

CHAPTER 5: MONITORING AND SUPERVISION

5.1 Introduction

5.1.1 An essential aspect of any privacy protection regime is oversight. The effectiveness of information protection provisions in protecting an individual's personality rights will depend largely on how they are applied and interpreted in practice.¹

5.1.2 It has been argued² that the rules for information protection come from three distinct perspectives, namely political, economic and technological:

- a) In Europe, information protection is an inherently political right and focuses on legal mechanisms to guarantee respect for a fundamental human right to privacy.
- b) By contrast, in the United States, information privacy is left to the marketplace and the desire to have market-based protection for consumers. Information protection is a question of economic power rather than political right.
- c) Across these two policy models of information protection, technological rules and defaults define information practices for network interactions.

5.1.3 The rules found in information protection laws furthermore usually belong to two main categories:³

- b) rules concerned directly with regulating the processing of personal information (so-called Information Protection Principles)⁴; and
- c) rules concerned primarily with monitoring and enforcing the first set of rules.⁵

¹ Roos 1998 *THRHR* at 505 in referring to the data protection provisions as they were then in the Open Democracy Bill.

² Reidenberg J "Technologies for Privacy Protection" Presentation delivered at the 23rd International Conference of Data Protection Commissioners, Paris Sept 2001(hereafter referred to as "Reidenberg presentation 2001") at 2 and the references made therein.

³ Bygrave *Data Protection* at 84.

⁴ See discussion of Data Protection Principles in Chapter 4.

⁵ The subject of discussion in this chapter.

5.1.4 The first category of rules can in turn be sub-divided into two main sub-categories:

- a) Rules regulating the manner and purposes of information processing. These rules ensure that the processing of information occurs with the participation of the data subject. Information processing should therefore be authorised, publicised and rectifiable.
- b) Rules relating to the quality of personal information.

5.1.5 The second main category of rules can also be broken down into two main sub-categories:

- a) Rules that facilitate monitoring and enforcement functions (supervision).
- b) Rules directly concerned with monitoring and enforcement functions (enforcement).

5.1.6 Four models, embodying the abovementioned rules for privacy protection, were identified in Issue Paper 24:⁶

- c) Comprehensive laws

In many countries around the world, there is a general law that governs the collection, use and dissemination of personal information by both the public and private sectors. The overwhelming majority of countries with information protection laws also have established special authorities (information protection authorities) to oversee specifically the implementation of these laws.⁷ A variation of these laws, described as a co-regulatory model, was adopted in Australia. Under this approach there is a comprehensive law, but industry may develop rules for the

⁶ EPIC and Privacy International *Privacy and Human Rights Report* 2002 at 3.

⁷ In most cases the authorities are empowered to issue legally binding orders. In some jurisdictions, however, the authorities either do not have such a competence at all, or they do not have it in relation to certain sectors. There is evidence to suggest that the recommendations of an Ombudsman can sometimes be equally as effective as orders. See Bygrave *Data Protection* fn 277 and the references made therein. Notable exceptions are the USA and Japan. Repeated attempts to set up a data protection authority at the federal level in the USA have stranded largely on account of America's deep-seated antipathy to regulation by governmental agencies. See Bygrave *Data Protection* at 70.

protection of privacy that are enforced by the industry and overseen by the privacy oversight agency.⁸

d) Sectoral laws

Some countries, such as the United States, have avoided enacting general information protection rules for the private sector in favour of specific sectoral laws governing for eg credit reporting, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. With this approach new legislation has to be introduced with each new technology - so protections frequently lag behind. The lack of legal protections for individual privacy on the Internet in the USA is a striking example of its limitations. There is also the problem of a lack of an oversight agency. In some countries, sectoral laws are, however, used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.⁹

e) Various forms of self-regulation

Information protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of conduct and engage in self-policing. However, in many countries, especially the United States, these efforts have been disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries provide only weak protections and lack enforcement. This is currently one of the policies promoted by the governments of the United States and Singapore.¹⁰

f) Technologies of privacy

With the recent development of commercially available technology-based systems,

⁸ EPIC and Privacy International *Privacy and Human Rights Report* 2002 at 4.

⁹ EPIC and Privacy International *Privacy and Human Rights Report* 2002 at 4.

¹⁰ EPIC and Privacy International *Privacy and Human Rights Report* 2002 at 4.

privacy protection has also moved into the hands of individual users. Users of the Internet and of some physical applications can employ a range of programs and systems that provide varying degrees of privacy and security of communications.¹¹ These include encryption, anonymous remailers, proxy servers and digital cash.¹² While technology has made our personal lives more transparent, privacy and technology are therefore not inherently antagonistic.¹³ Technology by itself is neither a privacy enhancer nor a privacy threat. This is to be determined by its uses.¹⁴ Technology will become a privacy enhancer if appropriate awareness, education, management processes/business models are developed.¹⁵ Some argue that new technologies may prove to be one of the most potent forces driving the right to informational self-determination.¹⁶

¹¹ Privacy Enhancing Technologies (PETs) have been defined with reference to the definition of Herbert Burkert in fn 288 in Froomkin AM "The Death of Privacy" *Stanford Law Review* Vol 52:1461 May 2000 (hereafter referred to as "Froomkin 2000 *Stanford Law Review*") at 1529 as technical devices organisationally embedded in order to protect personal identity by minimising or eliminating the collection of data that would identify an individual or a legal person. In addition to PETs embedded in organisations there are also a number of closely related technologies that people can use for self-help, especially when confronted by organisations that are not privacy friendly. One such device is the Platform for Privacy Preferences (P3P) which seeks to reduce the transaction cost of determining how much personal data should be surrendered in a given transaction. The P3P project provides a standard way for web sites to communicate about their data practices. Developed by the World Wide Web Consortium (W3C) P3P specification includes a standard vocabulary for describing a website's data practices, a set of base data elements that web sites can refer to in their privacy policies and a protocol requesting and transmitting website privacy policies. P3P enabled web sites make information available on how sites handle personal information about its users. P3P enabled browsers can then "read" this information automatically and compare it to the consumer's own set of privacy preferences; Froomkin 2000 *Stanford Law Review* at 1529.

¹² EPIC maintains a list of privacy tools at <http://www.epic.org/privacy/tools.htm>.

¹³ Valeri L "Is Technology a Privacy-enhancer or Privacy Threat? Some Thoughts" Presentation delivered at the 24th International Conference on Data Protection and Privacy Commissioners held in Cardiff on 9-11 Sept 2002 (hereafter referred to as "Valeri presentation 2001"). Technology has already alleviated many everyday intrusions: airport x-ray units have made hand searchers of luggage rare. Magnetic markers in books and clothing makes searches unnecessary. Encryption software make computer files infinitely more secure than paper documents in locked cabinets.

¹⁴ Valeri presentation 2001 at 8.

¹⁵ Technology solutions:

- privacy enhancing technologies
- anonymous and pseudonymous browsing, email, remailing systems
- platform for Privacy Preferences or P3P
- privacy policy generators
- smart cards/public key infrastructures
- biometric solutions readers, software etc
- cookie managers.

¹⁶ Piller *Macworld* at 7; Mark Heyink, in his submission to the Commission stressed that It is, however, increasingly clear that questions of information security, often thought to be the domain of the technologists and technologies that they create, have proved to be far more dependent on people and processes than on the technologies which support the processes. While the role of privacy enhancing technologies may be important in the future, it is likely that these privacy enhancing technologies will be driven by issues of compliance with legislation rather than the interests of markets to build technologies with this capacity. Further, it is unlikely in the foreseeable future, that privacy enhancing technologies implemented without also addressing human behaviour and establishing processes within which the technologies would be used, would work.

5.1.7 It was noted in the Issue Paper that, depending on their application, these models/instruments could be complementary or contradictory. In most countries several are used simultaneously. In the countries that protect privacy most effectively, all the instruments are used together to ensure privacy protection.¹⁷

5.1.8 This fact was confirmed in collating the responses to Issue Paper 24. It became clear that the different options to be evaluated in drafting privacy legislation for South Africa did not so much turn on the specific models or instruments used, but rather on the degree of regulation involved in each case. Three enforcement systems were identified through which the privacy principles could be implemented. These systems included all of the abovementioned models/instruments or parts thereof.¹⁸ They were identified as regulatory, self-regulatory and co-regulatory systems.

5.2 Enforcement systems

5.2.1 As indicated above, respondents were divided in their comments regarding the system to be chosen. Each option will therefore be discussed in this section (para 5.2) with the comments it elicited in each case discussed in para 5.3 below.

a) Regulatory system (eg. UK, New Zealand, the Netherlands, Canada)

Comprehensive law

5.2.2 A regulatory system makes provision for a comprehensive Act setting out the Principles

¹⁷ Bennett *Government Foundation Paper* 2001 at 28; Bennett CJ "The Data Protection Authority: Regulator, Ombudsman, Regulator or Campaigner?" Presentation delivered at 24th International Conference of Data Protection Commissioners, Cardiff, September 9-11, 2002 (hereafter referred to as "Bennett presentation 2002") further note that the data protection statute is just one influence on the behaviour of the data protection authority. The data protection authority is furthermore just one policy instrument in the 'privacy toolbox', others are self-regulatory instruments, privacy enhancing technologies and international instruments; See also Bennett CJ and Raab CD *The Governance of Privacy - Policy Instruments in Global Perspective* Ashgate Publishing Aldershot 2003 (reprinted in 2004) (hereafter referred to as "Bennett and Raab *The Governance of Privacy*") at 165.

¹⁸ It is interesting to note that there has been a continuing process of convergence and harmonisation of ideas to the extent that one can now speak of a global approach to privacy protection. At the same time the range of possible policy instruments has expanded.

of Information Protection¹⁹ as well as provisions dealing with the monitoring and enforcement of these principles.

Sectoral laws

5.2.3 As stated above the regulatory system may also include sectoral laws. These specific laws may precede the national adoption of general information protection legislation or may be passed after general legislation comes into force. Examples of countries with both general and sectoral laws are The Netherlands, Belgium, Germany, Austria, Finland, Norway, Sweden and Denmark. Taken together these laws cover a wide range of information-processing fields, including the census, public service “one stop shops”, public order, telecommunications, video surveillance, sensitive information registers, credit cards, public archives, the media, information matching in the field of taxation, genetic information and the collection of personal information for payroll wage-deduction.²⁰

5.2.4 It is important to note, though, that as with comprehensive statutes, their oversight and implementation will remain the key to their effectiveness.²¹

Oversight agencies

5.2.5 As seen above, most countries with an omnibus information protection or privacy act, have an official or agency that oversees enforcement of the act.²² The powers of these officials - Commissioner, Ombudsman or Registrar - vary widely by country. A number of countries, including Germany and Canada, also have officials or offices on a state or provincial level.

¹⁹ See Chapter 4 above.

²⁰ Bennett and Raab *The Governance of Privacy* at 106.

²¹ Ibid.

²² Bennett and Raab *The Governance of Privacy* at 108 refer to countries in OECD countries with Data Protection Supervisory Authorities: Office of the Federal Privacy Commissioner, Australia; Buro der Datenschutzkommission, Austria; Commissie Voor De Bescherming van de Persoonlijke Levenssfeer, Belgium; Privacy Commissioner of Canada; Office of Personal Data Protection, Czech Republic; Datatilsynet, Denmark; Der Bundesbeauftragte für den Datenschutz, Germany; Hellenic Data Protection Authority, Greece; Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary; Personuvernd, Iceland; Data Protection Commissioner, Ireland; Garante per la Protezione dei dati Personali, Italy; Commission a la Protection des Donnees Nominatives, Luxembourg; College Bescherming Persoonsgegevens, Netherlands; Privacy Commissioner, New Zealand; Datatilsynet, Norway; Bureau of the Inspector General for the Protection of Personal Data, Poland; Comissao Nacional de Protecao de Dados, Portugal; Commissioner for the Protection of Personal Data, Slovak Republic; Agencia de Proteccion de Datos, Spain; Data Inspection Board, Sweden; Federal Data Protection Commissioner, Switzerland; Information Commissioner, United Kingdom. OECD countries without supervisory authorities are Japan, Korea, Mexico, Turkey and the United States.

5.2.6 The most detailed treatment of the competence and functions of information protection authorities is found in the EU Directive. Art 28(1) states that each EU Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Members States pursuant to the Directive.²³

5.2.7 In contrast to the EU Directive, the OECD Guidelines have little to say about the need for, and competence of, national information protection authorities. Indeed, they do not require such authorities to be established. A similar situation has pertained up until recently with the CoE Convention. However, an additional Protocol to the Convention was adopted on 23 May 2001²⁴ by the CoE Committee of Ministers replicating in Art 1 the basic thrust of Art 28 of the Directive.²⁵

5.2.8 The UN Guidelines specifically address the need to establish national data protection authorities that are “impartial”, “independent” and “technically competent”.²⁶

5.2.9 The Commonwealth guidelines make provision for the establishment of an independent Privacy Commission, but on an optional basis. It recognises that small and developing countries may not be able to create such an office and may need to rely on courts or tribunals only to deal with allegations of damage caused by breach of the privacy law.^{27,28}

²³ Bygrave *Data Protection* at 71; Art 28(1) of the EU Directive reads as follows:

Article 28 **Supervisory authority**

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them.

²⁴ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) regarding the supervisory authorities and trans border data flows, ETS No 179, open for signature 8.11.2001.

²⁵ Bygrave *Data Protection* at 73.

²⁶ Bygrave *Data Protection* at 73 referring to para 8.

²⁷ Commonwealth Model Law for Private Bodies at 2. In terms of this Model Law the office of Privacy Commissioner is established by the appointment of a full-time Privacy Commissioner by the President upon the recommendation of the Minister, for five years subject to such terms and conditions as may be specified in the instrument of appointment. The Commissioner shall receive and investigate a complaint from any person in respect of any matter relating to -

- a) the collection, retention or disposal of personal information by a public authority; or
- (b) the use or disclosure of personal information held by a public authority; and have the powers to carry out an investigation in this regard.

With regard to private bodies the Privacy Commissioner shall have similar powers and

Codes of conduct

5.2.10 Some Commissioners have explicit responsibilities to negotiate privacy codes of

duties. Parliament shall appropriate annually, for the use of the Privacy Commissioner, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Commissioner, of his or her powers, duties and functions under this Act.

28

The functions of the Privacy Commissioner would be -

- (a) to monitor compliance by public authorities of the provisions of this Act;
- (b) to provide advice to public authorities on their obligations under the provisions, and generally on the operation, of this Act;
- (c) to receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;
- (d) to inquire generally into any matter, including any enactment or law, or any practice, or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed thereby;
- (e) for the purpose of promoting the protection of individual privacy, to undertake educational programmes on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner;
- (f) to make public statements in relation to any matter affecting the privacy of the individual or of any class of individuals;
- (g) to receive and invite representations from members of the public on any matter affecting the privacy of the individual;
- (h) to consult and co-operate with other persons and bodies concerned with the privacy of the individual;
- (i) to make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interests of the privacy of the individual;
- (j) to undertake research into, and to monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of individuals are minimised, and to report to the Minister the results of such research and monitoring;
- (k) to examine any proposed legislation (including subordinate legislation or proposed policy of the Government that the Commissioner considers may affect the privacy of individuals, and to report to the Minister the results of that examination;
- (l) to report (with or without request) to the Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of the individual;
- (m) to report to the Minister from time to time on the desirability of the acceptance, by [name of country] of any international instrument relating to the privacy of the individual;
- (n) to gather such information as in the Commissioner's opinion will assist the Commissioner in discharging the duties and performing the functions of the Commissioner under this Act;
- (o) to do anything incidental or conducive to the performance of any of the preceding functions; and
- (p) to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

conduct. Some countries' laws make specific provision for industries, professions, etc to draw up sectoral codes of conduct/practice on information protection in co-operation with information protection authorities.²⁹ An increasing number of schemes for the development of such codes is likely, given that the EU Directive requires Member States and the Commission to "encourage" the drafting of sectoral codes of conduct at national and community level, in pursuance of the measures contemplated by the Directive.³⁰

5.2.11 Codes of conduct are primarily instruments of self-regulation and will also be discussed below in para (b) and (c), dealing with the co- and self-regulatory systems.. They do, however, also offer some clear advantages in a legislated information protection regime. The procedure of negotiating codes may enhance the understanding of the privacy problem within different sectors. Codes are flexible instruments and once negotiated can be adapted to changing economic and technological developments.³¹

5.2.12 There are three different models that have evolved in those countries that use privacy codes. The first, and in many ways most stringent, is represented by the system under the New Zealand Privacy Act.³² The crucial aspect of the New Zealand approach is that codes of practice negotiated under the Privacy Act have the force of law. A breach of a ratified code of practice is as serious as a breach of the information privacy principles expressed in the law, which would then trigger the complaints and enforcement procedures in the legislation. The second, slightly more flexible regime, exists in the Netherlands. Although the Dutch system is similar in most respects to that in New Zealand, the codes are not formally binding on the courts. If an organisation can prove that it has met the requirements of its code, it will have a strong case. Conversely, a complainant's demonstration that the provisions of the code have been breached constitutes prima facie evidence of liability under the law. Codes therefore, have indirect, rather than direct legal effect. In other countries, such as the UK and Canada, the law simply empowers the Commissioner concerned to encourage the development of codes as a further instrument of compliance with the law. Indeed, this is all that is expected by the EU

²⁹ See eg Parts VI-VII of the New Zealand Act; s 51(3)-(4) of the United Kingdom Act; Part IIIAA of the Australian Act; and Art 25 of the Netherlands' Act.

³⁰ Bygrave *Data Protection* at 74 referring to Art 27; See discussion on codes of conduct below in para 5.6 below..

³¹ Bennett and Raab *The Governance of Privacy* at 113.

³² See Part VI of the New Zealand Privacy Act.

Directive.³³

5.2.13 Where a formal ratification process is laid out, as in New Zealand and the Netherlands, this can bureaucratise a process that, in theory, is supposed to allow the flexibility of self-regulation. Submission of the codes in some sectors are, furthermore, hindered by competition within the sector, and by unclear boundaries and overlaps that weaken the claim that the association submitting the code is sufficiently “representative”.³⁴

Other agencies

5.2.14 It should also be noted that information protection authorities are not alone in monitoring, encouraging and enforcing the implementation of information protection laws. A great number of other bodies are involved to varying degrees in one or more of the same tasks, even if their participation is not always formally provided for in information protection instruments.³⁵

5.2.15 On the international plane, notable examples of relevant bodies are the expert committees on information protection and information policy formed under the umbrella of the CoE and OECD. A variety of other inter- and non-governmental organisations are also emerging to play a role in the setting of information protection standards. These include the World Trade Organisation (WTO), World Intellectual Property Organisation (WIPO) and the World Wide Web Consortium (W3C). Many of these bodies will approach information protection from a market-oriented rather than a human rights perspective.³⁶ At a national level, obvious examples of relevant bodies are those charged with hearing appeals from the decisions of information protection authorities. Other examples are parliamentary committees, ombudsmen and national auditing offices.

Independence

5.2.16 The EU Directive requires that oversight authorities must act with complete

³³ Bennett and Raab *The Governance of Privacy* at 113.

³⁴ Ibid.

³⁵ Bygrave *Data Protection* at 73.

³⁶ Bygrave *Data Protection* at 74.

independence in exercising the functions entrusted to them.³⁷ The reference to “complete independence” means that great care must be taken in ensuring that the authorities’ inevitable *administrative* dependence on other bodies (eg through budget and personnel allocations) does not undermine the functional independence they are otherwise supposed to have. It also means that administrative and legal frameworks which leave open even a small possibility of an information protection authority being instructed by another administrative body on how to exercise its functions, most probably do not satisfy the criterion of Art 28(1).³⁸ However, they are clearly not judicial bodies and usually closely linked to the Ministry of Justice. Perhaps the best way to describe them is as “independent administrative agencies”.³⁹

5.2.17 This criterion of independence boils down to the capacity for a information protection authority to arrive at its own decision in a concrete case without being given case-specific instructions by another body as to what line it should take. Yet, insofar as such a decision is legally binding, it will usually be subject to political and legal review.⁴⁰ Moreover, decision making by an authority will be steered at a more general level by laws and regulations laid down by other bodies.⁴¹

5.2.18 Many authorities are appointed in special procedures, often involving Parliament - although some are appointed by the Government (in the UK by the Queen acting on the advice of Government) or, indeed, the Minister of Justice (the Netherlands).⁴²

5.2.19 The independence of privacy and information protection regulators is therefore a complex variable that is affected as much by processes of appointment and financing, as by the formal lines of authority stipulated in law. In the UK the Information Commissioner reports to Parliament and not to a government minister, and is generally regarded as well insulated from direct political interference.⁴³

³⁷ Art 28(1).

³⁸ Bygrave *Data Protection* at 71.

³⁹ Korff *Comparative Study* at 200.

⁴⁰ Korff *Comparative Study* at 201 argues that the very existence in States under the Rule of Law, of the above-mentioned kinds of almost discretionary powers in the hands of non-judicial bodies must raise questions. At the very least, the exercise of such powers should be subject to judicial overview and indeed, in appropriate cases, to prior judicial authorisation (such as the issuing of a search warrant).

⁴¹ Bygrave *Data Protection* at 70.

⁴² Korff *Comparative Study* at 203.

⁴³ Bennett and Raab *The Governance of Privacy* at 175 and 176.

5.2.20 The Directive contains several provisions which will stimulate an internationalisation, at least within the EU, of supervisory and monitoring regimes in the field of information protection.⁴⁴ Further, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereafter referred to as “Data Protection Working Party”) has been established pursuant to Art 29. This body is mainly composed of representatives from each Member State’s data protection authority. It acts independently from the Commission and other EU organs, and has advisory competence only. Its purpose is to provide advice on issues relating to the uniform application of national measures adopted pursuant to the Directive; data protection afforded by non-Member States; possible changes to the Directive and other instruments affecting data protection; and codes of conduct drawn up at Community level.⁴⁵

5.2.21 At the 23rd International Conference of Data Protection Commissioners⁴⁶ an accreditation procedure (for recognising the credentials of data protection authorities for the purposes of the International Conference) was established.⁴⁷ The following rules were set: the information protection authority must be a public authority implemented by legal purview; the authority must have the benefit of guarantees of autonomy and independence; the authority must dispose of effective competence, it should not only have a consultative role, but must also dispose of a power of surveillance which includes legal or administrative consequences.⁴⁸

Monitoring

5.2.22 Most information protection laws lay down special rules to enhance the ability of information protection authorities to monitor the practices of responsible parties. While information protection laws expound similar core principles, there are numerous differences

⁴⁴ See Art 28(6) in this regard.

