conducted worldwide. Is there a need for such research in South Africa? [Para 4.3.61]

10) How should a proposed Privacy Act interact with existing legislation dealing with privacy issues for example the Promotion of Access to Information Act, the Electronic Communications and the Transactions Act and the Financial Centre Act? [Para 5.2.17]

11) Does the opt-out approach constitute a valid consent of the consumer? If so, why? If not, why not? What are the implications for consumers and industry if opt-out consent is allowed? [Para 5.4.23]

12) Should institutions be allowed to share data, and if so, under what circumstances. What should the consent requirements be in this regard? In sharing data, who is responsible for the accuracy and maintenance of the data? [Para 5.5.15]

13) What are the perceptions of the public regarding
    a) the current information collection practices of government?
    a) the accuracy and maintenance of information held by government?
    b) the benefits on the one hand and risks on the other to be derived from integrated data sharing in government. Do people recognise the available safeguards and trust them ? [Para 5.5.28]

14) Do readers see data profiling as a natural element of marketing practice or is it an unacceptable infringement of the individual's privacy. What should the consent requirements be? [Para 5.6.10]

15) Have security issues been dealt with adequately in the ECT Act or should additional provision be made for the security protection of personal data in accordance with the principles of data protection? Comment is furthermore welcomed regarding practical issues surrounding identity theft, a practice which seems to have become a major problem for

financial institutions and their customers. [Para 5.8.30]

16) Should all the so-called principles of data protection be incorporated in a Data Privacy Act? If so, how? The principles are:

Principle 1: Fair and lawful processing
Principle 2: Openness
Principle 3: Collection Limitation
Principle 4: Use/Purpose Specification
Principle 5: Disclosure Limitation
Principle 6: Individual participation
Principle 7: Data Quality
Principle 8: Finality
Principle 9: Security Safeguards
Principle 10: Accountability
Principle 11: Sensitivity

[Para 6.2.125]

17) Should South African privacy legislation make provision for a statutory regulatory authority? What should the level of this authority be? Where should it be housed? [Para 7.2.35]

18) Would it adversely affect the country's international trade if a model is adopted that is not regarded as "adequate" in terms of Article 25 of the EU Directive? If so, how? [Para 5.3.9]

The Commission invites comment on all these issues. Respondents who prefer to direct their comments at selected questions only, are welcome to do so.