⁴⁵ Bygrave *Data Protection* at 73.

⁴⁶ Held in Paris, France 24-26 September 2001.

⁴⁷ Accredited members would have a legitimately full share in the resolutions which may be adopted.

⁴⁸ The document was prepared by the delegations from New Zealand, the United Kingdom and France who also formed the first accreditation committee in terms of the rules.

between them in terms of the monitoring and supervisory regimes they establish:⁴⁹

- a) One category requires responsible parties simply to **notify** information protection authorities of certain planned processing of personal information.⁵⁰ Upon notification, processing is usually allowed to begin.⁵¹ Most information protection laws, including the EU Directive (the other three main international information protection instruments, however, refrain from specifically laying down requirements for notification or for other control schemes) operate with this sort of requirement, though the ambit of their respective notification schemes has varied.⁵²
- b) Occasionally, the notification requirement is formalised as a system for **registration**.⁵³ Under this sort of system, responsible parties must, as a general rule, apply to be registered with the information protection authority, registration being a necessary pre-condition for their processing of personal information. Once application for registration is lodged, the controller is legally able to begin processing.⁵⁴ The UK used to be an example of the registration model.

⁴⁹ Bygrave *Data Protection* at 75.

⁵⁰ See eg sec 36 of Sweden's Personal Data Act. The notification requirement does not apply where the data controller has appointed an internal data protection officer.

⁵¹ Art 19(1) of the EU Directive stipulates the types of information to be notified to include "at least" :

- a) the identity of the data controller and his/her representative;
- b) the purposes of the data processing;
- c) the categories of data subject and data held on the latter;
the categories of recipients of the data;
- d) proposed transfers to third countries and a general description of adopted security measures for the processing.

⁵² Bygrave *Data Protection* at 75.

⁵³ Repealed ss 4-9 of the UK Act of 1984.

⁵⁴ Bygrave *Data Protection* at 75.

- c) Another category of control/oversight requires that responsible parties must apply for and receive specific authorisation (in the form of a **licence**) from the relevant information protection authority prior to establishing a personal register or engaging in a particular information-processing activity. Only a minority of information protection authorities operate, or have operated with comprehensive authorisation/licencing regimes, France being an example in so far as its public sector is concerned. It has been more common for countries to reserve a licencing requirement for certain designated sectors of business activity such as credit reporting or for overseas transfers of personal information or for the matching of information.⁵⁵

*Other functions*⁵⁶

5.2.23 Apart from monitoring the practices of responsible parties, agencies may also have other duties. Some examples are as follows:⁵⁷

- a) Governments may consult the body when the government draws up **legislation** relating to the processing of personal information; they would accordingly also take part in hearings in Parliamentary commissions.⁵⁸
- b) The bodies have the power to conduct **investigations**⁵⁹ and have a right

⁵⁵ Bygrave *Data Protection* at 76.

⁵⁶ See Art 28(2) and (5) of the EU Directive.

⁵⁷ Lopez JMF "The Data Protection Authority: The Spanish Model" Presentation at the 24th International Conference of Data Protection and Privacy Commissioners, Cardiff, Sept 9-11 2002 (hereafter referred to as "Lopez presentation 2002").

⁵⁸ Korff *Comparative Study* at 205 explains as follows: Governments and legislators often follow the authorities' advice; at the very least, their opinions ensure that the issues concerned are properly aired and debated. In several national systems, the providing of "opinions" furthermore formally or effectively becomes a part of enforcement. Thus, In France, the issuing of "favourable opinions" on the required regulations for proposed public-sector processing operations has in practice become a pre-condition. In the Netherlands a positive opinion, by the data protection authority is required before a sectoral code of conduct can play its intended role in the data protection compliance system.

⁵⁹ Such investigations can arise, in particular, out of doubts about a proposed processing operation as described in a ("full") registration form, or out of specific complaints from individual data subjects . Korff *Comparative Study* at 206. Action taken by data protection authorities on the basis of complaints from individual data subjects follows the same pattern: the authority gets in touch with the data user(responsible party) concerned, "advises" and act as a conciliator, and tries to reach an amicable solution to the dispute. In many cases, the issues are straight-forward and easily resolved on the basis of clear legal principles. For instance, a data user refusing to grant a data subject access to his or her data may need only to be "reminded" by the authority of his duty to allow such access. Other cases however are more complex, and in

to access information relevant to their investigations; impose **remedies** such as ordering the destruction of information or ban processing, and start legal proceedings, hear complaints and issue reports.⁶⁰

- c) The agency is generally responsible for public **education** and raising awareness actions, speeches, organisation and participation in symposiums, courses and seminars, publication of an annual report and the drawing up of information documents for citizens such as brochures, manuals and recommendations.
- d) **Liaison** both on international as well as national level which entails cooperation with various entities such as ombudsmen, the public prosecutor, universities, autonomic information protection authorities, chambers of commerce and professional organisations.
- e) In a number of countries, this official also serves as the enforcer of the jurisdiction's **Freedom of Information Act**. These include Hungary, Estonia, Thailand, Ireland, and the United Kingdom.⁶¹ On the sub-national level, many of the German Lund Commissioners have recently been given the power of information commissioner, and most of the Canadian provincial agencies handle both information protection and freedom of information.

5.2.24 The contemporary role of the Information Protection Authority is therefore that of ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer and international ambassador.⁶²

those the authority tries to reach a compromise acceptable to both the data user and the data subject. Again, this approach is almost always "successful", in the sense that the authority does not need to use formal enforcement measures: the authorities in the Member States only resort to "hard" enforcement measures in a minute proportion of complaints. Korff *Comparative Study* at 207-208.

⁶⁰ Korff *Comparative Study* indicates that criminal prosecutions are an extreme rarity, reserved for the most obstinate or crass law breakers such as companies which continue to maintain unregistered databases in spite of repeated warnings, or which export data in spite of such warnings or formal notices, or people who knowingly flout the law by selling confidential personal information (eg policemen who obtain access to criminal records or other confidential information on behalf of unauthorised third parties).

⁶¹ The Irish and UK Commissioners have opted for a systemic solution to the problem in that the mechanism for enforcing the provision of their access regime and their data protection regime is one and the same – a Commissioner who regulates both.

⁶² Bennett Conference Paper 2002.

5.2.25 A number of countries that do not have a comprehensive act still have a commissioner. The major duty of these officials is to focus **public attention** on problem areas, even when they do not have any authority to fix the problem. They can do this by promoting codes of conduct and encouraging industry associations to adopt them. They can also use their annual reports to point out problems.

5.2.26 Examples of the work done by Privacy Commissioners in other countries are as follows:

a) In Canada both the Privacy Act and PIPEDA are overseen by the independent Privacy Commissioner of Canada:

- Under the Privacy Act⁶³ the Commissioner has:
 - The power to investigate, mediate, and make recommendations, but cannot issue orders or impose penalties.
 - During the course of an investigation the Commissioner may subpoena witnesses and compel testimony, and enter premises in order to obtain documents and conduct interviews.
 - The Commissioner is also charged with conducting periodic audits of federal institutions to determine compliance with the Privacy Act, and to recommend changes where necessary.
 - The Commissioner can initiate a Federal Court review in limited circumstances relating to denial of access to records.
- The Commissioner's powers under PIPEDA⁶⁴ are very similar to those under the Privacy Act.

⁶³ The office received a total of 1,713 complaints under the Privacy Act between April 1, 2000, and March 31, 2001, an almost ten percent increase from the previous year. Office of the Privacy Commissioner of Canada **Annual Report to Parliament 2000-2001, Part One—Report on the Privacy Act** December 2001. The office closed 1,542 investigations, again an increase of 10 percent from the previous year. 339 of these cases related to issues of collection, use, disclosure, or disposal, 630 related to access, and 573 to time limits. Since November 2001, the office has received more than 8,047 requests for information concerning the Privacy Act. (E-mail from Dona Vallieres, Senior Director General, Communications and Policy, Privacy Commission of Canada to Nicole Anastasopoulos, Research Assistant, Electronic Privacy Information Center, July 10, 2002 (on file with the Electronic Privacy Information Center).

⁶⁴ The Office of the Privacy Commissioner began receiving complaints under PIPEDA on January 1, 2001. By January 17, 2001, it was reported that the office had already received four formal requests for investigations and numerous telephone inquiries. Tyler Hamilton, "Confidentiality Fears Swamping Privacy Watchdog," **The Toronto Star**, January 17, 2001. As of November 2001, the Office had received more than 8,859 E-mail from Dona Vallieres, Privacy Commission of Canada, to EPIC supra, n.496. requests for information concerning PIPEDA, 95 formal complaints (half of which involved banks) and initiated 198 investigations. Office of the Privacy Commissioner of Canada **Annual Report to Parliament 2000-2001, Part Two— Report on the Personal Information Protection and Electronic Documents Act**, December 2001, available at <http://www.privcom.gc.ca/information/ar/02_04_09_e.asp#000.htm>. The Commissioner's office completed and issued findings and recommendations on 27 complaints.

- The Commissioner has powers of recommendation only with regard to complaints submitted under the Act. Once a complaint is received, the Commissioner assigns an investigator to look into the matter. The investigator then submits his findings to the Commissioner who then considers the case and issues a report with recommendations.
- He can also request the organisation in question to submit, within a specified period of time, notice of any action taken or proposed to be taken to implement these recommendations.⁶⁵
- However, if the Commissioner is satisfied that there are reasonable grounds to investigate a matter under the Act, he may initiate his own complaint.⁶⁶
- The Commissioner is also authorised to conduct broad research into privacy issues and promote awareness and understanding of privacy issues among Canadians.

b) In the UK⁶⁷ the Information Protection Commissioner is appointed in terms of section 6(2) of the Data Protection Act of 1998 by the Queen by Letters Patent. Para 1(2) confirms that the Commissioner, officers and staff of the Commissioner are not to be regarded as servants or agents of the Crown. Tenure of office is for a period of five years but the Commissioner may be reappointed. The powers and functions of the Commissioner can be classified as follows;

- duties to promote good practice and compliance;
- dissemination of information;
- involvement in respect of drawing up codes of practice;
- dissemination of Community findings in relation to transfers to third countries;

⁶⁵ See generally Office of the Privacy Commissioner of Canada *Your Privacy Responsibilities: A Guide for Business and Organizations* December 2000.

⁶⁶ Perrin S, Black H, Flaherty D and Rankin TM *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* Toronto, 2001.

⁶⁷ Bainbridge *Data Protection* at 217 and 143.

- assessing processing with the consent of responsible parties;
- laying reports and codes of practice before each House of Parliament;
- assisting individuals where processing is for special purposes; and
- participating in international co-operation.

5.2.27 The Data Protection Act 1998 furthermore follows a twin track approach (as it did with the 1984 Act) by giving the Commissioner powers of enforcement whilst also providing for a number of criminal offences under the Act. The Commissioner therefore has powers and functions pertaining to notification, enforcement, prosecution of offenders and powers of entry and inspection all set out in the relevant sections of the act.

5.2.28 The act also makes provision for the Data Protection Tribunal. The purpose of the Tribunal is primarily to hear appeals from data controllers/responsible parties in respect of notices served by the Commissioner or determinations made by the Commissioner as to whether processing is for special purposes. A data subject, however, does not have a right to appeal to the Tribunal against a decision of the Commissioner.

5.2.29 In reality the information protection authorities in the EU Member States see themselves much more as advisers, facilitators and conciliators than as policemen: referees rather than Rambos. As the UK information protection authority once put it:⁶⁸

Powers of enforcement are vital but our approach is to seek to anticipate complaints by providing adequate advice, or where they arise to proceed by agreement and negotiation only taking formal action where action to achieve compliance cannot be agreed (Annual Report 1996 at 32).

Problems

5.2.30 Problems experienced by **agencies** in giving effect to information legislation are as

⁶⁸ Korff *Comparative Study* at 206.

follows:

- a) A major problem with many agencies around the world is a **lack of resources** to adequately conduct oversight and enforcement. Some are burdened with licensing systems, which use much of their resources. Others have large backlogs of complaints or are unable to conduct a significant number of investigations. Many that started out with adequate funding find their budgets cut a few years later.⁶⁹
- b) **Independence** is also a problem. In many countries, the agency is under the control of the political arm of the government or part of the Ministry of Justice and lacks the power or will to advance privacy or criticise privacy invasive proposals. Finally, in some countries that do not have a separate office, the role of investigating and enforcing the laws is done by a human rights ombudsman or by a parliamentary official.
- c) The authorities also pride themselves on the effectiveness of their “conciliatory” approach, pointing out that they have to resort to “hard” enforcement measures in only a very limited number of cases. This conciliatory approach by the information protection authorities may, however, reinforce the idea on the part of many responsible parties that information protection is “soft law”.⁷⁰

5.2.31 On the other hand, the enactment of comprehensive legislation may have the following negative implications for **responsible parties**:

⁶⁹ In 1995 in South Africa, the Task Group on Open Democracy *compiled its Policy Proposals* on the basis of preliminary consultations undertaken by the Task Group late in 1994; Task Group on Open Democracy ***Open Democracy Act for South Africa: Policy Proposals 1995 at 18***. They identified principles, rather than details to serve as the basis for further consultations early in 1995. In so far as costs and fees of implementation of legislation are concerned, the Task Group, in their proposal in terms of the Open Democracy Act made the following interesting remarks when the affordability of the Open Democracy Bill was discussed (At the time the Open Democracy Act also included sections pertaining to privacy protection. These were removed to form a separate Privacy Act. See discussion above in Ch 1).

The question of cost is an important one, but it must be evaluated in a context which takes account of all the material considerations.....Cost estimates can be exaggerated: there is general tendency for officials confronted with new legislation to fear it, and consequently to exaggerate the likely cost. For these reasons, there is a need to evaluate cost estimates cautiously, alert to the factors which tend to exaggerate them. Despite this it is clear that the administration of the Act will compete for resources urgently needed elsewhere and that it is the responsibility of the Task Group to make recommendations which will minimise the cost to government of the act.

⁷⁰ Korff *Comparative Study* at 207.

- a) The informationbase owners may face additional costs in having to comply with whatever legislation is passed;⁷¹
- b) Responsible parties may be liable for stringent penalties for poor or non-compliance; and
- c) List brokers may suffer loss of business if third party lists are withdrawn until these are compliant. This could put companies out of business. The implication of not being able to do business should not be underestimated.⁷²

*Sanctions and remedies*⁷³

5.2.32 All information protection legislation stipulate a variety of sanctions and remedies for breach of their provisions. Provision is usually made for a combination of penalties (fines and imprisonment), compensatory damages and where applicable, revocation of licences and deregistration.

5.2.33 In some jurisdictions, the enforcement of information protection laws rarely involves meting out penalties in the form of fines or imprisonment. A variety of other means of remedying recalcitrance - most notably dialogue and, if necessary, public disclosure via the mass media - seem to be preferred instead. In other words, information protection laws often works by persuasion, is enforced by shame and punished by blame.⁷⁴

5.2.34 The topic of sanctions and remedies is dealt with only in very general terms by the CoE Convention, OECD Guidelines and UN Guidelines. The EU Directive is more specific. It requires that data subjects be given the right to a "judicial remedy" for "any breach" of their rights pursuant to the applicable national data protection law.⁷⁵ It also stipulates that decisions

⁷¹ The USA is currently debating the merits of privacy legislation and a major part of the debate concerns the costs to business.

⁷² It was argued that ways should rather be found to guide these companies and make things work in a practical way instead of finding ways to make life difficult and in the same process put people out of work. Barnard F "Informal Notes from the DMA to the Law Commission re a possible new Data Privacy Act for SA" 14 September 2001 at 6.

⁷³ See discussion in Chapter 6 below.

⁷⁴ Bygrave *Data Protection* at 79 and references therein.

⁷⁵ Art 22.

by a data protection authority which give rise to complaints “may be appealed against through the courts”.⁷⁶

(b) Self-regulatory system (eg USA)

5.2.35 The United States is a good example of the second category of enforcement systems namely the self-regulatory system. Industries in the private sector are encouraged to self-regulate. The law only intervenes on a narrowly targeted basis to solve specific issues where the marketplace is perceived to have failed.⁷⁷

5.2.36 American privacy policies are derived in part from the Constitution, in part from federal laws, in part from state law and in part from the common law. Ad hoc sectoral statutes, thus, address only an eclectic set of problems. In addition, voluntary policies adopted by companies and trade associations are significant influences.⁷⁸

5.2.37 Sectoral laws can be regarded as a patchwork of laws that regulate the collection and dissemination of different types of personal information in different ways, depending on how it is acquired, by whom, and how it will be used. Although these laws provide some level of privacy protection, they are not comprehensive in the sense that they do not apply uniformly to all service providers.⁷⁹

5.2.38 For instance, in the USA, Congress has created specific statutory rights to privacy for oral and electronic communications;⁸⁰ financial, educational and credit information;⁸¹ criminal

⁷⁶ Art 28(3).

⁷⁷ Reidenberg presentation 2001at 2.

⁷⁸ Ibid.

⁷⁹ US Department of Commerce *Privacy and the NII: Safeguarding Telecommunications-related Personal Information* October 1995 (US Department of Commerce *Privacy Report*) at 11.

⁸⁰ Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510 et seq (1995).

⁸¹ The Right to Financial Privacy Act, 12 U.S.C. 3401 (1978); the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g (1974); and the Fair Credit Reporting Act, 15 U.S.C. 1681 (1970).

history,⁸² and even video rental records.⁸³ All of these laws were passed following collaboration among civil liberties-, consumer-, and industry groups.⁸⁴

5.2.39 However, the eclectic statutory response illustrates the limitations of this method. Few meaningful legal privacy protections exist for some important categories of records, for example, marketing information.⁸⁵ Sectoral regulations are reactive and inconsistent. Furthermore, credit reporting agencies providing credit history information in connection with credit eligibility decisions are regulated, but direct marketing organisations providing similar information for pure marketing purposes are not. Drug abusers for example, have stronger protection than web users and video rental titles must be held confidential, though medical records can be disclosed.⁸⁶

5.2.40 This statutory gap-filling approach also leaves many areas of information processing untouched and runs counter to the cross-sectoral nature of modern information processing.⁸⁷

5.2.41 Since there are no comprehensive privacy legislation, there is also no oversight agency. As a result, individuals with complaints about privacy must pursue expensive lawsuits, or they may have no recourse at all. Also, foreign governments have nowhere to bring concerns about disparate privacy regulation.⁸⁸

5.2.42 In the USA there is general distrust of State control of economic and social matters, accompanied by scepticism towards legislative regulation of the private sector except where there are proven to exist flagrant imbalances of power between private parties which cannot be

⁸² Privacy Act of 1974, 5 U.S.C. 552a (1974); Freedom of Information Act, 5 U.S.C. 552 (1966).

⁸³ The Video Privacy Protection Act 1988, 18 U.S.C. 2710.

⁸⁴ Goldman *Brandeis Lecture* at 2 and references therein to the abovementioned legislation.

⁸⁵ Gellman RM "Data Privacy Law (book review)" *Government Information Quarterly* vol 14 no 2 1997 at 215-217 in a review of the book by Schwartz PM and Reidenberg JR *A Study of United States Data Protection* Charlottesville, VA Michie 1996.

⁸⁶ Reidenberg presentation 2001at 2.

⁸⁷ Reidenberg presentation 2001at 5.

⁸⁸ Gellman book review supra.

corrected otherwise than by legislative intervention. Industries have therefore been encouraged to self-regulate.⁸⁹

5.2.43 It is often overlooked that self-regulation is nothing new, but actually nothing more or less than the default position of the way in which most problems are solved in an orderly society. If legislation or other forces do not intervene, it is self-regulation by which individuals and organisations handle their interests.⁹⁰

5.2.44 The incentives for self-regulation can be described as moral persuasion, the desire to avoid adverse publicity and the seeking of a competitive advantage through regulating privacy practices.⁹¹

5.2.45 However, since the economic incentive to provide strong privacy protection is either weak, nonexistent, or at least non-uniformly distributed among all participants in the marketplace, most serious proposals for self-regulation among market participants rely on the threat of government regulation if the responsible parties fail to regulate themselves sufficiently.⁹²

5.2.46 In a more positive sense, self-regulation is often advanced as a means of experimenting and to prepare for regulation in a positive way. Self-regulation may also serve as a sector-specific way to implement legislation and to avoid too much detail in the legislation itself. A last option is that self-regulation can serve as a way to provide solutions beyond the scope of the existing legislation, which may or may not result in a new cycle of policymaking along the lines mentioned above.⁹³

⁸⁹ Froomkin *Stanford Law Review* 2000 at 1525.

⁹⁰ Hustinx PJ "Co-regulation or self-regulation by public and private bodies - the case of data protection" Published in *Freudendesgabe für Alfred Bullesbach 2002 Umbruch von Regelungssystemen in der Informationgesellschaft* (hereafter referred to as "Hustinx") at 2.

⁹¹ Bennett *Government Foundation Paper* 2001 at 23; Raab C D "Privacy Protection: The Varieties of Self-regulation" Paper delivered at the International Conference of Data Protection and Privacy Commissioners held in Cardiff on 9-11 Sept 2002 (hereafter referred to as "Raab presentation 2002").

⁹² Froomkin 2000 *Stanford Law Review* at 1525.

⁹³ Hustinx at 2.

5.2.47 In order for institutions to regulate themselves four interrelated policy instruments may play a role⁹⁴ namely privacy statements, privacy codes, privacy standards and privacy seals.

iii) Privacy commitments/ statements

5.2.48 Privacy commitments perform no other function than to indicate to clients, consumers and regulators that the organisation has considered privacy protection at some level, and believed that it would be good policy to state a set of commitments. They place on record what the organisation believes it does with a consumer's or a client's personal information. Many examples can be found in the privacy statements on contemporary public and private sector websites.⁹⁵ It is brief pledges intended for external consumption rather than to affect internal organisational functions. It rarely reflects any deep organisational culture and is often symbolic in nature. It may however be useful in stating the company's policies in brief, open and "user friendly" manner.⁹⁶

ii) Codes of conduct

5.2.49 Codes offer a flexibility and can be adapted to the specific economic, technological and regulatory contexts of different sectors. With or without legislation, codes will continue to be significant instruments by which organisational responsibilities are defined, employee obligations are communicated and citizen rights are established.⁹⁷

5.2.50 The successful implementation of privacy policy is inextricably linked to the ways in which that policy is developed. Before any codification takes place, a central question should be posed: Should the policy merely reflect existing business approaches, or should it reflect goals for which the organisation might strive in future. The correct answer is that it should reflect a

⁹⁴ Raab presentation 2002 at 1.

⁹⁵ Bennett *Government Foundation Paper* 2001 at 17.

⁹⁶ Bennett presentation 2002 at 18.

⁹⁷ Bennett CJ "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association" Prepared for the "Voluntary Codes Project" of the Office of Consumer Affairs Industry, Canada and Regulatory Affairs Treasury Board, March 1997 available at <http://web.univ.za/polisci/bennett> accessed on 29/10/2002 (hereafter referred to as Bennett Evaluation of Privacy Codes" at 4.

thorough understanding of existing practices, as well as a commitment to improve.⁹⁸

5.2.51 In short, the organisation should be prepared to implement any policy it codifies. The term “code of conduct” should be reserved for codified policies that not only state commitments to the outside world, but also bind employees to these obligations.

5.2.52 Many codes are developed in the absence of a regulatory framework in order to avoid or anticipate further regulatory intervention.⁹⁹ The debate about personal privacy protection for the private sector is often couched as a choice between the “voluntary” code and legislation. This is a false dichotomy. The range of possible incentives for compliance falls along a complicated continuum. At the one end is the purely voluntary code in which there is neither internal nor external compulsion to develop, adopt or implement privacy standards. At the other is the code existing within a full set of statutory obligations and liabilities. Some codes, for example that of the Canadian banking industry, fall in the middle of this continuum where a complicated and fluctuating range of incentives and sanctions are continuously at work.¹⁰⁰

5.2.53 Five kinds of privacy code can be identified¹⁰¹ according to their scope of application: organisational code¹⁰², the sectoral code,¹⁰³ the functional code¹⁰⁴, the professional code¹⁰⁵ and the technological code¹⁰⁶.

⁹⁸ Bennett Evaluation of Privacy Codes 1997 at 16.

⁹⁹ In contrast to codes that are developed to implement or supplement legislation as is the case within the framework of statutory data regimes.

¹⁰⁰ Bennett Evaluation of Privacy Codes 1997 at 21.

¹⁰¹ Raab presentation 2002 at 9-11. See also Bennett and Raab *The Governance of Privacy* at 123-126.

¹⁰² This applies to one agency that is bound by a clear organisational structure.

¹⁰³ The defining feature of a sectoral code is that there is a broad consonance of economic interest and function and a similarity in the kinds of personal information collected. Examples are the banking industry, life insurance etc.

¹⁰⁴ This code is defined less by the economic sector and more by the practice in which the organisation is engaged, for example direct mail and marketing. The Direct Marketing Association in South Africa represents businesses in a wide number of sectors.

¹⁰⁵ Codes developed for those directly involved in information processing activities eg market researchers, and health professionals.

¹⁰⁶ As new potentially intrusive technologies have entered society, codes have developed to deal with their specific application.

iii) Privacy standards

5.2.54 Privacy standards extend the self-regulatory code of practice in some important ways. Standards imply that a process exists through which an organisation's claims that they are adhering to privacy rules can be objectively tested. Technical standards may, for instance, include both a code of practice for computer security for instance and a standard specification for security management systems, which includes a risk analysis for the different categories of information stored by the organisation.¹⁰⁷

5.2.55 The idea of a more general privacy standard¹⁰⁸ that could incorporate the entire range of privacy protection principles was negotiated in Canada.¹⁰⁹ In this case the federal government announced its intention to introduce federal legislation based on the standard shortly after the standard was published, so there was never a pure test of whether a market mechanism alone would encourage registrations. General standards, similar to that of Canada's CSA, were also negotiated in Australia and Japan.¹¹⁰

5.2.56 The Centre Europeenne de Normalisations (CEN), responsible for the negotiation of standards within Europe and supported by the Article 29 Working Party, has begun to study the feasibility of an international privacy standard. This would comprise a general information protection standard which would set out practical operational steps to be taken by an organisation in order to comply with relevant information protection legislation, a series of sector specific initiatives in key areas such as health information and human resource

¹⁰⁷ Bennett presentation 2002 at 22. See in this regard the British Standard, BS7799.

¹⁰⁸ Bennett presentation 2002 at 23.

¹⁰⁹ The Model Code for the Protection of Personal Information was passed in September 1995 and was subsequently approved as a "National Standard of Canada" by the Standards Council of Canada.

¹¹⁰ In 1999 the Japanese Standards Association released JIS Q 15001. In Australia a set of National Privacy Principles were issued in 1998 by the Privacy Commissioner. The idea was to get Australian business to adopt these Principles in a formal manner. As in Canada, this initiative was overtaken by a more general legislative approach.

management and task specific initiatives mainly related to the online environment.¹¹¹

iv) Privacy seals

5.2.57 One logical corollary of any standard is a commonly understood mark, symbol or cachet that can be awarded to any organisation that is successfully certified or registered. The development of a specific “mark” or “seal” for privacy protection has, however, proliferated on the Internet. These programmes are built on the premise that consumers should be able to have consistent disclosure of privacy practices from all sites with which they interact.

5.2.58 To build consistency, these licencing programmes require participating websites to post a privacy policy disclosing their online information-gathering and dissemination practices. A cornerstone of these programmes is an online branded seal displayed by member websites and which is only awarded to sites that adhere to established privacy principles and agree to comply with ongoing oversight and dispute resolution procedures.¹¹²

5.2.59 What is needed therefore is a granting organisation responsible for examining private enterprises’ applications for the privacy mark and then certifying them. The enterprise must also have a compliance programme complying with the previously set guidelines (based on the guidelines of the business to which the enterprise belong). It must also demonstrate that personal information is appropriately managed based on the compliance programme or that a feasible structure has been established. The certification is then in existence for a specific period, for example two years.¹¹³

5.2.60 Current seal programmes have not, however, inspired great confidence.¹¹⁴ Furthermore, the more privacy seal programmes in existence, the more the consumer will be confused, and the more difficult it will be for any one system to achieve a reputation as the methodology by

¹¹¹ Bennett presentation 2002 at 24.

¹¹² Bennett presentation 2002 and references therein.

¹¹³ Bennett presentation 2002 at 25.

¹¹⁴ See discussion in Froomkin 2000 *Stanford Law Review* at 1525 as to the actions of the trustmarkholder TRUSTe. It became clear that firms licence the trustmark and some corporate sponsors contribute huge sums of money in support. If the trustmarkholder would start suspending trustmarks it would lose revenue; if it were to get a reputation for being too aggressive towards clients, they may decided they are better off without the trustmark and the attendant hassle.

which privacy protective practices can be claimed and assured.¹¹⁵

5.2.61 Ideally these four instruments (commitments, codes, standards and seals) should be cumulative. The self-regulatory process should involve:¹¹⁶

- a) an agreement and statement of organisational policy;
- b) a codification of that policy throughout the organisation or sector;
- c) a verification of those practices through some external and independent conformity assessment process; and
- d) the assignment of a “seal of good housekeeping”.

5.2.62 More often than not, however, public claims are made without adequate internal analysis, or external auditing. And privacy seals are invariably awarded without proper codification and verification of organisational practices. Therefore, the number of organisations that have engaged in privacy self-regulation in this cumulative and logical manner are very few.¹¹⁷

5.2.63 A more generic problem with self-regulatory schemes is that they regulate only those motivated or principled enough to take part in them.¹¹⁸

5.2.64 In 1998 the Department of Commerce in the USA was requested to report to the President on industry efforts to establish self-regulating regimes to ensure privacy online and to develop technological solutions to protect privacy.¹¹⁹ In this document it was stressed that to implement meaningful, consumer-friendly, self-regulatory regimes to protect privacy, self-regulation must do more than articulate broad policies or guidelines.

¹¹⁵ Bennett presentation 2002 at 26.

¹¹⁶ Bennett presentation 2002 at 26.

¹¹⁷ Bennett presentation 2002 at 26.

¹¹⁸ Froomkin 2000 *Stanford Law Review* at 1528.

¹¹⁹ National Telecommunications and Information Administration, Department of Commerce USA *Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy* Notice and request for public comment RIN 0660-AA13 dated 6 May 1998(hereafter referred to as “ NTIA Commerce Report”) at 1.

Effective self-regulation also involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from non-compliance.

5.2.65 A self regulatory privacy regime should therefore include mechanisms to assure compliance with the rules and appropriate recourse to an injured party when the rules are not followed. Such mechanisms are:

- a) Consumer recourse mechanisms: mechanisms through which complaints and disputes can be resolved. They should be readily available and affordable.
- b) Verification Procedure: This provides attestation that the assertions businesses make about their privacy practices have been implemented as represented. Because verification may be costly for business, appropriate cost-effective ways must be found to provide companies with the means to provide verification.
- c) Consequences: Failure to comply with fair information practices should have consequences. Examples of such consequences include cancellation of the right to use the certification seal or logo, posting the name of the non-complier on a “bad actor” list, disqualification from membership in an industry trade association. Non-compliers could also be required to pay the costs of determining their non-compliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion.

c) Co-regulatory system (eg Australia)

5.2.66 The third system identified is the co-regulatory system. This concept refers to self-regulation by an industrial association with governmental oversight and ratification.¹²⁰ It has been argued that this mixture of legislation and self-regulation may provide the optimum solution, offering advantages of flexibility and low-compliance of self-regulatory systems with the

¹²⁰

Bennett and Raab *The Governance of Privacy* at 184 notes that a distinction should be made between co-regulation and enforced self-regulation.

rights, obligations and enforceable bottom line of legislative guarantees.¹²¹

5.2.67 In Australia a set of National Privacy Principles were issued for the private sector in February 1998 by the Privacy Commissioner. At this stage only the public sector was formally regulated. The overall aim was to get Australian business to adopt these Principles in a formal manner, and thus to produce greater consistency in the Australian marketplace.

5.2.68 In December 1998, the Commonwealth Government announced its intention to legislate to support these Privacy Principles. The Privacy Amendment (Private Sector) Act was passed in December 2000 and came into force a year later. The broad acceptance by business of a set of national standards eased the process by which information protection law could be introduced for the private sector.

5.2.69 In this co-regulatory system industry codes play a far more central role than in other countries.¹²² It can be seen as a form of voluntary regulation within the confines of broader legislative provisions.

5.2.70 In Australia an organisation or industry registering a Privacy Code under the Australian Privacy Act, must prove and be legally accountable for the Code providing at least the same level of protection that the ten National Privacy Principles of the Australian Privacy Act require – preferably more.¹²³ Where a code is not established, the Privacy Principles set out in the Act automatically apply.

5.2.71 Any business or profession may develop a Code of Practice. The code must then be submitted to the Privacy Commissioner for approval. If the Code is deemed to be acceptable then the Commissioner may issue it. The Privacy Commissioner may also create and issue a Code, based on his or her own initiative or on the application of any other person. Legislation sets out the conditions subject to which a Commissioner may issue a Code. It may for instance stipulate that the code should provide for the appointment of an independent adjudicator to

¹²¹ Parliament of Australia Senate Legal and Constitutional Committee **Privacy in the Private Sector** Chapter 7 The Co-regulation model 1999 accessed at http://www.aph.gov.au/senate/committee/legcon_ctte/ on 2005/04/25.

¹²² Bennett and Raab *The Governance of Privacy* at 129.

¹²³ Michalsons for IMS. In March 2003, the Internet Industry Association of Australia lodged an application for registration of their Privacy Code of Practice for member companies with the Federal Office of the Privacy Commissioner. Concurrently, they have sought a ruling from the EU regarding adequacy and it is expected to have a positive resolution for trans-border transfer once local ratification is complete.

whom complaints may be made, the responsibilities and duties of such an adjudicator etc. It may also make provision for the review procedures of an adjudicator's decision under the approved privacy code.¹²⁴

5.2.72 Caution should be exercised where a code of conduct exists in that the code should not create a lesser standard than those set out in the Privacy Principles and thereby fall below the adequacy standard set out in the EU Directive. Another aspect to be noted is that companies operating in two or more industries (eg media and communications) should not be subject to multiple codes.¹²⁵ The cost of compliance with these standards may, furthermore, out-weigh the cost of compliance with formal legislation.¹²⁶

5.2.73 Relatively few Codes have so far been established. By far the greater number of businesses within the private sector, especially small to medium sized organisations rely solely on the Privacy Principles as set out in the Act, without feeling the need to develop a Code of Conduct.

5.3 Submissions received: Evaluation of options identified

5.3.1 In their submissions, the following specific comments were made by respondents regarding the systems identified above:

a) Regulatory system

(i) Comprehensive law¹²⁷

5.3.2 Respondents in favour of the regulatory approach stated that a new privacy law is now urgently required.¹²⁸ The legislature must facilitate good practice in so far as the protection of privacy in general and informational privacy in particular are concerned and should, through the

¹²⁴ See for example Part IIIA of the Australian Privacy Act 1988 as amended.

¹²⁵ Senate Committee at 6.

¹²⁶ Bennett and Raab *The Governance of Privacy* at 129.

¹²⁷ USA Department of Commerce only the respondent not in favour of a comprehensive law. See discussion on self-regulation in Para 5.3.43 below.

¹²⁸ Financial Services Board; ENF for Nedbank.

enactment of appropriate legislation, make provision for the mechanisms to facilitate this including the appointment of a body responsible for the administration of such legislation with sufficiently defined powers and functions. Where these rights are not respected the legislation should provide for judicial remedies which should be imposed on anyone, whether in the private or public sector, who fails to comply with the provisions of privacy and information protection legislation.¹²⁹

5.3.3 Respondents agreed that the legislation enacted should follow the broad principles laid down in the OECD Guidelines and in the EU Directive and argued that to follow the self-regulatory approach, the sectoral law approach or even the co-regulatory approach, will not generally be sufficient to qualify such legislation within the "adequate protection" requirement of the EU Directive.¹³⁰

5.3.4 It was argued that consolidated national information protection legislation will:

- * Provide a consistent approach to privacy and information protection across all sectors of the economy based on the founding principles¹³¹ listed in Chapter 4.¹³²
- * Go a long way in providing guidance and clarity in the regulatory and legislative environments pertaining to privacy and information protection.¹³³ The current legal situation is fraught with legal uncertainty (even as regards public sector rights to obligatorily demand disclosures from individuals), which must be clarified as soon as possible in the public interest.¹³⁴
- * Create an overall stable and investment-friendly regulatory and legislative framework, benefitting the South African economy and its people.¹³⁵

129 ENF for Nedbank.

130 Nedbank; See discussion in Ch 7 below regarding the adequacy requirement.

131 Fair and lawful processing, Openness; Collection limitation; Use/Purpose specification; Disclosure limitation; individual participation; Data quality; Finality; Security safeguards; Accountability and Sensitivity.

132 Vodacom.

133 Vodacom.

134 Financial Services Board, Banking Council.

135 Vodacom.

- * Give effect to both the South African common law and the Constitution of the Republic of South Africa in recognising and protecting the right to privacy (Section 14 of the Constitution).¹³⁶
- * Ensure that South African organisations are able to compete in the international information-technology based services market through cross-border transactions.¹³⁷

5.3.5 The objectives of a information protection system should essentially be:¹³⁸

- * To require compliance by responsible parties with the rules. A good system is generally characterised by a high degree of awareness among responsible parties of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.
- * To provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.
- * To provide appropriate redress to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which provides for compensation to be paid and sanctions imposed where appropriate.
- * To create a balance between protection and use of information on the one hand and ensuring adherence to privacy principles of the data subject on the use of the information.

(ii) Regulatory agency for South Africa?

5.3.6 An important question in the privacy debate in South Africa is whether an Information

¹³⁶ Eskom Legal Department; The Legislature forms part of the State and the latter must “*respect, protect, promote and fulfil the rights in the Bill of Rights*” (section 7(2) of the Constitution). In promoting the current type of new law, the State will be doing exactly what is so required.

¹³⁷ ENF for Nedbank.

¹³⁸ ENF for Nedbank.

Privacy Act should make provision for an information protection agency. In parallel debates during consultations on the Open Democracy Bill about the necessity of a regulating agency to ensure enforcement of this Act (which of course included privacy provisions at that stage),¹³⁹ the following interesting viewpoints were held:

- (a) The **Human Rights Commission (HRC)**¹⁴⁰ noted that the Open Democracy Bill did not establish an information protection authority as such, but used the Human Rights Commission to perform some of the functions of such an authority. The Bill furthermore set out internal appeal procedures. Should these be exhausted, and an aggrieved applicant (or respondent) remained dissatisfied, the Bill made provision for the High Court as the forum for relief.¹⁴¹ The HRC believed the High Court to be an inappropriate forum since it is inaccessible to ordinary people, both geographically, and in terms of costs, and it does not present a speedy remedy. It also lacks flexibility around issues of procedure, thereby preventing a development of sound jurisprudence, particularly on the question of the exemptions. The HRC stressed that this was particularly relevant to access to information, where there is no existing precedent, and a body of jurisprudence needs to be developed from scratch. The HRC submitted that an effective and appropriate enforcement mechanism would be crucial to the successful implementation and functioning of the Bill and referred to various options which could replace the use of the High Court, and the court system. These included the creation of a tribunal system, or the use of an ombudsman or Information Commissioner to resolve disputes. The HRC stressed that these options needed careful consideration, with emphasis on the short-term cost implications of setting up new bureaucracies, and the long term cost implications of clogging up the court system even further.¹⁴²

¹³⁹ The Bill subsequently became known as the Promotion of Access to Information Act 2 of 2002. The Act did not establish an information or data protection authority. The Justice Portfolio Committee has however now requested the Department of Justice to investigate the possibility of establishing an office for an Information Commissioner.

¹⁴⁰ Submission to the Open Democracy Bill.

¹⁴¹ PAIA eventually made provision for Magistrates' Courts and magistrates to be specifically designated by the Minister of Justice in terms of sec 1 and 91A of the Act as a forum for relief. To date, this has not happened yet.

¹⁴² PAIA currently also assigns responsibility for promotional and related functions and for dispute-resolution to separate bodies, as did the draft Open Democracy Bill. Moreover, responsibility for dispute-resolution is itself currently split between the Public Protector, which deals with disputes over mal-administration and the courts, which deal with disputes over enforcement of substantive rights under PAIA. The Human Rights Commission devotes three full-time staff to its PAIA responsibilities. The Head of Research and Documentation, of which the PAIA Unit is a part, also devotes significant time and energy to the unit. A committee called "PAIA.com" oversees the work of the PAIA Unit. Section 8 of the Human Rights Commission Act allows the Commission to attempt dispute-resolution through mediation, conciliation or negotiation and to rectify any act or omission regarding fundamental rights. It also has additional power conferred by other legislation.

- (b) The **Open Democracy Lobby Group**¹⁴³ agreed with the HRC and proposed the consideration of the introduction of an interim procedure between the internal and external review by the courts. Such a procedure would be directed towards conciliation and mediation, with the view to facilitating settlements of matters, and would utilise an informal and inquisitorial procedure. It would however have authority to make a decision if settlement is not achieved. This could be introduced in the form of an Information Officer, some form of a tribunal, or an Ombudsman.
- (c) In their submissions **IDASA and COSATU** made provision for the establishment of an Information Ombudsman appointed by the Minister, in consultation with the Portfolio Committee for Justice and Constitutional Affairs. The main object of the Ombudsman was stated to be to dispose of complaints lodged in terms of the Promotion of Access to Information Act in a procedurally fair, economical and expeditious manner.¹⁴⁴

5.3.7 One of the South African Law Reform Commission's preliminary proposals set out in its Issue Paper¹⁴⁵ dealing with privacy and information protection was that a statutory regulatory agency should be established. A flexible approach was however, advised in which industries would develop their own codes of conduct which would then be overseen by the regulatory agency. Comment was invited on these proposals.

5.3.8 The Commission received a mixed reaction from respondents. Many of the comments received were in favour of a statutory agency,¹⁴⁶ but some differed as to the powers to be

¹⁴³ Submission to Select Committee on Security and Justice on 11 August 1998 (sponsoring organisations: Black Sash, Environmental Justice Networking Forum, The Human Rights Committee, Idasa, The Legal Resources Centre, The SA Catholic Bishops Conference, SA Council of Churches, SA NGO Coalition).

¹⁴⁴ In order to achieve his or her main object, the Ombud: a) would investigate any complaint and may make the order which any court of law may make; (b) may, if it is expedient and prior to investigating a complaint, require any complainant first to approach an organization established for the purpose of resolving disputes, and approved by the registrar. After the Ombud has completed an investigation, he or she shall send a statement containing his or her determination and his or her reasons, signed by him or her, to all parties concerned as well as to the clerk or registrar of the court which would have had jurisdiction had the matter been heard by a court. Any determination of the Ombud shall be deemed to be a civil judgment of any court of law had the matter in question been heard such court, and shall be so noted by the clerk or the registrar of the court, as the case may be. A writ or warrant of execution may be issued by the clerk or the registrar of the court in question and executed by the sheriff of such court after expiration of a period of six weeks after the date of the determination, on condition that no application contemplated in section 14 has been lodged. Any party who feels aggrieved by a determination of the Ombud may, within six weeks after the date of the determination, apply to the division of the Supreme Court which has jurisdiction, for relief, and shall at the same time give written notice of his or her intention so to apply to the other parties to the complaint.

¹⁴⁵ SALRC Issue Paper 24.

¹⁴⁶ Eg MFSA; SAHA; ENF for Nedbank; ISPA; IMS.

afforded to such an institution.¹⁴⁷ Some respondents expressed their opposition to the creation of an oversight agency.¹⁴⁸

Respondents in favour of the creation of an agency argued as follows:

5.3.9 It was noted that a key requirement of an adequate and effective information protection system is that an individual faced with a problem regarding his personal information is not left alone, but is given some institutional mechanism to assist in ensuring his problems are addressed. Effective privacy protection must therefore include mechanisms for assuring compliance with the information protection principles, recourse for individuals affected by non-compliance of the principles, and consequences for responsible parties in cases of non-compliance. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse procedures by which each individual's complaint or dispute is investigated and resolved by reference to the Principles; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and correct and that privacy practices have been implemented as presented; and (c) mechanisms to remedy problems arising out of responsible parties' failure to comply strictly with the principles. Sanctions must be sufficiently rigorous to ensure that these mechanisms can operate effectively.¹⁴⁹

5.3.10 It was stated that the important role that over-arching privacy law has in establishing public policy objectives is acknowledged and a statutory regulatory authority as an essential part of an enforceable and comprehensive information protection regime, as set out above, is supported by research.¹⁵⁰ The establishment of a regulatory authority responsible for the enforcement of rights and resolution of disputes under the legislation, as well as the promotion, publicity, education, advice, assistance, monitoring and reporting to Parliament is therefore imperative.¹⁵¹

¹⁴⁷ SAFPS; FSB.

¹⁴⁸ Eg. Vodacom; SABC; LOA.

¹⁴⁹ ENF for Nedbank.

¹⁵⁰ IMS.

¹⁵¹ SAHA.

5.3.11 Of course, this does not mean that such an authority is the sole means of achieving this objective – but, rather, that it should be viewed as an essential cornerstone to a multi-faceted regime that provides the modern South African the benefits of e-commerce, economic and telecommunication infrastructure growth, privacy-enhancing technologies and control over their personal information in this progressive environment.¹⁵²

5.3.12 It should, however, be kept in mind that the right to privacy is not absolute and may be limited in appropriate circumstances, provided due process is respected and transparent mechanisms are in place. This limitation, however, requires a properly resourced oversight body/person (such as a privacy commissioner/ ombudsperson/ regulator) to ensure that the rights granted to individuals can be enforced and to ensure that where these rights need to be suspended, that they are done so with the maximum respect for the right as a whole.¹⁵³

152 IMS.

153 ISPA.

5.3.13 To cultivate a privacy culture in South Africa, it is incumbent upon government to launch educational campaigns on the right to privacy and access to information. It is a fact that the vast majority of South African citizens are wholly ignorant of the mere existence of the right to access information entrenched in the Constitution and as further detailed in the PAIA.¹⁵⁴ There is not currently sufficient championing of the right to access to information at higher levels of government.¹⁵⁵ It is also important to link privacy rights to increased usage of information and communication technologies. Many users of electronic communications do not trust these networks to secure their information. Where information gathering bodies are subject to codes of conduct, these should be publicised and users educated on the implications of a responsible party/gatherer violating such codes.¹⁵⁶ However, public relations and awareness campaigns require funds and, in an accountable government environment, require a quantifiable measurement of success in order to sustain access to these critical funds.¹⁵⁷

5.3.14 It was furthermore emphasised that the legislation should have enough teeth to ensure that all responsible parties comply with the legislation, in particular companies who sell information, marketing information and the like. There should be sufficient enforcement mechanisms and suitable punishment for those who flagrantly do not comply with the requirements of the information protection legislation.¹⁵⁸ A separate regulatory authority to oversee compliance within South Africa should have sufficient ability to ensure effective enforcement of contraventions of such legislation.

5.3.15 It was argued that it would be important in an independent review mechanism to include provision for making binding orders. This would meet concerns expressed in numerous quarters that PAIA currently fails to provide for sufficiently cheap, accessible, quick, effective and authoritative dispute-resolution.¹⁵⁹

¹⁵⁴ ISPA.

¹⁵⁵ SAHA.

¹⁵⁶ ISPA; ISPA has a code of conduct for members and all their members have to clearly display their privacy policies on their Internet web sites and draw users attention to the existence and provisions of such policies and they believe that similar provisions should bind other entities.

¹⁵⁷ IMS.

¹⁵⁸ Nedbank.

¹⁵⁹ SAHA.

5.3.16 Even in Canada it has been suggested the Federal Information Commissioner should be better resourced and given the power to make binding orders.¹⁶⁰ Provincial Information Commissioners' order-making *power* encourages parties to settle their disputes before orders are made. Whilst Canada's Federal Information Commissioner is unable to issue binding orders, it operates in a long-standing democratic system characterised by an entrenched culture of governmental openness and accountability, a feature not yet present in South Africa's young democracy.¹⁶¹

5.3.17 It was suggested that the way in which the local procedures should operate should take into account the problems experienced in the EU with regard to enforcement, ie it should be clear whether a particular contravention would amount to a criminal offence or not. It is suggested that a robust system be put in place to assist data subjects, with the regulatory authority having sufficient power to curtail non-compliance.¹⁶²

5.3.18 In addition, it is important that the legislation contemplates an easy means for data subjects to report on contraventions, which would not involve huge costs. Even if greater awareness is achieved, the over complicated enforcement processes involved in the PAIA (requiring litigation over the most simple dispute) dilute the value of the legislation.¹⁶³

5.3.19 Furthermore, the reliance on outdated court processes to ensure compliance with these protections undermines their benefits.¹⁶⁴ The need was stressed for a cheap, accessible, quick, effective and authoritative dispute-resolution mechanism. In particular, what is required is access to a mechanism available after the rejection of an internal appeal against denial of access to information, but before the commencement of court action.¹⁶⁵

¹⁶⁰ See Roberts A "New Strategies for Enforcement of the Access to Information Act" (2002) 27 *Queens Law Journal* 647-682.

¹⁶¹ SAHA.

¹⁶² Nedbank.

¹⁶³ ISPA.

¹⁶⁴ Internet Service Providers Association.

¹⁶⁵ SAHA.

5.3.20 In a submission to the Commission received from the Human Rights Commission¹⁶⁶ they argued that, on the basis of international experience and current public experience in South Africa, there is a need for a public statutory regulatory body. There are long established bodies in other jurisdictions, which further illustrate the need. The Unit shares the COSATU position on this issue. It is furthermore necessary, when looking into the enforcement mechanism of the right to privacy in terms of the proposed Privacy Act, that such a platform has the capacity capabilities to achieve the purpose of the proposed Act.

5.3.21 In April 2003, SAHA spent a week in Canada to examine that country's model. What impressed them was the extent to which, at federal level, the Commissioner's interventions had led to resolution and avoided expensive litigation. In its own work SAHA has taken six refusals to the High Court and each time an out of court settlement occurred. The settlements were facilitated by the State Attorney, who played a powerful mediating role. This is precisely what an Information Commissioner could do at a fraction of the cost.¹⁶⁷

5.3.22 In this regard, an adequately resourced oversight body/person is important to ensure that individuals and companies can have recourse to the law without the need for an expensive process.¹⁶⁸

5.3.23 With regard to the anticipated costs of implementation of the requirements of a information protection statute, together with the costs of setting up and maintaining a regulatory authority, it is suggested that (rather than compromising on the broad principles and more formal requirements which would ensure consistent compliance and provide satisfactory protection to data subjects) a phase-in period is allowed for local businesses to convert existing data and databases and to implement processes and procedures in order to comply with the legislative requirements.¹⁶⁹ The Law Commission was urged to ensure in its proposals for legislation that the costs for the protection of privacy are not onerous on service providers and operators. While the creation of a privacy culture in South Africa is wholly supported as well as the development of legislation to facilitate the development of that culture, one would wish to avoid a "double

¹⁶⁶ PAIA Unit South African Human Rights Commission "Comments on the DATA Protection Document" 1 June 2004.

¹⁶⁷ SAHA.

¹⁶⁸ ISPA.

¹⁶⁹ Nedbank.

taxation” for members who have to absorb the costs of enabling surveillance and at the same time protect privacy.¹⁷⁰

5.3.24 It is also important to recognise the need for additional resources to be committed to ensure effectiveness of any new independent review mechanism, for items such as staffing and training.¹⁷¹ It is imperative that an oversight authority should have adequate funding (now and in the future) as well as resources to adequately conduct oversight and enforcement.¹⁷² Whether the entity is a single person, or has regional officers/offices, government has to be lobbied to ensure that this ‘regulator’ is adequately resourced to carry out its mandate.¹⁷³

5.3.25 Moreover, such a body must be independent, that is, able to criticise any privacy invasive proposals.¹⁷⁴ This also requires sufficient insulation and protection from other arms of government. It was even suggested that such a person/office be afforded Chapter 9 protection as envisaged by the Constitution. Finally, this office should be coordinated and streamlined with other sector regulators to ensure effective regulation of the sector.¹⁷⁵

5.3.26 The question as to where a statutory authority should be situated produced different views:

- * Some respondents felt that, rather than to create another regulatory authority, the regulation of information protection had to be placed in the hands of an existing authority, such as the Human Rights Commission¹⁷⁶ or the Department of

¹⁷⁰ The Internet Service Providers’ Association; The Department of Communications noted that it is currently in the process of drafting directives for the implementation of the RIC Act, in consultation with industry. This Act has some severe cost implications for the communications industry and currently cost-sharing models with the government have been precluded which will certainly have an impact downstream on smaller providers and consumers.

¹⁷¹ SAHA.

¹⁷² EPIC and Privacy International *Privacy and Human Rights* 2002 at 13 and 14; MFSA.

¹⁷³ The Internet Service Providers’ Association.

¹⁷⁴ EPIC and privacy International *Privacy and Human Rights* 2002 at 13 and 14; MFSA.

¹⁷⁵ The Internet Service Providers’ Association.

¹⁷⁶ Society of Advocates, KwaZulu Natal; Financial Services Board stated that a mere supervisory authority with mere overseeing and advisory functions is acceptable, as otherwise those functions would have to be left to relevant State departments where specialist knowledge and experience will obviously not always be present. It would suffice if the Human Rights Commission is utilised for that purpose, with the Access to Information Act as a precedent (see section 10 and Part V of that Act).

Communication.¹⁷⁷

- * Others specifically indicated that they did not support the view that the authority should reside within or be related to the existing Human Rights Commission.¹⁷⁸
- * The Public Protector was furthermore not deemed to be the appropriate body to perform the function of dispute-resolution under PAIA and privacy legislation for the following reasons:¹⁷⁹
 - Its role is limited to disputes over mal-administration, whilst what is required is a more effective mechanism to deal with disputes over enforcement of substantive rights under PAIA and privacy legislation.
 - It deals solely with the public sector, whilst PAIA covers both the public and private sector as will privacy legislation. This in turn reflects the application of the rights of privacy and access to information to both the public and private sectors.
 - It has no power to make binding orders.

5.3.27 Another related question was whether the rights to access to information and privacy should be dealt with by separate agencies or whether one agency for both would be possible. It was argued that if separate agencies dealt with each right, a third authority or independent process would be required to ensure they were appropriately balanced when they, or actions of authorities responsible for them, conflicted. This would be impractical. Consideration of appropriate features of an authority responsible for privacy therefore requires consideration of existing regulatory arrangements regarding the right to access to information.¹⁸⁰

5.3.28 In Canada there are two commissioners at federal level– one for Freedom of Information and one for Privacy. This has led to clashes between the two officials. It may be better to have one officer combine both roles in South Africa. It would also be necessary to clarify the role of this officer in relation to the role of the Human Rights Commission which has statutory functions in terms of PAIA.¹⁸¹

¹⁷⁷ ENF for Nedbank; See also the discussion on sector-specific regulators below.

¹⁷⁸ Eg The Banking Council.

¹⁷⁹ SAHA.

¹⁸⁰ SAHA.

¹⁸¹ National Archives.

5.3.29 It was argued that there seems no reason why an oversight body should not be given authority to investigate complaints in terms of both the Promotion of Access to Information Act and any proposed information privacy legislation. It was submitted that such legislation is so closely related that a single referee would seem to be the most practical and financially sound method of ensuring compliance. It is worth noting that since the enactment of the PAIA there appears to have been virtually no compliance policing and an oversight body would be ideally suited to perform this task on receipt of complaints from consumers and members of the public.¹⁸²

5.3.30 In its report to the Human Rights Commission on its role with respect to PAIA, SAHA argued that sec 8 of the Human Rights Act dealing with dispute resolution does not allow the HRC to undertake dispute-resolution under PAIA, because PAIA establishes a legislative scheme to enforce the Act conferring specific power to resolve disputes on the Public Protector and very general and vague powers of this type on the Human Rights Commission. Given this, neither PAIA nor the Human Rights Commission Act should be interpreted to allow the Commission to “cut across” the dispute-resolution functions conferred on the Public Protector or to go beyond the specific role assigned to it by PAIA. The Commission itself, however, takes the view that its role regarding constitutional rights allows it to resolve disputes under PAIA in light of PAIA implementing a constitutional right. The Commission’s Legal Department does informally attempt to resolve disputes and its Complaints Committee of three Commissioners considers disputes which cannot be resolved informally. However, given uncertainty over the Commission’s powers under PAIA, it was recommended as follows:¹⁸³

- * Removal of the current role of the Public Protector in dispute-resolution under PAIA;
- * Insertion into both PAIA and privacy legislation of specific provisions conferring powers of dispute-resolution on either the Human Rights Commission or an independent Information and Privacy Commissioner.¹⁸⁴

182 SAFPS.

183 SAHA.

184 SAHA also argued that the Human Rights Commission is currently inadequately resourced to perform this role, even before considering its role regarding dispute-resolution. The need for adequate resourcing should therefore also be considered with respect to promotional and related functions under privacy legislation.

5.3.31 In conclusion the following recommendations were made:¹⁸⁵

- * That a statutory regulatory authority be responsible for privacy and information protection and that such an authority be:
 - responsible for access to information as well as privacy and information protection;
 - either the Human Rights Commission or a new independent Information and Privacy Commissioner;
 - responsible for both promotion, publicity, education, advice, assistance, monitoring, and reporting to Parliament and for enforcement of rights and dispute-resolution;
 - specifically empowered to resolve disputes under provisions of both PAIA and privacy legislation - this would involve amendments to PAIA;
 - accessible as a dispute-resolution mechanism intermediate between internal appeal against decisions of public or private bodies and recourse to the courts; and
 - empowered to make binding orders to resolve disputes.
- That *consideration* be given to assigning particular commissioners to issuing binding orders if the responsible authority also undertakes activities such as advising parties as to their legislative rights and facilitating handling of their complaints or applications at an earlier stage of the dispute-resolution process
- That the following steps in the dispute-resolution process under privacy legislation and PAIA be voluntary, at the discretion of the applicant or complainant:
- Internal appeals against decisions of public or private bodies (currently a compulsory step under PAIA); and
 - dispute-resolution by the independent regulatory authority, intermediate between internal appeals against decisions of public or private bodies and recourse to litigation in the courts.

Respondents who were against the creation of a new independent oversight agency submitted the following arguments:

5.3.32 The idea was supported that self-regulation should be developed by sector players,

¹⁸⁵

SAHA.

founded on the general principles established in the legislation. This would enable sectors to tailor information protection regulation to the specific characteristics of the relevant sector, however, still done on the basis of the principles established in the legislation. It was acknowledged that the legislation should provide recourse for consumer complaints or disputes for failure to comply with the code of conduct in accordance with the principles of self-regulation. The principle of positive regulation should, however, prevail, i.e. regulatory intervention should only be considered for repeated failure to comply with the legislation, eg through the prescription of appropriate and proportionate penalties for repeated breach of information protection provisions. It was noted that the self-regulatory approach that is currently specified in the Electronic Communications and Transactions (ECT) Act could provide guidance in this regard, and re-course for appeal of decisions should remain with the High Court.¹⁸⁶

5.3.33 It was furthermore argued that where recommendations are made for the establishment of a single information privacy regulatory authority, the implication is that such regulatory authority should be well-funded, well-skilled, and well-resourced to perform its task. However, it is of paramount importance that role clarity and jurisdiction in terms of a dedicated information privacy regulatory authority versus a sector-specific regulatory authority is obtained.¹⁸⁷ By implication, any duplication or overlap in jurisdiction with sector-specific regulatory authorities must be avoided, since it will simply result in “forum shopping” or inconsistent approaches in dealing with privacy and information protection matters.¹⁸⁸

5.3.34 Furthermore, the legislation will need to indicate clearly how co-operation with sector-specific regulatory authorities will occur, especially in dealing with customer complaints.¹⁸⁹

5.3.35 As an alternative, a more efficient, practical and workable option might be to task sector-specific regulatory authorities with information privacy issues for each particular sector, subject to specifying their powers in the information protection legislation.¹⁹⁰ If this second approach is followed, it is important that sector authorities are sufficiently funded, skilled and resourced to

¹⁸⁶ Vodacom.

¹⁸⁷ The difference between a sector-specific regulatory authority (instituted by the state) and a self-regulatory adjudicator (instituted and funded by the particular industry) should be noted.

¹⁸⁸ Vodacom. In analogy, the current concurrent jurisdiction of ICASA and the Competition Commission can be considered.

¹⁸⁹ Vodacom.

¹⁹⁰ See also the discussion above in para 5.3.27.

perform this additional role.¹⁹¹

5.3.36 Having a sector-specific regulatory authority will ensure that there is an authority whose duty it is to ensure that information protection policies and legislation are adequate and in line with international practice. This will also ensure that there is proper and adequate policing of issues around privacy protection. Such a regulatory authority will also be better placed to make determinations as to whether there is a need for sectoral privacy laws and particularly whether there is a need for specific privacy laws which apply specifically to state owned entities.¹⁹² The existing regulatory bodies, which oversee the various industries, have adequate systems and insight to properly ensure compliance and makes the need for an independent regulatory agency or authority unnecessary.¹⁹³

5.3.37 An example provided of a sector with an existing regulatory body is the long-term insurance industry. The FSB oversees the financial services industry and it was argued that they would be the most appropriate regulatory body to oversee the protection of information in long-term insurance.¹⁹⁴ It has insight into the industry and already has systems in place and is actively involved in monitoring compliance, which would minimise costs.¹⁹⁵ Members of an independent oversight agency will not have insight into the requirements and environment applicable to the long-term insurance industry. For instance, the types of products marketed and the processes in place in the long-term insurance industry usually are complex. An outsider may not easily be aware of all of the conflicting issues, if an outsider were to regulate the industry.¹⁹⁶ The long-term insurance industry is also regulated by the Life Offices' Association (LOA). The LOA has various Codes of Conduct which include the protection of registers and information. Add to this that legislation already exists that regulates this industry on this point (like the Policy Protection Rules and the Financial and Advisory Services Act) and one will quickly see that there is no room for a statutory regulatory agent. Moreover, one must also consider that such an

¹⁹¹ Vodacom.

¹⁹² SABC.

¹⁹³ LOA submission.

¹⁹⁴ LOA.

¹⁹⁵ LOA.

¹⁹⁶ LOA.

agency will have virtually no experience in this industry and will be compelled to draw on the experience of the FSB or the LOA, creating a multiplicity of functions. Another example is the banking industry which has the Banking Council of South Africa, in addition to being regulated by the Financial Services Board.¹⁹⁷

5.3.38 It was argued that it would be more sensible to amplify the functions of these bodies, rather than to create a new agency. Agencies are indeed administratively expensive and tardy and reliant on the government to come to life. Government involvement at this juncture adds no value and will retard the process to the point where the law becomes meaningless. One needs only to look at the government initiatives in terms of the ECT Act which have not seen the light of day several years post promulgation to understand this statement.¹⁹⁸

5.3.39 It was proposed that the envisaged legislation should rather lay down the criteria in terms of which information may be collected, kept and used and that the body which collected the information be the guardian of its information. Should the collecting body not meet the criteria of the legislation or refuse access to its information, an aggrieved party will have recourse to the courts. It is foreseen that a single statutory regulatory authority cannot control the databases of both the public and private sector in view of their vastly different roles and mandates. The creation of yet another statutory body will also be costly and may prolong the implementation of information protection laws.¹⁹⁹

There were respondents who were in favour of a regulatory authority, but only if such an authority had only mediating and educational and ombuds functions. Arguments were as follows:

5.3.40 The appointment of an information commissioner should be avoided, but an ombudsperson with legislative power should be considered.²⁰⁰ The ombudsperson would be responsible for responding to complaints from consumers and other aggrieved persons who believe that their right of privacy have been infringed. It is foreseen that there should be a number of Ombudsman offices in the main centres of the country and an electronic means of submitting

197 LOA.

198 Liberty.

199 SAPS.

200 SAFPS; See also "What Price Privacy" *Finance Week* 26 November 65 where it is estimated by research agency Jupiter that by 2006 business spending on privacy and security issues will be five times that of 2001. This is considered a luxury that the fledgling South African economy and democracy simply cannot afford.

complaints via an Internet website and fax on demand service. It is foreseen that the office of The Ombudsman would operate along similar lines to that of The Banking Adjudicator, but with legislative powers to enforce compliance.²⁰¹

5.3.41 The appointment of a Commissioner to act as a policeman in ensuring compliance with information privacy legislation is, however, not supported. Any proposed legislation should, if submitted, be based on the USA Safe Harbour style of enactment and that industry bodies would be required to ensure compliance by their members and associate organisations. The establishment of a massive bureaucracy to monitor information privacy legislation is not in the best interests of South Africa which, unlike first world countries, has neither the economy nor infrastructure to effectively operate such a system.²⁰²

5.3.42 An oversight body is, however, necessary in South Africa to focus public attention on problem areas, even though they might not have the authority to fix the problem. They can for example promote codes of practice and encourage industry associations to adopt them.²⁰³

(b) Self-regulatory system

5.3.43 One submission was received in which self-regulation (only sectoral legislation/codes of conduct and then only when and if necessary, no oversight agency) as a way of privacy protection was promoted. It was received from the United States Department of Commerce and set out the position regarding privacy protection in the United States as follows:²⁰⁴

- * The importance of protecting the privacy of individuals' personal information is a priority for the federal government and consumers. The United States Government is focused on creating the best environment for growth through a deliberate and balanced approach to privacy that is open to innovations.
- * Despite the benefits of information sharing, concerns about privacy are real and legitimate. Consumers repeatedly cite fears that their personal information will be

201 SAFPS.

202 SAFPS.

203 MFSA.

204 United States Department of Commerce.

misused as a reason for not doing business online. Therefore, moves to bolster on and off-line privacy and to protect consumer interests will fuel trust and the broader growth of cross-border trade, on-line communications, innovation, and business.

- * At this time, the U.S. does not have federal comprehensive legislation of mandatory “baseline” privacy requirements. Instead, the U.S. has adopted a flexible approach to privacy protection. The U.S. believes that self-regulatory initiatives (including company codes of conduct, “seal programs” and alternative dispute resolution mechanisms), coupled with a governmental enforcement backstop, are effective tools for achieving meaningful privacy protections.
 - * On the other hand, in certain highly sensitive areas, legislative solutions are appropriate. Congress has adopted legislation to protect certain highly sensitive personal information, including children’s information, medical records and financial information. In addition, the Administration has moved forward with an agenda to further prevent identity theft, spamming and the unauthorized use of social security numbers.
 - * In order to achieve these ends, the U.S. Federal Trade Commission (FTC) has announced a major privacy enforcement initiative that increases resources dedicated to protecting consumers from the negative consequences of the misuse of consumer information, whatever the source. The FTC is committed to vigorously enforcing current laws that impact consumer privacy, including unwanted and fraudulent telemarketing sales, spam, Internet fraud, identity theft and The Children’s Online Privacy Protection Act, to name just a few areas, in addition to enforcing commercial privacy policy promises.
 - * The U.S. believes that it is important to continue its dialogue with the business community and consumer groups to encourage broader adoption of privacy protections and adherence to self-regulatory privacy policies. Multilateral and private-sector initiatives have an important role to play in encouraging the development and use of privacy-enhancing technologies and in promoting consumer education and awareness about online privacy issues. The U.S. has continued its commitment to work with other countries, private sector groups such as the Global Business Dialogue on Electronic Commerce (GBDe) and the Trans-Atlantic Business Dialogue (TABD), multilateral organizations such as the Organization for Economic Cooperation and Development (OECD), and other
-

stakeholders, such as consumer groups, to promote internationally compatible approaches to privacy.²⁰⁵

- * Reference was also made to the role of privacy sector initiatives. The following privacy resources and organizations were referred to:
- a) Codes of Conduct/Privacy Frameworks;²⁰⁶
 - b) Privacy Policy Generator Tools;²⁰⁷

205

USA; **OECD**. Current OECD work on privacy and the protection of personal data builds on the 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. The October 1998 Ottawa Declaration on the Privacy of Global Networks reaffirmed the commitment of the OECD member countries to protect privacy on global networks and specifically recognized self-regulatory approaches. The OECD's current work program includes further encouraging the use of privacy-enhancing technologies and promoting user education and awareness about online privacy issues.

GBDe. The GBDe has also been active on the privacy front. The GBDe is in a unique position to facilitate discussion between consumers, industry and government. It is helping to lead the international effort to address consumer confidence on and off-line with the aim of making recommendations to governments. The GBDe has prepared draft personal data privacy protection guidelines which calls for companies to set company policies that respect and use the guidelines whether or not they are required by applicable law. The U.S. believes that the GBDe draft guidelines, and similar initiatives, are useful alternatives to the "one-size fits-all" legislative approach to data privacy protection.

APEC. APEC is in the process of developing the APEC Privacy Framework that will include both privacy principles and implementation mechanisms. The Framework will build upon the 1980 OECD Privacy Guidelines (referenced above) to create a system of privacy protection that is appropriate for the particular conditions in the APEC economies. The framework will focus on a cooperative approach that will balance and promote both effective privacy protection and the free flow of information in the Asia Pacific region.

206

Online Privacy Alliance (<http://www.privacyalliance.org/>)

The alliance has developed guidelines for creating an effective privacy policy, establishing enforcement mechanisms, and protecting children's privacy online. The alliance is comprised of more than 40 global corporations and associations.

Privacy Leadership Initiative (PLI) (<http://understandingprivacy.org>)

PLI has developed model practices for the exchange of personal information between business and consumers. Comprised of more than 20 companies and associations.

Network Advertising Initiative (<http://www.networkadvertising.org/>)

Created by leading online advertisers engaged in "online profiling". Sets forth self-regulatory principles for online advertisers to protect consumers' privacy while engaging in online advertising.

Global Business Dialogue on Electronic Commerce (GBDe) (<http://www.gbde.org/gbde2003.html>)

A worldwide, CEO-led, business initiative, established in January 1999 to assist in the creation of a policy framework for the development of a global online economy. Has developed personal Data Protection Guidelines for online merchants, trustmark providers, and any other businesses.

AICPA/CICA Privacy Framework

(http://www.aicpa.org/innovation/baas/ewp/2003_06_ed_execsumm.asp)

The Assurance Services Executive Committee (ASEC) of the American Institute of Certified Public Accountants (AICPA) and the Assurance Services Development Board (ASDB) of the Canadian Institute of Chartered Accountants (CICA) have issued an exposure draft of a proposed Privacy Framework. The proposed Framework provides criteria and related material for protecting the privacy of personal information and can be used by certified public accountants (CPAs) in the United States and chartered accountants (CAs) in Canada, both in industry and in public practice, to guide and assist the organizations they serve in implementing privacy programs.

207

USA; **Organization for Economic Cooperation and Development (OECD)** (<http://cs3-hq.oecd.org/scripts/pwv3/pwvhome.htm>)

Electronic commerce is a central element in the OECD's vision of the potential that our networked world holds for sustainable economic growth, more and better jobs, expanding world trade, and improved social conditions. The OECD's analysis has permitted a broad-based policy reflection on the establishment of the various elements that can provide a favorable environment for electronic commerce.

Direct Marketing Association (DMA) (<http://www.the-dma.org/privacy/creating.shtml>)

This tool has been developed to help marketers create policies that are consistent with The DMA's Privacy Principles for Online Marketing.

- c) Privacy “Seal” Programs/Verification Services;²⁰⁸
- d) Alternative Dispute Resolution Providers;²⁰⁹ and
- e) Privacy Protection Training/Awareness.²¹⁰

208

TRUSTe (<http://www.truste.org/>)

TRUSTe is an independent, non-profit privacy organization whose mission is to build users' trust and confidence on the Internet and, in doing so, accelerate growth of the Internet industry. Through extensive consumer and Web site research and the support and guidance from many established companies and industry experts, TRUSTe has earned a reputation as the leader in promoting privacy policy disclosure, informed user consent, and consumer education. TRUSTe was founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium, who act as independent, unbiased trust entities. The TRUSTe privacy program-based on a branded online seal, the TRUSTe "trustmark"-bridges the gap between users' concerns over privacy and Web sites' desire for self-regulated information disclosure standards. Also serves as a verification system and dispute resolution provider for its seal-holders.

BBBOnline (<http://www.bbbonline.org/>)

BBBOnline is a wholly owned subsidiary of the Council of Better Business Bureaus. *BBBOnline's* mission is to promote trust and confidence on the Internet through the *BBBOnline* Reliability and Privacy Seal Programs. *BBBOnline's* web site seal programs allow companies with web sites to display the seals once they have been evaluated and confirmed to meet the program requirements. The *BBBOnline* Privacy Seal confirms a company stands behind its online privacy policy and has met the program requirements regarding the handling of personal information that is provided through its web site. Also serves as a dispute resolution provider for its seal-holders.

BBBOnline is also developing the Global Trustmark Alliance (GTA). GTA will help expand the access of businesses online to the international marketplace by increasing consumer confidence around the world in cross-border Internet transactions. The Alliance, a partnership between non-profit business and consumer associations and governments around the world, will be especially helpful to small and medium sized businesses (SMEs) that particularly suffer from name recognition problems outside their local marketplaces.

Direct Marketing Association (The DMA) (<http://www.the-dma.org>)

The Direct Marketing Association (The DMA) is the largest trade association for businesses interested in interactive and database marketing. Companies displaying The DMA Member logo have committed to the association's Privacy Promise. The DMA's Privacy Promise is an assurance to consumers that U.S. marketers who are DMA members will use personal information in a manner that respects consumers' wishes. Also serves as a dispute resolution provider for its seal-holders.

AICPA WebTrust (<http://www.cpawebstrust.org/>)

The WebTrust program is a set of e-commerce standards comprised of prevailing best practices and requirements from around the world; an independent verification that a site meets the standards; and an internationally recognized web trust seal, announcing that an e-Commerce site meets the stringent standards. Also serves as a dispute resolution provider for its seal-holders.

SquareTrade (<http://www.squaretrade.com/cnt/jsp/index.jsp>)

SquareTrade's mission is to build trust in transactions and to create a better online trading experience. SquareTrade's services aim to help buyers identify trustworthy sellers they can buy from safely, as well as help good sellers show buyers that they can be trusted.

Entertainment Software Rating Board (ESRB) (<http://www.esrb.org/privacy.asp>)

ESRB Privacy Online addresses consumers' concerns regarding privacy by requiring Web publishers to develop and implement meaningful and informative privacy policies and practices for their websites. ESRB protects the rights of Web consumers, and the interests of Web publishers, and help make the Internet a secure, reliable, and private place to share information and conduct business. Also serves as a verification system and dispute resolution provider for its seal-holders.

209

In addition to the “seal” programs listed above, the following organizations provide dispute resolution services for their members/clients:

American Arbitration Association (<http://www.adr.org/index2.1.jsp>)

The American Arbitration Association is available to resolve a wide range of disputes through mediation, arbitration, elections and other out-of-court settlement procedures. The American Arbitration Association assists in the design of ADR systems for corporations, unions, government agencies, law firms and the courts. The American Arbitration Association has played an instrumental role in establishing systems, which may utilize a variety of dispute resolution techniques, to address a full range of disputes involving, but not limited to, employment, consumer, technology, health care, bankruptcy, financial services, accounting, international trade and mass claims.

JAMS (<http://www.jamsadr.com/home.asp>)

JAMS provides the highest quality dispute resolution services to our clients and to our local, national and global communities. JAMS' neutrals include the ADR industry's most respected mediators, arbitrators, private judges, facilitators, special masters (or referees) and neutral advisors.

Privacy Council (<http://www.privacycouncil.com/>)

Privacy Council consultants have worked for years with organizations in the United States and around the world on privacy-related issues. Their expertise ranges from helping organizations to develop privacy programs to ensuring that their Web sites comply with privacy laws. Privacy Council is also in the process of enhancing its existing services to provide dispute resolution for its clients.

210

GetNetWise (<http://www.getnetwise.org>)

5.3.44 With respect to the possibility of legislative measures in South Africa to address privacy protection issues, caution was expressed against the unintended consequences of broadly prescriptive legislative measures. Possible costs to be noted resulting from implementing privacy legislation, which may be highly resource intensive for government and private sector.

5.3.45 It was suggested that, as important trade partners, South Africa and the United States should work together on approaches for addressing legitimate concerns about privacy protection and relevant trans-border issues. The initiatives used in the USA as set out above could serve as useful alternatives to “one-size-fits-all” legislative approaches to privacy protection. South Africa was encouraged to actively consider these efforts and the role that self-regulatory programs can play in bolstering privacy protection.

5.3.46 In concluding their comments it was stated that the challenge for the U.S. and its partners is to achieve internationally compatible standards for privacy protection while preventing the interruption of trans-border information flows, the life-blood of electronic commerce and cross-border trade and services.

5.3.47 Another respondent, however, raised a cautionary note²¹¹ in indicating that the absence of a contractual remedy in the South African law for damages to personality interests²¹² undermines theories of market based or self regulation. While the market might generate an incentive to incorporate privacy policies in agreements there is no corresponding legal incentive to adhere to the policy. It could be argued that customers will eventually refuse to contract with

ISP organization that educates parents on tools and measures to protect their children’s privacy and security online.
Center for Democracy and Technology (<http://www.cdt.org/privacy/>) and the **Privacy Leadership Initiative** Created “privacy toolboxes” for online users, which are posted on their websites. These “toolboxes” typically tell users how they can limit disclosure of their personal information, what choices they have about how such information is used and shared, and under what circumstances they can access it

Econsumer.gov (<http://econsumer.gov/>)

Website provides means of consumer reporting in Internet privacy complaints and those relating to cross-border e-commerce transactions.

U.S. Federal Trade Commission (<http://www.ftc.gov>)

Provides public information on privacy compliance initiatives and safeguards.

211 Andrew Rens.

212 According to two Appellate Division cases only patrimonial damages can be recovered on the strength of a breach of contract. In *Administrator, Natal v Edouard 1990 (3) SA 581 (A) at 595-596* the court held that only patrimonial damages may be recovered for breach of contract. While the ratio decidendi in that case concerned a sui generis claim for pain and suffering, the principle was applied to ‘sentimental damages’ in *Jansen Van Vuuren ao NNO v Kruger 1993(4) SA 842 (A)*, in which it was held that “only patrimonial damages can be recovered on the strength of a breach of contract”. Infringement of personality is a circumstance that affects both the lawfulness of conduct and amount of an award. This produces the same problem that arose under the Aquilian action, that these types of damages are not appropriate for damage to personality. Damages for harm to personality interests have a rather different conceptual basis and while this is in itself problematic it fits breaches of privacy better than contractual damages does.

an entity if it notoriously does not keep its promises, however ease of incorporation and corporate access to channels of communication undermines this. The status of privacy as a constitutional right also raises problems for a purely market based approach since the law on contracting around constitutional rights is not clear.²¹³

(c) Co-regulatory system

5.3.48 Respondents in favour of the co-regulatory system made it is clear that they see information protection legislation as the appropriate legal instrument in terms of which to control the collection, processing and security of personal information. However, while regulation should provide benefits for society in general it should not place unnecessary and excessive burdens on industries. In particular, it should be ensured that the compliance and enforcement costs of regulation should not exceed the benefits.²¹⁴

5.3.49 A framework should, therefore, make provision for regulatory and self-regulatory mechanisms that complement each other. Ensuring high quality and effective information processing and information security systems should be an area of self-regulation. Cognizance should, furthermore, be taken of voluntary ombud which exist outside legislation but could be an important part of any framework.²¹⁵

5.3.50 One respondent²¹⁶ indicated that sectoral laws which complement more comprehensive legislation may be the best option. The view was raised that the legislature should enact information protection laws specific to state owned entities while at the same time ensuring that general or sectoral privacy protection laws are such that each state owned entity is able to apply its own privacy regulatory policies in whichever industry the state owned entity falls without any constraints or conflicts. An organisation is best placed to understand the needs, demands and restrictions of its particular business and could thus be solely responsible for determining the manner in which it regulates privacy and information protection under the guidance and authorisation of some kind of regulatory body. Alternatively, the organisation

²¹³ Andrew Rens.

²¹⁴ Credit Bureau Association.

²¹⁵ Credit Bureau Association.

²¹⁶ SABC.

could work closely with the body responsible for structuring its specific policy and code in the development of such policies and codes. Other entities, particularly state owned entities, in other industries could also work closely with such a regulatory body to ensure that the laws developed and enacted are practical.²¹⁷

5.3.51 Another view was that the idea of a flexible approach is supported wherein industries would develop their own codes of practice, but that the concept of a regulatory overseer is not supported. A statutory regulatory agency should be established but this should be in the form of an ombudsman's office, who would have legislative powers to react to complaints of non compliance with the proposed legislation. Within the proposed legislation the Ombudsperson should be provided with powers to adjudicate, suspend, caution and in the event of serious non-compliance, even close down any organisation or concern that does not comply with the industry standard which would form part of a specific industry.²¹⁸

5.3.52 The following framework to deal with privacy and information protection was proposed:

- * A general Privacy Act should constitute a generic framework to apply across different industries. The overriding legislation should not be too specific, in order not to be too restrictive in its impact. For that reason, the definitions in that Act should be wide and generic in nature, and should only contain the general principles. The generic nature would be important to assist different industries in complying with the proposed Act.²¹⁹
- * Compliance should be monitored by the different regulatory bodies overseeing the various industries, with codes of conduct made applicable within the various industries. It would be up to each industry to ensure compliance with general guidelines, but with particular rules operating within their own industry.²²⁰

217 SABC.

218 SAFPS. In addition to the above SAFPS, in conclusion again re-iterates the need for inclusion in the legislation of a provision similar to section 29 of the UK Data Protection Act. It argues that a failure by the legislature to include such a provision will result in wholesale fraudulent activity by unscrupulous and criminal elements in society.

219 LOA; In order to assist the Minister to draft appropriate regulations, it is proposed that a formal Advisory Council be appointed, with representation from different industries. Such representation should include long-term insurers as well as intermediary bodies. This process follows the general trend, which has emerged in recent years with legislation such as the Financial Intelligence Centre Act and the Financial Advisory and Intermediary Services Act. Representation should also include contact with bodies such as the International Security Forum, and other international bodies, who have conducted much research into data protection and privacy issues.

220 LOA.

- * This would provide a real incentive for Industry to “own’ their legal obligations and be educated about them. By being informed and pro-active, tangible business benefits and competitive advantage can be gained.²²¹
- * By ensuring that there is an enforcement agency with oversight obligations and registration procedures for industry Codes of Conduct that is governed by a supporting legislative framework enshrining Privacy Principles, industry-specific practices and policies can be codified and measured (via standards).²²²

5.3.53 This flexible and pragmatic approach by way of enforceable sectoral and regulatory approved codes of conduct will therefore balance and accommodate varying interests. It will also be the most pragmatic route to follow.²²³

5.3.54 An example supplied of an industry already subject to various codes was said to be that of the long-term insurance industry. All members of the LOA are contractually bound to comply with the various codes of conduct of the LOA. A breach of any one of the codes of conduct can lead, in terms of the disciplinary provisions of the LOA, to the imposition of fines, suspension and termination of membership of the LOA. Peer pressure and market forces also compel insurers to comply with the codes.²²⁴ Many of the principles espoused in the Issue Paper are already present in the LOA Code.²²⁵

221 Michalsons for IMS.

222 Michalsons for IMS.

223 Sanlam Life: Law Service.

224 Details of each of the LOA codes of conduct are available at www.loa.co.za. It is not intended to go into each of the codes in detail, but merely to provide two examples of the role the LOA plays with regard to privacy and data protection. The LOA Code on the Life Register provides in clause 1 as follows:

“The insurance risks which insurers are asked to cover, and the claims they are asked to pay, must be properly assessed. To do this insurers must be able to obtain information relevant to those risks and claims.

The Life Register is a data base through which insurers can share information about persons who propose for, or who are the lives assured under, policies and who have “notifiable impairments” that are relevant to the risk or claim assessment.”

225 LOA; Annexure B to the Code on the Life Registry provides for access by the public to any data contained on the LOA Life Register relating to whether any data relating to that person exists on the Register and/or the nature of entries relating to that person. In terms of section 7.6 of the Code, “Should the accuracy of the information on the Registry be questioned by the person to whom the information relates, this issue is to be dealt with between that person and the life office concerned.” The Code on the Life Register deals also with how a data subject may obtain information via his/her appointed medical doctor. Generally, the purpose of the information being stored is disclosed by the LOA and is freely available to the public.

5.4 The proposed information protection system for South Africa

5.4.1 In comparing different information protection laws, cross-national regulatory trends²²⁶ can be identified.²²⁷ Some of these are as follows:

- * increasing regulatory density, therefore more detailed discriminating provisions and requirements;
- * increasing concern to lay down procedural mechanisms for enforcing compliance with the information principles;
- * a shift in regulatory focus, for instance the encouragement of sectoral codes of practice;
- * a trend away from comprehensive licencing regimes to requirements for mere notification/registration of information-processing operations; and
- * enhancement of opportunities for participatory control.

5.4.2 A highly efficient information protection system would therefore comprise:²²⁸

- * a strong and unambiguous law;
- * an active and assertive regulatory authority;
- * a strong commitment by responsible parties, reflected at least in the establishment of the requisite procedures for compliance and, in particular, by an effort to collect as little information as possible for the carrying out of legitimate activities;
- * with respect to private sector compliance, a set of market incentives that drive companies to be pro-privacy and to implement those goals through strong self-regulatory mechanisms;
- * a vigilant, concerned and activist citizenry that is prepared to complain, to exercise access and correction rights, and to opt out of secondary uses of their information;

Regarding the accuracy of information, it is in the interests of long-term insurers to ensure that information maintained on a centralised LOA database is maintained and kept up to date. Some of these codes, such as the HIV Protocol are even more stringent with regard to the application of security regarding the data retained by life offices relating to the HIV status of individuals; LOA; "The purpose of the HIV Testing Protocol is to ensure that the life industry follows the highest standards in all aspects of HIV screening of applicants for life assurance.... It addresses issues such as identification, confidentiality, informed consent, pre- and post-test counselling, transmission of test results, accreditation of test kits and laboratories and the use of exclusion clauses."

²²⁶ In data protection discourse it is popular to categorise these trends in terms of generations: ie first-, second- and third-generation data protection laws. See Bygrave *Data Protection* at 88.

²²⁷ Bygrave *Data Protection* at 88.

²²⁸ Bennett and Raab *The Governance of Privacy* at 207.

- * the application, as far as possible at the outset of system development, of privacy-enhancing technologies to assist in the overall provision of privacy protection.

No a priori judgment can be made about the relative importance of each of these; all are necessary conditions for high quality information protection. None is a sufficient condition.

5.4.3 It is therefore clear that, though conceived as distinct rule sets, the legal, technological and market models of fair information practices are interdependent as tools for effective information protection. The different models/ instruments need to be channelled in the same direction so that the rules support each other rather than frustrate each other.²²⁹ PET's (privacy enhancing tools) is furthermore to be regarded as a useful complement to existing regulatory and self-regulatory approaches.²³⁰

5.4.4 In evaluating the different systems discussed above, the following points should be noted:

- * The Commission does not regard the self-regulatory system to be a suitable system for South Africa. In evaluating the responses it was clear that this option received very little support. The Commission furthermore agrees with the argument that large areas of information processing go unregulated in such a system, resulting in a confusing patchwork of provisions that reveals large gaps resulting in information protection that becomes "fragmented, incomplete, and discontinuous".²³¹ Under these circumstances, individuals' rights are difficult and costly to pursue.²³²
- * Over time it has also become clear that the existence of vigorous supervisory authorities are a sine qua non of good privacy protection inasmuch as laws are not self-implementing and the culture of privacy cannot securely establish itself

229 Reidenberg presentation 2001at 3.

230 Bennett and Raab *The Governance of Privacy* at 153 referring to PISA's (Privacy Incorporated Software Agent) project specification which says that "rather than relying on legal protection and self-regulation only, the protection of consumer's privacy is more effective if transactions are performed by means of technologies that are privacy enhancing". See also Principle 6 dealing with security, sec 18 of the proposed Act which refers to technical and organisational measures to be implemented by the responsible parties to secure information.

231 Reference by Bennett and Raab *The Governance of Privacy* to Gellman R "Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions" *Software Law Journal* 1993 Vol 6 199-231 at 238.

232 Bennett and Raab *The Governance of Privacy* at 105.

without an authoritative champion.²³³

- * The regulatory and co-regulatory system both make provision for a comprehensive act and a supervisory authority. The interaction between a supervisory authority, industry specific regulators and self-regulating adjudicators should be established clearly. It should, however, be noted that in co-regulating systems many sectors (especially small to medium industries) do not necessarily have adjudicators or regulators. Even if the co-regulatory system is adopted in a country, provision will therefore still have to be made for those industries without sector-specific adjudicators through a general supervisory authority.²³⁴ A sector-specific regulator, on the other hand, would also not be able to address problems in other sectors, once again leaving a gap that can only be filled by a supervisory authority.
- * It is envisaged that a single statutory regulatory authority will administer both the information privacy legislation and the access to information legislation.

5.4.5 The Commission's preliminary proposal is therefore that a comprehensive act should be instituted with or without sectoral legislation and codes of conduct, to be implemented within a regulatory system, implemented by a statutory regulatory authority working in conjunction with individual sectors.

5.4.6 The Commission therefore proposes that the information protection enforcement system be set out as follows:

²³³ Bennett and Raab *The Governance of Privacy* at 107.

²³⁴ Very few industries did in fact make use of the co-regulatory system in countries where it was available, reason being that the institution of an adjudicator was not found to be cost-effective and the fall-back system overseen by the regulatory authority seemed to be working well.

CHAPTER 5
SUPERVISION

Part A
Information Protection Commission

Establishment of Commission

34. *There is hereby established a body to be known as the Information Protection Commission.*

Constitution of Commission and period of office of members

35. (1)(a) *The Commission must consist of the following members, appointed by the State President -*

- (i) *a chairperson known as the Information Commissioner;*
- (ii) *two other persons known as ordinary members of the Commission.*

(b) *Members of the Commission must be appropriately qualified, fit and proper persons for appointment on account of the tenure of a judicial office or on account of experience as an advocate or as an attorney or as a professor of law at any university, or on account of any other qualification relating to the objects of the Commission.*

(c) *The chairperson of the Commission must perform his or her functions under this Act in a full-time capacity and must not be employed in any other capacity during any period in which the person holds office as Information Commissioner.*

(d) *The other members of the Commission must be appointed in a part-time capacity.*

(e) *The Chairperson must direct the work of the Commission and the Secretariat.*

(f) *No person will be qualified for appointment as a member of the Commission if that person –*

- (i) *is a member of Parliament;*
- (ii) *is a member of a local authority;*
- (iii) *is an unrehabilitated insolvent; or*
- (iv) *has at any time been convicted of any offence involving dishonesty.*

(2) *The State President may appoint one or more additional members if he deems it*

necessary for the investigation of any particular matter or the performance of any duty by the Commission.

(3) *The members of the Commission will be appointed for a period of not more than five years and will, at the expiration of such period, be eligible for reappointment.*

(4) *A person appointed as Information Commissioner may resign from office by writing under his or her hand addressed to the President and will in any case vacate office on attaining the age of seventy years.*

(5) *A member may be removed from office only for inability to discharge the functions of the office (whether arising from infirmity of body or mind or any other cause) or for misbehaviour.*

Remuneration, allowances, benefits and privileges of members

36. (1) *A member of the Commission who-*

(a) *is a judge of the Constitutional Court, the Supreme Court of Appeal or a High Court will, notwithstanding anything to the contrary contained in any other law, in addition to his or her salary and any allowance, including any allowance for reimbursement of travelling and subsistence expenses, which may be payable to him or her in his or her capacity as such a judge, be entitled to such allowance (if any) in respect of the performance of his or her functions as such a member as the President may determine;*

(b) *is not such a judge and is not subject to the provisions of the Public Service Act, 1994 (Proclamation 103 of 1994), will be entitled to such remuneration, allowances (including allowances for reimbursement of travelling and subsistence expenses incurred by him in the performance of his functions under this Act), benefits and privileges as the Minister in consultation with the Minister of Finance may determine.*

(2) *The remuneration, allowances, benefits or privileges of different members of the Commission may differ according to -*

(a) *the different offices held by them in the Commission; or*

(b) *the different functions performed, whether in a part-time or full-time capacity, by them from time to time.*

(3) *In the application of subsections (1) and (2), the President or the Minister, as the case may be, may determine that any remuneration, allowance, benefit or privilege contemplated in those subsections, will be the remuneration, allowance, benefit or privilege determined from time to*

time by or under any law in respect of any person or category of persons.

Secretary and staff

37.(1) The secretary of the Commission and such other officers and employees as are required for the proper performance of the Commission's functions, will be appointed in terms of the Public Service Act, 1994 (Proclamation 103 of 1994).

(2) The Commission may, with the approval of the Minister in consultation with the Minister of Finance, on a temporary basis or for a particular matter which is being investigated by it, employ any person with special knowledge of any matter relating to the work of the Commission, or obtain the co-operation of any body, to advise or assist the Commission in the performance of its functions under this Act, and fix the remuneration, including reimbursement for travelling, subsistence and other expenses, of such person or body.

Funds

38. Parliament will appropriate annually, for the use of the Commission, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Commission, of its powers, duties and functions under this Act.

Powers and duties of Commission²³⁵

39. (1) The powers and duties of the Commission will be---
education

- (a) to promote, by education and publicity, an understanding and acceptance of the information privacy principles and of the objects of those principles;*
- (b) for the purpose of promoting the protection of personal information, to undertake educational programmes on the Commission's own behalf or in co-operation with other persons or authorities acting on behalf of the Commission;*
- (c) to make public statements in relation to any matter affecting the protection of the*

²³⁵

The current proposal of the Law Commission is that the Information Commission will be responsible for the supervision of both the Promotion of Access to Information Act and the Protection of Personal Information Act. See Chapter 5 and para 4.2.207 in Chapter 4 of the discussion paper. Should this proposal be approved, the powers and duties of the Commission will be extended and PAIA amended accordingly.

personal information of a person or of any class of persons;

monitor compliance

- (d) *to monitor compliance by public and private bodies of the provisions of this Act;*
- (e) *to undertake research into, and to monitor developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of persons are minimised, and to report to the responsible Minister the results of such research and monitoring;*
- (f) *to examine any proposed legislation (including subordinate legislation) or proposed policy of the Government that the Commission considers may affect the protection of the personal information of individuals, and to report to the responsible Minister the results of that examination;*
- (g) *to report (with or without request) to the Minister from time to time on any matter affecting the protection of the personal information of a person, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the personal information of a person;*
- (h) *when requested to do so by a public or private body, to conduct an audit of personal information maintained by that body for the purpose of ascertaining whether or not the information is maintained according to the information privacy principles;*
- (i) *to monitor the use of unique identifiers of data subjects, and to report to the Minister from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the personal information of a person;*
- (j) *to maintain, and to publish, make available and provide copies of such registers as are prescribed in this Act.*
- (k) *to examine any proposed legislation that makes provision for -*
 - (i) *the collection of personal information by any public or private body; or*
 - (ii) *the disclosure of personal information by one public or private body to any other public or private body, or both; to have particular regard, in the course of that examination, to the matters set out in section 40(3) of this Act, in any case where the Commission considers*

that the information might be used for the purposes of an information matching programme; and to report to the responsible Minister the results of that examination;

consultation

- (l) to receive and invite representations from members of the public on any matter affecting the personal information of a person;*
- (m) to consult and co-operate with other persons and bodies concerned with the protection of information privacy;*
- (n) to act as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by one person in the interests of the protection of the personal information of another person;*
- (o) to provide advice (with or without a request) to a Minister or a public or private body on their obligations under the provisions, and generally, on any matter relevant to the operation, of this Act;*

complaints

- (p) to receive and investigate complaints about alleged violations of the protection of personal information of persons and in respect thereof make reports to complainants;*
- (q) to gather such information as in the Commission's opinion will assist the Commission in discharging the duties and carrying out the Commission's functions under this Act;*
- (r) to attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation;*
- (s) to serve any notices in terms of this Act and further promote the resolution of disputes in accordance with the prescripts of this Act;*

research and reporting

- (t) to report to the Minister from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a person;*

- (u) *to report to the Minister on any other matter relating to protection of information that, in the Commission's opinion, should be drawn to the Minister's attention;*

codes of conduct

- (v) *to issue, from time to time, codes of conduct, amendment of codes and revocation of codes of conduct;*
- (w) *to make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct;*
- (x) *to review an adjudicator's decision under approved codes of conduct;*²³⁶

general

- (y) *to do anything incidental or conducive to the performance of any of the preceding functions;*
- (z) *to exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commission by or under this Act or any other enactment.*

(2) *The Commission may, from time to time, in the public interest or in the interests of any person or body of persons, publish reports relating generally to the exercise of the Commission's functions under this Act or to any case or cases investigated by the Commission, whether or not the matters to be dealt with in any such report have been the subject of a report to the responsible Minister.*

Commission to have regard to certain matters

40. (1) *The Commission is independent in the performance of its functions.*

(2) *In the performance of its functions, and the exercise of its powers, under this Act, the Commission must -*

- (a) *have due regard to the protection of personal information as set out in the*

²³⁶

This section will only apply if the Act provides for the appointment of self-regulating adjudicators.

information protection principles; and

- (b) *have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way; and*
 - (c) *take account of international obligations accepted by South Africa, including those concerning the international technology of communications; and*
 - (d) *consider any developing general international guidelines relevant to the better protection of individual privacy.*
- (3) *In performing its functions in terms of sec 39(1)(k) of this Act with regard to information matching programmes, the Commission must have particular regard to the following matters -*
- (a) *whether or not the objective of the programme relates to a matter of significant public importance;*
 - (b) *whether or not the use of the programme to achieve that objective will result in monetary savings that are both significant and quantifiable, or in other comparable benefits to society;*
 - (c) *whether or not the use of an alternative means of achieving that objective would give either of the results referred to in paragraph (b) of this section;*
 - (d) *whether or not the public interest in allowing the programme to proceed outweighs the public interest in adhering to the information protection principles that the programme would otherwise contravene;*
 - (e) *whether or not the programme involves information matching on a scale that is excessive, having regard to -*
 - (i) *the number of agencies that will be involved in the programme; and*
 - (ii) *the amount of detail about an individual that will be matched under the programme;*

Programmes of Commission

41. (1) *In order to achieve its objects the Commission must from time to time draw up programmes in which the various matters which in its opinion require consideration are included in order of preference, and must submit such programmes to the Minister for approval.*

(2) *The Commission may include in any programme any suggestion relating to its objects*

received from any person or body.

(3) The Commission may consult any person or body, whether by the submission of study documents prepared by the Commission or in any other manner.

(4) The provisions of sections 2, 3, 4, 5 and 6 of the Commissions Act, 1947 (Act 8 of 1947), will apply *mutatis mutandis* to the Commission.

Protection of Commission

42. No criminal or civil proceedings lie against the Commission, or against any person acting on behalf or under direction of the Commission, for anything done, reported or said in good faith in the course of the exercise or performance or purported exercise or performance of any power, duty or function of the Commission under this Act.

Meetings of Commission

43.(1) Meetings of the Commission must be held at the times and places determined by the chairperson of the Commission.

(2) The majority of the members of the Commission will constitute a quorum for a meeting.

(3) The Commission may regulate the proceedings at meetings as it may think fit and must keep minutes of the proceedings.

Reports of Commission

44.(1) The Commission must prepare a full report in regard to any matter investigated by it and must submit such report to the Minister for information.

(2) The Commission must within five months of the end of a financial year of the Department for Justice and Constitutional Development submit to the Minister a report on all its activities during that financial year.

(3) The report referred to in subsection (2) must be laid upon the Table in Parliament within fourteen days after it was submitted to the Minister, if Parliament is then in session, or, if Parliament is not then in session, within 14 days after the commencement of its next ensuing session.

Committees of Commission

45.(1) The Commission may, if it deems it necessary for the proper performance of its functions-

- (a) establish a working committee, which must consist of such members of the Commission as the Commission may designate;

- (b) *establish such other committees as it may deem necessary, and which must consist of-*
 - (i) *such members of the Commission as the Commission may designate; or*
 - (ii) *such members of the Commission as the Commission may designate and the other persons appointed by the Minister for the period determined by the Minister.*
- (2) *The Minister may at any time extend the period of an appointment referred to in subsection (1) (b) (ii) or, if in his opinion good reasons exist therefor, revoke any such appointment.*
- (3) *The Commission must designate the chairman and, if the Commission deems it necessary, the vice-chairman of a committee established under subsection (1).*
- (4) (a) *A committee referred to in subsection (1) must, subject to the directions of the Commission, perform those functions of the Commission assigned to it by the Commission.*
 - (b) *Any function so performed by the working committee referred to in subsection (1) (a) will be deemed to have been performed by the Commission.*
- (5) *The Minister or the Commission may at any time dissolve any committee established by the Commission.*
- (6) *The provisions of sections 41(4) and 43 will mutatis mutandis apply to a committee of the Commission.*

Part B

Information Protection Officer²³⁷

Information protection officer to be appointed

- 46.(1) *Each responsible party must ensure that there are, within that body, one or more information protection officers whose responsibilities include -*
- (a) *the encouragement of compliance, by the body, with the information protection principles;*
 - (b) *dealing with requests made to the body pursuant to this Act;*
 - (c) *working with the Commission in relation to investigations conducted pursuant to Chapter 6 of this Act in relation to the body;*
 - (d) *otherwise ensuring compliance by the body with the provisions of this Act.*
- (2) *Officers must take up their duties only after the responsible party or body which appointed*

²³⁷

See sec 1 of PAIA for the definition of "information officer" and sec 17 regarding the designation of deputy information officers. It is envisaged that one officer should be designated in an organisation to deal with both privacy and information matters. It should be noted that PAIA does not currently make provision for the appointment of officers in private bodies. Comment is invited.

them has registered them with the Commission.

Comment is invited.

5.5 Notification, registration and licensing schemes

a) Introduction

5.5.1 A primary condition for effective information protection is that of transparency.²³⁸ Worldwide, responsible parties are enjoined to be open about their processing activities.²³⁹ This obligation may include the requirement to inform (and to receive authorisation from) the supervisory authority of their processing activities.²⁴⁰

5.5.2 We have seen above that there are three main categories to the rules monitoring the activities of responsible parties.²⁴¹ In some countries mere notification is necessary before processing may start. Others require registration and a third group insists on licensing as a precondition. A further requirement may be for the oversight authority to keep a register of the processing activities of which it has been informed.

5.5.3 In terms of the notification requirement responsible parties simply notify information protection authorities of certain planned processing of personal information. Upon notification, processing is usually allowed to begin. Most information protection laws, including the EU Directive operate with this sort of requirement, though the ambit of their respective notification schemes varies.²⁴²

5.5.4 Occasionally, the notification requirement is, or has been, formalised as a system for registration. Under this system, responsible parties must as a general rule apply to be registered with the information protection authority as a necessary precondition for their processing of personal information. When applying for registration, a responsible party is to supply the

²³⁸ See Principle 5: Openness as discussed in Chapter 4 para 4.2.125 above as well as the proposed clause 17(1).

²³⁹ See in this regard Principle 6 of the OECD Guidelines set out in fnnt 227in Chapter 4 above; See also Principle 3 of the UN Guidelines.

²⁴⁰ Bennett and Raab *The Governance of Privacy* at 99.

²⁴¹ Para 5.2.22.

²⁴² Bygrave *Data Protection* at 75.

authority with basic details of its intended processing operations.²⁴³

5.5.5 The final category requires that responsible parties must apply for and receive specific authorisation (in the form of a licence) from the relevant information protection authority prior to establishing a personal information register or engaging in a particular information-processing activity. Only a minority of countries operate, or have operated, with registered or comprehensive licensing schemes.²⁴⁴

5.5.6 The maintenance of national registers of responsible bodies is furthermore not a universal feature of information privacy laws, and there are many exemptions from such notification requirements where registers do exist. Over the years there has been an attempt to reduce the onerous burden placed on responsible parties by the obligation to notify or register their activities, whether through simplification or automation of the process, or through broadening the range of exemptions (eg in the UK and Germany).²⁴⁵ In countries with new legislation, lighter notification responsibilities have been established from the start. Registration has never been seriously considered in information protection regimes in North America or Australasia.²⁴⁶

5.5.7 Compliance with notification everywhere also remains very low indeed.²⁴⁷ One reason why notification is not more strongly pursued is that the information protection authorities in fact largely agree that the notified particulars are a very poor indication of what goes on in practice and that it adds little, if anything, to compliance with the more onerous requirements of the laws.

5.5.8 Many of the authorities would prefer to spend their resources on other measures which could contribute more effectively to compliance by responsible parties.²⁴⁸ It was argued²⁴⁹ that

²⁴³ Bygrave *Data Protection* at 75.

²⁴⁴ Sections 4-9 of the UK Act of 1984 (repealed); Sweden's Data Act of 1973 (repealed); French Act (in relation to the public sector).

²⁴⁵ In the UK a House of Commons select committee guessed in 1994 that about one third of controllers had failed to register. In Germany too, a system of central registration was considered "mere wishful thinking". In 1998 the system of registration in the UK under the 1984 Act was replaced by a scheme of notification; See also the problems experienced by the HRC in South Africa with the implementation of the disclosure provisions in terms of PAIA.

²⁴⁶ Bennett and Raab *The Governance of Privacy* at 99.

²⁴⁷ In the Netherlands there was found to be a discrepancy between the number of companies listed in the Companies Register and the number of responsible parties who notified their operations.

²⁴⁸ Korff *Comparative Study* at 170.

what matters for information protection is that the responsible parties respect the information protection rules when they process personal information and not that they send in papers to the oversight authority. The general perception worldwide is that bureaucracy should be contained²⁵⁰ and that the supervisory authority should concentrate its activities both on giving advice and spreading awareness about information protection and supervising compliance.²⁵¹

5.5.9 It would therefore seem as though a light notification system which provides the oversight authority with enough statistical and other information to be able to comply with its educational and monitoring functions will be sufficient.

5.5.10 Notification appears to serve three main purposes:²⁵²

- * it is helpful for data subjects because it is a major token of transparency in respect of the processing of personal information and can be the starting point for lodging a complaint with the competent authorities, via the controls carried out in the Register of processing operations (or of notifications);
- * it is helpful for responsible parties as it helps in raising their awareness of notification duties and keeps them “tuned” to the need for complying with information protection requirements;
- * it is helpful for information protection authorities because it allows them to keep abreast of the information processing situation in their countries (they can “feel the pulse”) and, at the same time, enables several analyses to be carried out (statistical or otherwise) with a view to refining the approach to recommendation, audits and inspections.²⁵³

5.5.11 As to the latter point, it should be clarified that a distinction should be drawn between notification for prior checking purposes (as per Article 20 of the Directive) and notification submitted for processing that is not subjected to prior checking (as per Article 18 of the

249 EU Article 29 Working Party “Report on the Obligation to Notify the National Supervisory Authorities on the Best Use of Exceptions and Simplification and the Role of the Data Protection Officers in the European Union” **WP 106** Adopted on 18 January 2005 (hereafter referred to as “**WP 106 on Notification**”) at 18 referring to the position in Sweden.

250 Roos thesies at 354 referring to Jay and Hamilton Data Protection 135 states as follows:” By the 1990’s the registration system came to be considered as ‘burdensome, bureaucratic and unnecessarily detailed’”.

251 See discussion below.

252 **WP 106 on Notification** at 6.

253 Register provides information for educational purposes.

Directive).²⁵⁴

b) Processing operations which must be notified

5.5.12 The system of notification as set out in Articles 18-21 of Directive 95/46/EC reflects the different traditions in the EU member states at the time the Directive was negotiated in the early nineties.^{255 256}

5.5.13 The Directive requires, subject to several derogations, that responsible parties or their representatives notify the authority concerned of basic information about any wholly or partly automatic processing operations they intend to undertake (Art 18(1)).²⁵⁷ Some countries extend the duty to notify processing operations also to all processing of information held in manual filing systems, some extend it to some manual systems while others provide for wide exemptions.²⁵⁸

5.5.14 It should be noted that even where processing is not required to be notified, such as most descriptions of manual processing, the responsible party is still under a duty to provide certain information to anyone making a written request. The purpose of this duty is to ensure transparency of processing even though not formally notified.

5.5.15 The general rule under the Data Protection Directive is that the duty of notification to the competent information protection authority is an obligation for all responsible parties. However, immediately after this general obligation, the Directive sets out extensive exemptions whose application is left to the discretion of the Member States. The idea is that some benign forms of automatic processing may be performed without the responsible party having an entry in the

²⁵⁴ See discussion below.

²⁵⁵ Whereas some relied heavily on notification and the keeping of registers, others sought to minimise these obligations or did have alternative systems in place.

²⁵⁶ **WP 106 on Notification** at 4.

²⁵⁷ Art 18 (1) provides as follows:
Obligation to notify the supervisory authority
 1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

²⁵⁸ Korff **Comparative Study** at 168.

register.²⁵⁹

5.5.16 The legal framework for the exemptions to the duty of notification is mainly provided for in paragraphs 2 to 5 of Article 18²⁶⁰ of the Directive. There is no Member State where at least some partial exemptions from notification obligations have not been implemented.²⁶¹

5.5.17 Besides these general exemptions, Article 9 of the Directive allows Member States to provide exceptions or derogations for the processing of personal information carried out solely for journalistic purposes or the purpose of artistic or literary expression. This might lead to an exemption to the duty of notification in these cases.²⁶²

5.5.18 The supervisory authorities therefore usually make an effort to exempt from the duty of notification routine business activities and similar activities (unsuitable administrative formalities) to the extent permitted, with the proviso that the processing would not have any significant impact upon privacy. This has led to a broad catalogue of exemptions and considerable simplification.²⁶³

²⁵⁹ Bainbridge *Data Protection* at 69.

²⁶⁰ Art 18(2) -(5) provides as follows:
 2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
 · where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
 · where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
 * for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
 * for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

²⁶¹ The exemption mechanism is useful in itself to allow data protection authorities to focus on really “dangerous” processing operations, i.e. those possibly jeopardising fundamental rights and freedoms.

²⁶² *WP 106 on Notification* at 8; see, however, the discussion on exemptions in Chapter 4 above.

²⁶³ The Netherlands is a good example of the extensive reliance on certain categories of processing exemptions. As stipulated in article 43 of the Exemption Decree, some combinations of exempted processing operations are also exempted. In addition to that, the Data Protection Authority and the Ministry of Justice are currently reviewing the possibility to further extend the list of exemptions.

5.5.19 The Art 29 Working Party of the EU was requested to investigate possible means of providing further simplification to the duty of notification in the Member States. In its report²⁶⁴ it confirmed the importance of having notification as a general requirement but identified best practices as regards the duty of notification to be followed.²⁶⁵

5.5.20 As a general rule failure to notify is regarded as a criminal offence of strict liability.²⁶⁶

c) Notifiable particulars and publication of particulars

5.5.21 With some exceptions the types of information to be notified must include at least the name and address of the responsible party and of his representative, if any; the purpose of the processing; a description of the category of data subject and of the information relating to them; the recipients to whom the information might be disclosed; proposed transfers of information to third countries; and a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing(Art 19).²⁶⁷

²⁶⁴ *WP 106 on Notification.*

²⁶⁵ *WP 106 on Notification* at 4. In its recommendations at 22 the Art 29 Working Committee stated that:

- * If amendments to the existing legal framework were envisaged, notification as a general requirement should not be eliminated.
- * However, the Article 29 Working Party invites the Member States to make good use of the possibilities for exceptions and simplification available under the Directive and, where this is not yet the case, recommends Member States to empower the data protection authorities with appropriate regulatory powers to implement these exceptions accordingly.
- * Notification should be regarded as a means to draw the responsible parties' attention to the need for abiding by data protection legislation. However, notification should not be just another bureaucratic step.
- * States should enhance and pursue the userfriendly approach that is de facto adopted by Member States in dealing with notification requirements. This means enhancing the implementation of electronic and online notification mechanisms. Furthermore, the use of ready-made lists of purposes/data categories as already available in several Member States should be enhanced as this can reduce errors and harmonise notifications.
- * Data Protection authorities within the Article 29 Working Party agree on the need to streamlining the exemption system.

²⁶⁶ Bainbridge *Data Protection* at 67 for UK example.

²⁶⁷ Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:
 - (a) the name and address of the controller and of his representative, if any;
 - (b) the purpose or purposes of the processing;
 - (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
 - (d) the recipients or categories of recipient to whom the data might be disclosed;
 - (e) proposed transfers of data to third countries;
 - (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

5.5.22 To the extent that they require notification, the states list (at least) all the matters mentioned in Art. 19(1)(a) – (f) of the Directive, quoted above; and they all of course also stipulate that if such aspects of a processing operation change, the change too must be reported. However, they differ considerably in their specification of additional notifiable particulars.²⁶⁸

5.5.23 All the EU member states provide for the establishment of a publicly accessible register of processing operations, containing all the notified particulars, except for details of the security measures taken by responsible parties in accordance with the Directive. The contents of these registers will vary because of the differences in the notifiable particulars.²⁶⁹

5.5.24 The register must be open for inspection to any person. Where the processing is not subject to notification, the responsible party or authority must make the relevant information available on request.²⁷⁰ Whereas these registers used to be available at the Offices of the oversight authority, they are lately made available for inspection on the Internet at the oversight agency's web site.²⁷¹

d) Prior checking

5.5.25 “Prior checks” or requirements that responsible parties obtain the “prior authorisation” of

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority. The register shall contain at least the information listed in Article 19 (1) (a) to (e). The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request. Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide of a legitimate interest.

²⁶⁸ Korff *Comparative Study* at 173.

²⁶⁹ Ibid.

²⁷⁰ Roos thesis at 725.

²⁷¹ Bainbridge *Data Protection* at 74 for UK example.

their national information protection authority, are the strictest form of control over processing operations.

5.5.26 The EU Directive allows for a system of “prior checking” by national information protection authorities with respect to processing operations that are likely to present specific risks to the rights and freedoms of data subjects (Art 20(1)).²⁷²

5.5.27 Elaborating on what might constitute such processing operations, recital 53 refers to operations that are likely to pose specific risks “by virtue of their nature, their scope or their purposes, such as excluding individuals from a right, benefit or contract, or by virtue of the specific use of new technologies”.²⁷³

5.5.28 The system is most widely developed in France, where (under the current, pre-implementation law) all processing operations in the public sector must be based on a *regulation*, adopted after the information protection authority has first given its “advice” - which in practice comes close to a “prior check”.

5.5.29 In the UK the term “assessable processing” is used. The Commissioner will consider the processing and give written notice to the responsible party stating whether and to what extent the processing is likely or unlikely to comply with the provisions of the Act.²⁷⁴ However, no processing have to date been made subject to a “prior check” in the UK (even though the 1998 law does provide for the possibility).²⁷⁵

5.5.30 There are substantial differences between the EU member states as concerns the kinds of operations for which they stipulate such prior formalities. Examples are the processing of

²⁷²

Art 20(1) provides as follows:

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

²⁷³

WP 106 on Notification at 3.

²⁷⁴

Bainbridge *Data Protection* at 78.

²⁷⁵

Korff *Comparative Study* at 173.

sensitive information, processing for the purpose of credit referencing, and processing involving interconnections between different databases. It is also required for the processing by private-sector entities, staff recruitment agencies, processing for the keeping of legal information systems, or for the transfer of sensitive information to third countries without adequate protection.²⁷⁶

5.5.31 In the Netherlands, a “prior check” must be carried out for the use of an identification number for a different purpose than the one for which the number is intended, in order to match information with information processed by a different responsible party; for the recording of information obtained through a responsible party’s own observations (which include both secret video surveillance and the capturing of Internet or intranet activities) if the data subject is not informed of this; and for the processing of information on criminal-legal matters etc., other than by licenced detective agencies.²⁷⁷

5.5.32 It would appear from Art 28(3) of the Directive, together with recitals 9, 10 and 54 that information protection authorities may stop planned information-processing operations pursuant to this system of “prior checking”.²⁷⁸

5.5.33 Recital 54 makes it clear, though, that such a system is to apply only to a minor proportion of information processing operations: with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited. In other words, information protection regimes in which prior checking is the rule rather than exception do not conform with the Directive.²⁷⁹

5.5.34 In some sectors, the obtaining of prior opinions or prior checks, or prior authorisations or permits does become the norm, especially if (a) failure to obtain such a permit can lead to the loss of a licence and (b) the information protection authority puts in a concerted effort to convince those in the sector of the serious repercussions that failure to comply with the required formality may entail. It also helps if the sector in question is not too large. Purely because of resource implications, such a system must, however, by its nature, be limited to selected areas or kinds of

²⁷⁶ Korff *Comparative Study* at 174.

²⁷⁷ Ibid.

²⁷⁸ *WP 106 on Notification* at 3.

²⁷⁹ *WP 106 on Notification* at 4.

responsible parties.²⁸⁰

e) In-house officials

5.5.35 Article 18 (2) of the Directive²⁸¹ allows Member States to exempt responsible parties from notification duties where “the responsible party, in compliance with the national law which governs him, appoints a personal information protection official, responsible in particular:

- * For ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive;
- * For keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2) (...).²⁸²

5.5.36 The main task of the in-house official is to ensure compliance with the Law and any other information protection-relevant legal provisions in all the personal information processing operations of his employer or principal. To this end, the responsible party must provide the official with an overview of its processing operations, which must include the information which (if it was not for the fact that the responsible party has appointed an in-house official) would have had to be notified to the authorities (as discussed below, under the heading notification) as well as a list of persons who are granted access to the various processing facilities. In practice, it is often the first task of the official to compile this information, and suggest appropriate amendments (e.g., clearer definitions of the purpose(s) of specific operations, or stricter rules on who has access to which information). Once an official has been appointed, new planned automated processing operations must be reported to him or her before they are put into effect. The official’s tasks also include verifying the computer programmes used in this respect; and training the staff working with personal information. More generally, the official is to advise the responsible party on relevant operations, and to suggest changes where necessary. This is a delicate matter, especially if the legal requirements are open to different interpretations. The official may, “in

²⁸⁰ Korff *Comparative Study* at 175.

²⁸¹ Art 18(2) provides as follows:
2. Member States may exempt controllers from notification where] the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- * For ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive.
- * For keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2), thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

²⁸² This alternative to notification provided by the Directive is currently implemented in Germany, the Netherlands, Sweden, Luxembourg and France.

cases of doubt” contact the relevant supervisory authority. However (except in the special context of a “prior check”), this is not obligatory.²⁸³

5.5.37 The Dutch Data Protection Act stipulates that if there is a privacy officer, notifications can be done to the privacy officer (thus not to the data protection authority). The Dutch Data Protection Authority has developed a special notification programme for privacy officers. This adapted version of the notification programme offers the privacy officer the possibility to further process the notifications within an own database and/ or intranet of the organisation.²⁸⁴

5.5.38 It is the Commission’s preliminary recommendation that a system of light notification (subject to exemptions) and prior investigation be implemented. However, since the Information officer contemplated in Chapter 5 above is appointed by the responsible party and not by the Commission and is not subject to independence requirements, an exemption in this regard has been excluded. It will be an offence to process personal information without notification unless the processing is exempt from notification and liability will be strict. Comment is invited on all of these proposals. The proposed legislative enactment will read as follows:

²⁸³ Korff *Comparative Study* at 176.

²⁸⁴ About 165 privacy officers are currently installed. The Dutch authority expects this number to increase further. They are active in all sectors of society. Examples are banks, insurance companies, trade unions, financial regulatory bodies, schools, hospitals, municipalities, ministries, and a variety of big and medium-size business.

CHAPTER 6
NOTIFICATION AND PRIOR INVESTIGATION

Part A
Notification

Processing to be notified to Commission

47. (1) The fully or partly automated processing of personal information intended to serve a single purpose or different related purposes, must be notified to the Commission before the processing is started.

(2) The non-automated processing of personal information intended to serve a single purpose or different related purposes, must be notified where this is subject to a prior investigation.

Notification to contain specific particulars

48. (1) The notification must contain the following particulars -

(a) the name and address of the responsible party;

(b) the purpose or purposes of the processing;

(c) a description of the categories of data subjects and of the information or categories of information relating thereto;

(d) the recipients or categories of recipients to whom the information may be supplied;

(e) planned cross-border transfers of information;

(f) a general description allowing a preliminary assessment of the suitability of the planned information security measures to be implemented by the responsible party, intended to safeguard the confidentiality, integrity and availability of the information which is to be processed.

(2) Changes in the name or address of the responsible party must be notified within one week and changes to the notification which concern (1)(b) to (f) must be notified in each case within one year of the previous notification, where they appear to be of more than incidental importance.

(3) Any processing which departs from that which has been notified in accordance with the provisions of (1)(b) to (f) must be recorded and kept for at least three years.

(4) More detailed rules can be issued by or under regulation concerning the procedure for submitting notifications.

Exemptions to notification requirements

49.(1) It may be laid down by regulation that certain categories of information processing which are unlikely to infringe the fundamental rights and freedoms of the data subject, are exempted from the notification requirement referred to in section 47.²⁸⁵

(2). Where it is necessary in order to detect criminal offences in a particular case, it may be laid down by regulation that certain categories of processing by responsible parties who are vested with investigating powers by law, are exempt from notification.

(3) The notification requirement does not apply to public registers set up by law or to information supplied to an administrative body pursuant to a legal obligation.

Register of information processing

50.(1) The Information Protection Commission must maintain an up-to-date register of the information processing notified to it, which register must contain, as a minimum, the information provided in accordance with section 48(1)(a) to (f).

(2) The register may be consulted by any person free of charge.

(3) The responsible party must provide any person who so requests with the information referred to in section 48(1)(a) to (f) concerning information processing exempted from the notification requirement.

(4) The provisions of subsection (3) do not apply to -

(a) information processing which is covered by an exemption under Chapter 4.

(b) public registers set up by law.

Failure to notify

²⁸⁵

It is envisaged that the exemptions granted to certain categories of bodies from the provisions set out in Chapter 2 (publication and availability of certain records) of PAIA will also be applicable in so far as the notification requirements in terms of this Act are concerned.

51. (1) If section 47(1) is contravened, the responsible party is guilty of an offence.
- (2) Any person who fails to comply with the duty imposed by notification regulations made by virtue of section 96 is guilty of an offence.

Part B

Prior investigation

Processing subject to prior investigation

52. (1) The Commission must initiate an investigation prior to any processing for which responsible parties plan to -

(a) process a number identifying persons for a purpose other than the one for which the number is specifically intended with the aim of linking the information together with information processed by other responsible parties, unless the number is used for the cases defined in Chapter 4,²⁸⁶

(b) process information on criminal behaviour or on unlawful or objectionable conduct for third parties;

(c) process information for the purposes of credit reporting; and

(d) transfer special personal information, as referred to in section 24, to third countries without adequate information protection laws.

(2) The provisions of subsection (1) may be rendered applicable to other types of information processing by law or regulation where such processing carries a particular risk for the individual rights and freedoms of the data subject.

Responsible party to notify Commission where processing is subject to prior investigation

53. (1) Information processing to which section 52 (1) is applicable must be notified as such by the responsible party to the Commission.

(2) The notification of such information processing requires responsible parties to suspend the processing they are planning to carry out until the Commission has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

²⁸⁶

Exemptions.

(3) *In the case of the notification of information processing to which section 52 (1) is applicable, the Commission must communicate its decision in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.*

(4) *In the event that the Commission decides to conduct a more detailed investigation, it must indicate the period of time within which it plans to conduct this investigation, which period must not exceed thirteen weeks.*

(5) *The more detailed investigation referred to under (4) leads to a statement concerning the lawfulness of the information processing.*

(6) *The statement by the Commission is deemed to be equivalent to an enforcement notice served in terms of sec 83 of this Act.*

5.6 Codes of conduct

5.6.1 As noted above, codes of conduct are found in all the privacy systems discussed above.²⁸⁷ Since the Commission has, however, already indicated its preference for a regulatory system, the discussion in this section will be restricted to codes of conduct as found within this system. Five kinds of privacy code can be identified²⁸⁸ according to the scope of application: organisational code²⁸⁹, the sectoral code,²⁹⁰ the functional code²⁹¹, the professional code²⁹² and the technological code²⁹³.

²⁸⁷ See para 5.2.10-5.2.13 (regulatory system), paras 5.2.49 - 5.2.53 (self-regulatory system) and para 5.2.69-5.2.73 (co-regulatory system). See also section 13 of the Irish Act; Parts VI-VII of the New Zealand Privacy Act, 1993; section 51(3) and (4) of the UK Data Protection Act, 1998; Part IIIAA of the Australian Privacy Act, 1988 and Article 25 of the Dutch Personal Data Protection Act.

²⁸⁸ Raab presentation 2002 at 9-11. See also Bennett and Raab *The Governance of Privacy* at 123-126.

²⁸⁹ This applies to one agency that is bound by a clear organisational structure.

²⁹⁰ The defining feature of a sectoral code is that there is a broad consonance of economic interest and function and a similarity in the kinds of personal information collected. Examples are the banking industry, life insurance etc.

²⁹¹ This code is defined less by the economic sector and more by the practice in which the organisation is engaged, for example direct mail and marketing. The Direct Marketing Association in South Africa, for instance, represents businesses in a wide number of sectors.

²⁹² Codes developed for those directly involved in information processing activities eg market researchers, and health professionals.

²⁹³ As new potentially intrusive technologies have entered society, codes have developed to deal with their specific application.

5.6.2 The EU Directive clearly provides for the use of codes of conduct.²⁹⁴ To contribute to the proper implementation of the Directive at the national level, Article 27 of the Directive²⁹⁵ directs the EU member states and the EU Commission to encourage the development of codes of conduct. EU member states are required to facilitate the approval procedure of draft codes and amendments or extensions to existing codes prepared by trade associations and other bodies. Organisations representing certain industry sectors, and established in multiple Member States, may furthermore submit draft Community codes, and amendments or extensions to existing Community codes, to the Article 29 Working Party to determine whether the drafts comply with the Directive.²⁹⁶

5.6.3 The OECD Guidelines, furthermore, provide that member countries should encourage and support self-regulation, whether in the form of codes of conduct, or otherwise.²⁹⁷

5.6.4 Codes of conduct are, therefore, seen as a useful means to clarify the application of information protection law in a particular sector, and can also be used as an alternative to sectoral regulation.²⁹⁸ In theory, the drafting of codes should be a simpler, more flexible means to achieve the same end, the laying down of sector-specific rules applying the more general information protection rules.²⁹⁹ It furthermore has the advantage that, once negotiated, the codes

²⁹⁴ The Directive does not, however, provide any indication of the exact legal status to be provided to such codes.

²⁹⁵ Article 27
 1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
 2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority. Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.
 3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

²⁹⁶ Wugmeister M, Retzer K & Rich C "Codes of Conduct: The Solution for International Data Transfers?" *Morrison & Foerster Legal Updates & News* July 2003 (Article first published in WDPR, June 2003, reprinted with permission of publisher) accessed at http://www.mofo.com/tools/print.asp?mofo_dev/news/updates/files/update1170.html (hereafter referred to as Wugmeister et al *Codes of Conduct*).

²⁹⁷ Paragraph 19(b) OECD Guidelines. Paragraph 19(b) is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action.

²⁹⁸ See sections 15 and 16 of the Financial Advisory and Intermediary Services Act 37 of 2002 for an example of the successful use of codes of conduct to regulate different sectors of the financial services industry.

²⁹⁹ Korff *Comparative Study* at 196.

can be adapted to changing economic and technological developments.³⁰⁰

5.6.5 A substantial portion of a code of conduct should therefore deal explicitly with the information privacy principles, covering how compliance with each principle is to be secured. Some of the principles will bear more heavily on some sectors than others and will require more detailed consideration.³⁰¹

5.6.6 Codes will typically be promoted or initiated by trade associations, representative or professional bodies or Government departments, and will cover the application of the information privacy principles to particular groups of “agencies” (eg health sector, law enforcement agencies, direct marketing companies etc) or for particular types of information (eg. employment information, credit information). The Information Commissioner may also initiate codes of practice.³⁰²

5.6.7 While it is preferable for codes to emanate from the representative associations themselves, the Commission will be free to initiate codes of conduct wherever it is considered that the best interests of data subjects so require. Naturally, any actions in this area will have to be on the basis of full consultation with all interests affected, including both representative bodies and the public more generally.³⁰³

5.6.8 The Commission may, however, prefer to rely on the issuing of its own sectoral rules (rather than on leaving the initiative, at least initially, to the sectors concerned). In several countries some specific sectors are already regulated in some detail in the law or in regulations issued under the law (e.g., the direct marketing- and credit reference sectors) - but elsewhere (e.g. in the UK) the possibility of issuing State-imposed sectoral rules is regarded more as a “stick behind the door”, to be used only if a sector does not itself put forward adequate rules.³⁰⁴

5.6.9 In practice, self-regulation and State-imposed sectoral regulation are not as different as one might expect: self-regulation increasingly takes place in a legal framework which allows for,

³⁰⁰ Bennett and Raab *The Governance of Privacy* at 113.

³⁰¹ Office of the New Zealand Privacy Commissioner **Draft Guidance Note on Codes of Practice under Part VI of the Privacy Act** Issue No. 5 dated 5 December 1994 (hereafter referred to as “NZ *Codes of Practice Guidance note*”) at 3.

³⁰² NZ *Codes of Practice Guidance note* at 2.

³⁰³ Korff *Comparative Study* at 197 with reference to the Irish Commissioner in his 2001 Annual Report.

³⁰⁴ *Ibid.*

or indeed requires, the assessment and/or approval of “voluntary” codes, while State regulation may involve the drawing up of rules in consultation with (or even by) sectoral organisations.³⁰⁵

5.6.10 The development and adoption of a code by an organisation could be used to send a powerful message to consumers that the organisation is conscious of the privacy concerns of individuals and is active in protecting their privacy rights.³⁰⁶ They also allow organisations to remove suspicions about the improper collection, processing and dissemination of personal information that may exist and thereby facilitate an “enhanced measure of understanding on both sides.”³⁰⁷

5.6.11 As discussed above, there are three different models that have evolved in those countries that use privacy codes:

- a) The first, and in many ways most stringent, is represented by the system under the New Zealand Privacy Act. The crucial aspect of the New Zealand approach is that codes of practice negotiated under the Privacy Act have the force of law. A breach of a ratified code of practice is as serious as a breach of the information privacy principles expressed in the law, which would then trigger the complaints and enforcement procedures in the legislation.
- b) The second, slightly more flexible regime, exists in the Netherlands. Although the Dutch system is similar in most respects to that in New Zealand, the codes are not formally binding on the courts. If an organisation can prove that it has met the requirements of its code, it will have a strong case. Conversely, a complainant’s demonstration that the provisions of the code have been breached constitutes prima facie evidence of liability under the law. Codes therefore, have indirect, rather than direct legal effect.³⁰⁸

305 Korff *Comparative Study* at 196.

306 Malcolm Crompton, Federal Privacy Commissioner of Australia in his forward to the *Guidelines on Privacy Code Development* published by the Office of the Federal Privacy Commissioner September 2001. See also the reference to other reasons for developing a code set out at 18 of the same document: a code may -

- * be a good way of changing the culture of an organisation or industry by raising awareness of privacy and by introducing a compliance regime;
- * serve as a guide to regulation by providing industry standards written in industry specific language. It is often quicker and easier to amend codes than it is to amend the law, allowing organisations to keep up with developments and respond to concerns.

307 Bennett and Raab *The Governance of Privacy* at 113 referring to Hustinx P “The Use and Impact of Codes of Conduct in the Netherlands” Paper presented to the 16th Conference of Data Protection Commissioners, The Hague, 1994.

308 To date, the Dutch Data Protection Authority (“DPA”) has approved fifteen codes of conduct, mainly in the financial services, pharmaceutical, and direct marketing services sector that can be used to satisfy national requirements for the

- c) In other countries, such as the UK and Canada, the law simply empowers the Commissioner concerned to encourage the development of codes as a further instrument of compliance with the law. Indeed, this is all that is expected by the EU Directive.³⁰⁹

5.6.12 In Europe the stipulations in the Directive confirm a trend towards what one may call *quasiself-regulation* (whereby it may be noted that the paragraph concerning Community Codes clearly envisages the “approval” of such codes, while the paragraphs concerning national codes refer more vaguely to the obtaining of an “opinion”). The laws in all the EU Member States now include provisions on the drafting of self-regulatory codes of conduct. In most, the laws refer to the “checking” or “assessing” of the compatibility of the code with the law; to the issuing of an “opinion” on that conformity; or to the drawing up of codes “*in cooperation*” with the information protection authority.³¹⁰

5.6.13 A certain tension has been noted in the EU between the views taken of codes by industry and regulators. The former sometimes feel that the latter are too rigorous in their initial assessments of draft codes submitted for an “opinion”, while the latter sometimes feel that the former are trying to use codes as a means to evade certain strict rules in the law. The process for obtaining an “opinion” or assessment is consequently often long (as is also the case, it may be noted, with regard to the approval of Community Codes).³¹¹

5.6.14 It has been argued that where a formal ratification process is laid out, as in New Zealand and the Netherlands, this can bureaucratise a process that, in theory, is supposed to allow the flexibility of self-regulation. Another problem encountered is that the submission of the codes in some sectors may be hindered by competition within the sector, and by unclear boundaries and overlaps that weaken the claim that the association submitting the code is sufficiently “representative”.³¹²

processing of personal data. These codes are used to promote compliance with sector specific data protection requirements.

309 Bennett and Raab *The Governance of Privacy* at 113.

310 Ibid.

311 Ibid. Note that some codes modify the application of the Information Privacy Principles (prescribing more stringent or less stringent standards or by exempting actions). This is the position in New Zealand. In Australia the law stipulates that the codes should be at least the equivalent of the privacy principles as stated in the Act. The current proposal for South Africa is that the codes should be the exact equivalent of the privacy principles.

312 Bennett and Raab *The Governance of Privacy* at 113.

5.6.15 The following guidance have been given on the matters that should be addressed in particular in acceptable codes of conduct:³¹³

- * what type of personal information is covered;
- * for what purpose is this information processed;
- * how is the personal information obtained;
- * how can the personal information be processed;
- * to whom will the personal information be disclosed; and
- * for how long will the personal information be retained.

5.6.16 A code of conduct will furthermore include provisions for:³¹⁴

- * commencement, review and expiry of the code;
- * a precise definition of the scope or application of the code;
- * a complaints procedure and how individuals can exercise any rights flowing from the code. Depending on the nature of the particular sector, this may range from an independent complaints mechanism to an obligation for the privacy officer of a body to reconsider any complaint received or a senior person independent of the person whose decision is complained about.

5.6.17 Particular procedures for the adoption of codes of conduct may differ in various countries, as do the status for such codes. However, it might be advisable to stress that the process for adopting draft codes should not be too cumbersome (whereby it could be added that the operation of a code in practice can be, and should be, kept under review).³¹⁵

5.6.18 Organisations need to be aware, however, that to develop and implement a privacy code requires a commitment of resources. Costs will vary from scheme to scheme, with the establishment of a complaint handling body adding substantially to the resource requirements.³¹⁶

³¹³ Korff *Comparative Study* at 198.

³¹⁴ NZ *Codes of Practice Guidance Note* at 4.

³¹⁵ Korff *Comparative Study* at 198.

³¹⁶ Office of the Federal Privacy Commissioner Australia *Guidelines on Privacy Code Development* September 2001 (hereafter referred to as "Australian *Privacy Code Guidelines*") at 20.

5.6.19 An exciting new development to be noted³¹⁷ is that a code of conduct approach is developing to cross-border information transfers.³¹⁸ More and more companies are pushing for the development of global codes that would govern their global information processing practices and at the same time facilitate all their international information transfers. Given the growing number of cross-border information transfers, the idea of relying on global rules for all cross-border information transfers is attractive.³¹⁹

5.6.20 It is the Commission's preliminary recommendation that provision should be made in the proposed legislation for the development of codes of conduct in appropriate circumstances. This would contribute to the proper implementation of the information protection principles in each sector. In order to facilitate the enforcement of the provisions set out in the codes, it is further recommended that the codes should have legal binding powers on the bodies to which it will apply. Comment is invited. The legislative enactment of this provision will read as follows:

³¹⁷ Especially in so far as South Africa's trade with the rest of Africa is concerned.

³¹⁸ Wugmeister *Codes of Conduct* et al at 1.

³¹⁹ See further discussion on cross-border data transfers at Chapter 7 below.

CHAPTER 7
CODES OF CONDUCT

Issuing of codes of conduct

54. (1) *The Commission may from time to time issue a code of conduct.*

(2) *A code of conduct must---*

(a) *incorporate all the information protection principles or set out obligations that, overall, are the equivalent of all the obligations set out in those principles; and*

(b) *prescribe how the information protection principles are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which these bodies are operating.*

(3) *A code of conduct may apply in relation to any one or more of the following -*

(a) *any specified information or class or classes of information;*

(b) *any specified body or class or classes of bodies;*

(c) *any specified activity or class or classes of activities;*

(d) *any specified industry, profession, or calling or class or classes of industries, professions, or callings.*

(4) *A code of conduct must also---*

(a) *impose, in relation to any body that is not a public body, controls in relation to the comparison (whether manually or by means of any electronic or other device) of personal information with other personal information for the purpose of producing or verifying information about an identifiable person;*

(b) *provide for the review of the code by the Commission;*

(c) *provide for the expiry of the code.*

Proposal for issuing of code of conduct

55. (1) *The Commission may issue a code of conduct under section 54 of this Act on the Commission's own initiative or on the application of any person.*

(2) *Without limiting subsection (1) of this section, but subject to subsection (3) of this section, any person may apply to the Commission for the issuing of a code of conduct in the form submitted by the applicant.*

(3) *An application may be made pursuant to subsection (2) of this section only -*

(a) by a body which is, in the opinion of the Commission, sufficiently representative of any class or classes of bodies, or of any industry, profession, or calling as defined in the code; and

(b) where the code of conduct sought by the applicant is intended to apply in respect of the class or classes of body, or the industry, profession, or calling, that the applicant represents, or any activity of any such class or classes of body or of any such industry, profession, or calling.

(4) Where an application is made to the Commission pursuant to subsection (2) of this section, or where the Commission intends to issue a code on its own initiative, the Commission must give public notice in the Gazette that the issuing of a code of conduct is being considered, which notice must contain a statement that -

(a) the details of the code of conduct being considered, including a draft of the proposed code, may be obtained from the Commission; and

(b) submissions on the proposed code may be made in writing to the Commission within such period as is specified in the notice.

(5) The Commission must not issue a code of conduct unless it has considered the submissions made to the Commission in terms of subsection (4) and is satisfied that all persons affected by the proposed code has had a reasonable opportunity to be heard.

(6) The decision as to whether an application for the issuing of a code has been successful must be made within a reasonable period of time which must not exceed fourteen weeks.

Notification, availability and commencement of code

56. (1) Where a code of conduct is issued under section 54 of this Act,---

(a) the Commission must ensure that there is published in the Gazette, as soon as reasonably practicable after the code is issued, a notice---

(i) indicating that the code has been issued; and

(ii) indicating where copies of the code are available for inspection free of charge and for purchase; and

(b) The Commission must ensure that so long as the code remains in force, copies of the code are available -

(i) for inspection by members of the public free of charge; and

(ii) *for purchase by members of the public at a reasonable price.*

(2) *Every code of conduct issued under section 54 of this Act comes into force on the 28th day after the date of its notification in the Gazette or on such later day as may be specified in the code and is binding on every class or classes of body, industry, profession or calling referred to therein.*

Amendment and revocation of codes

57. (1) *The Commission may from time to time issue an amendment or revocation of a code of conduct issued under section 54 of this Act.*

2) *The provisions of sections 54 to 58 of this Act must apply in respect of any amendment or revocation of a code of conduct.*

Procedure for dealing with complaints

58. (1) *The code may prescribe procedures for making and dealing with complaints alleging a breach of the code, but no such provision may limit or restrict any provision of Chapter 8 (Complaints and proceedings by the Commission) of this Act;*

(2) *If the code sets out procedures for making and dealing with complaints, the Commission must be satisfied that:*

- (a) *the procedures meet the:*
 - (i) *prescribed standards; and*
 - (ii) *Commission's guidelines (if any) in relation to making and dealing with complaints; and*
- (b) *the code provides for the appointment of an independent adjudicator to whom complaints may be made; and*
- (c) *the code provides that, in performing his or her functions, and exercising his or her powers, under the code, an adjudicator for the code must have due regard to the matters that section 40(2) requires the Commission to have due regard to; and*
- (d) *the code requires a report (in a form satisfactory to the Commission) to be prepared and submitted to the Commission within five months of the end of a financial year of the Department for Justice and Constitutional Development on the operation of the code during that financial year; and*

- (e) *the code requires the report prepared for each year to include the number and nature of complaints made to an adjudicator under the code during the relevant financial year.*
- (3) *A person who is aggrieved by a determination, including any finding, declaration, order or direction that is included in the determination, made by an adjudicator (other than the Commission) under an approved code of conduct after investigating a complaint may apply to the Commission for review of the determination.*
- (4) *The adjudicator's determination continues to have effect unless and until the Commission makes a determination under Chapter 8 relating to the complaint.*

Guidelines about codes of conduct

59. (1) *The Commission may provide written guidelines -*

- (a) *to assist bodies to develop codes of conduct or to apply approved codes of conduct; and*
- (b) *relating to making and dealing with complaints under approved codes of conduct; and*
- (c) *about matters the Commission may consider in deciding whether to approve a code of conduct or a variation of an approved code of conduct.*

(2) *Before providing guidelines for the purposes of paragraph (1)(b), the Commission must give everyone the Commission considers has a real and substantial interest in the matters covered by the proposed guidelines an opportunity to comment on them.*

(3) *The Commission may publish guidelines provided under subsection (1) in any way the Commission considers appropriate.*

Register of approved codes of conduct

60. (1) *The Commission must keep a register of approved codes of conduct.*

(2) *The Commission may decide the form of the register and how it is to be kept.*

(3) *The Commission must make the register available to the public in the way that the Commission determines.*

(4) *The Commission may charge reasonable fees for:*

- (a) *making the register available to the public; or*
- (b) *providing copies of, or extracts from, the register.*

Review of operation of approved code of conduct

61. (1) *The Commission may review the operation of an approved code of conduct.*

(2) *The Commission may do one or more of the following for the purposes of the review:*

- (a) *consider the process under the code for making and dealing with complaints;*
- (b) *inspect the records of an adjudicator for the code;*
- (c) *consider the outcome of complaints dealt with under the code;*
- (d) *interview an adjudicator for the code;*
- (e) *appoint experts to review those provisions of the code that the Commission believes require expert evaluation.*

(3) *The review may inform a decision by the Commission under section 57 to revoke the approved code of conduct with immediate effect or at a future date to be determined by the Commission.*

Effect of code

62. *Where a code of conduct issued under section 54 of this Act is in force, failure to comply with the code, must, for the purposes of Chapter 8 of this Act, be deemed to be a breach of an information protection principle.*

5.7 Information matching (profiling)

5.7.1 It has already been established that the mere collecting and storing of information may constitute an infringement of a subject's right to privacy if it is an unreasonable act. A further, more serious infringement, may occur where information which relates to the individual is structured in such a way that it can begin to answer questions about that person, so as to put his or her private behaviour under surveillance. This practice is referred to as information matching or profiling.

5.7.2 One example where profiling is used for ordinary marketing purposes is where a process referred to as information mining, enables the retailer to engage in targeted marketing. An on-line

bookstore might offer a customer recommendations based on what the customer has bought in the past, or looked at on the web site, usually other books by the same author or on the same subject.³²⁰

5.7.3 Another example, with more serious consequences for the data subject, is where the fact that a data subject purchases large quantities of halaal meat at times which relate to Muslim feast days may be passed on to a security agency which has also established that the subject has purchased books on the web relating to terrorist tactics, and that he or she has looked for information on how to get an American visa. Adverse inferences may then be drawn with regard to the subject on account of this accumulated information, which may, or may not, be correct.³²¹

5.7.4 Generally speaking, profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics.³²²

5.7.5 As such, the profiling process has two main components:

- (a) profile generation – the process of inferring a profile;
- (b) profile application – the process of treating persons/entities in light of this profile.³²³

5.7.6 The first component typically consists of analysing personal information in search of patterns, sequences and relationships, in order to arrive at a set of assumptions (the profile) based on probabilistic reasoning. The second component involves using the generated profile to help make a search for, and/or decision about, a person/entity. The line between the two components can blur in practice, and regulation of the one component can affect the other component.³²⁴

5.7.7 There is, generally speaking, no objection to the compiling of statistical information and profiles from personal information, where it is not possible to trace the personal information of

³²⁰ Andrew Rens.

³²¹ Tilley at 3.

³²² Bygrave Data Protection L A “Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling” Computer Law and Security Report, 2001 Vol 17 at 17-24 accessed at <http://folk.uio.no/lee/publications/> on 2005/07/29 (hereafter referred to as “Bygrave *Computer Law and Security Report* 2001”) at 2.

³²³ Bygrave *Computer Law and Security Report* 2001 at 2.

³²⁴ Bygrave *Computer Law and Security Report* 2001 at 2.

any identifiable individual from such profiling.³²⁵ Profiling is a valuable marketing tool and freely allowed as long as it is not making individualised personal information available. This view was also confirmed in the response to a question posed in the Issue Paper 24 as to the acceptability of profiling.

5.7.8 An example of anonymous profiling would be in the development of score cards (for credit risk management) where banks would typically use the services of specialist score card developers where the latter would require to be provided with anonymous account information from the particular bank for analysing.³²⁶

5.7.9 However, in so far as information which can identify a person is concerned, different opinions were expressed. Some respondents saw identifiable profiling as a natural part of their business, while others expressed concern about the practice. A distinction was furthermore made between the data subject in this category having knowledge of the collection of the information and on the other hand having specifically given permission for the collection and use of the information.³²⁷

5.7.10 Commentators, who were concerned about the use of profiling and argued for consent requirements, stated the following:

- a) Since it is not possible to guarantee a subject's anonymity, affirmative consent should be required because of the potential for a trail to lead to a customer through an IP address and cookies.³²⁸

³²⁵ ISPA notes that in practice Internet users are uniquely identifiable by the IP (Internet Protocol) address, which is assigned to them when they connect to the Internet. While it may not be immediately practical or possible for any third party to tie that IP address to a name and address, it is technically possible to track that IP address as the person 'surfs the web'. This is standard practise with online advertising companies, which may advertise on many websites. Some advertisements leave a cookie on your computer, which is an additional level of unique identification, and this cookie can be used to harvest personal information and surfing habits. In the same measure, by merely accessing the image of an online advert, you are leaving an 'imprint' of your IP address in a log on a web server. If the same advertising host advertises on millions of web sites, it becomes easily possible to track user habits by processing the logs each time an advert is viewed, and by requesting referrer information in each instance. (Each time you click a link to go to a website or another section of the website, the web server on the receiving end not only gets information on the file you want, but also information on which link directed you there. This information is very useful for statistical analysis of who uses a website, and is largely harmless when it is impossible to tie an identity of an individual to an IP address.

³²⁶ The Banking Council.

³²⁷ Andrew Rens.

³²⁸ Internet Service Providers Association.

- b) Written consent is necessary for non public information.³²⁹ Consent should be obtained from the data subject involved prior to information profiling taking place.³³⁰ Responsible parties who sell information to information profilers should obtain the prior consent of the data subject before proceeding to sell the information to information profilers, unless the public interests or those of the State dictate otherwise. Data subjects whose information is sold for information profiling purposes without the individual's consent should be provided with adequate remedies to enable them to take action against the responsible party in breach.³³¹
- c) If personal information is being used for this purpose without the consent of the data subject it should constitute an unacceptable infringement on his privacy.³³² The consent requirement should, however, not apply with regard to the prevention and detection of fraud.³³³
- d) Where consent must be provided for, "implied" consent may particularly be feasible, but the new law should then clearly set out for information of the whole of the public, when and how it will operate in practice.³³⁴

5.7.11 On the other hand, those who felt that information profiling was a natural part of conducting business argued as follows:

- a) The development of credit scores within the credit information system should be allowed with the knowledge of the data subject but without a consent requirement. Alternatively, the use of credit information to develop credit scores should be defined as a legitimate use /purpose.³³⁵

329 Strata.

330 Eskom Legal Department.

331 SABC.

332 ENF for Nedbank.

333 SAFPS.

334 Financial Services Board.

335 Credit Bureau Association.

- b) Information profiling is a statutory requirement in terms of FICA and banks adhere to the requirements of this Act. It is further used for fraud prevention and behavioural scoring within the banking industry.³³⁶ It was argued that information profiling for marketing purposes can and should be a natural element of marketing practices as long as it is done within defined parameters and subject to an 'opt out' consent option. The banking industry, for example, has access to clients' financial records, spending patterns, and as such is able to compile profiles of clients. Use of this information to curb and prevent fraud, enhance services and products, introduce services and products, manage relationships with clients, extend or deny credit facilities, etc should be encouraged, but subject to the provision that the use/storage of such information does not constitute an unreasonable act and if appropriate, is consented to by the client.
- c) Information profiling is a further reality in the law enforcement community that provides valuable input in respect of a suspect's modus operandi and assists the law enforcement agency in planning and conducting operations.³³⁷
- d) Information profiling is essential in the long-term insurance industry. The industry has to deal with population demographics, in order to revise the morbidity and mortality tables. These tables are based upon underlying information, and unless the industry is able to retain and use this type of information, the industry will be unable to determine the risks involved and no objective criteria for the determination of risk will be possible.³³⁸
- e) Profiling is a natural part of conducting business. Profiling assists, for instance, in targeting those customers who are or may be interested in a product. Any law prohibiting this practice will constitute an enormous blow to the South Africa economy.³³⁹

5.7.12 The EU Directive only deals with profiling as such in article 15(1) which provides for automated decisionmaking.³⁴⁰ Article 15(1) states that EU member states shall grant the right

³³⁶ The Banking Council.

³³⁷ SAPS.

³³⁸ LOA.

³³⁹ LOA.

³⁴⁰ **Article 15 Automated individual decisions**

- (i) Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects

to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of information intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.”

5.7.13 As an information protection provision, Art. 15(1) is rather special in that, unlike the bulk of other rules in information protection instruments, its primary formal focus is on a type of *decision* as opposed to information processing. As such, Art. 15(1) is akin to traditional administrative law rules on government decision making. This characteristic, though, does not have large practical significance given that decisions inevitably involve the processing of information. Moreover, the impact of Art. 15(1) is likely to be considerably greater on the decision-making processes of the private sector than on the equivalent processes of the public sector.³⁴¹

5.7.14 Article 15 derives from several concerns. The central concern is rooted in the perceived growth of automatisisation of organisational decisions about individual persons. The drafters of the Directive appear to have viewed as particularly problematic the potential for such automatisisation to diminish the role played by persons in shaping important decision-making processes.³⁴² The use of extensive information profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his ‘information shadow’.³⁴³

5.7.15 A second expressed fear is that the increasing automatisisation of decision-making processes engenders automatic acceptance of the validity of the decisions reached and a

relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

- (ii) Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

See, however, art 14 (b) of the Directive dealing with the right to object to direct marketing. This article does not deal with profiling as such.

³⁴¹ Bygrave *Computer Law and Security Report* 2001 at 2.

³⁴² Bygrave *Data Protection* at 3.

³⁴³ Bygrave *Computer Law and Security Report* 2001 at 5.

concomitant reduction in the investigatory and decisional responsibilities of humans. Up until recently, such assessments have tended to be based primarily on information collected directly from the data subjects in connection with the assessment at hand. It is likely, though, that these assessments will increasingly be based on pre-collected information found in the databases of third parties. Indeed, with effective communication links between the databases of large numbers of organisations, sophisticated software to trawl these databases, and appropriate adaptation of the relevant legal rules it is easy to envisage computerised decision-making processes that operate independently of any specific input from the affected data subjects. Additionally, there is ongoing growth in the frequency, intensity and ambit of organisational profiling practices. Not only is profiling an emergent industry in its own right, but the techniques upon which it builds (e.g. information warehousing and information mining) are evermore sophisticated. An important rationale for the right in Art 15(1) is, therefore, protection of human integrity and dignity in the face of an increasingly automated and inhumane world.³⁴⁴

5.7.16 Marketing profiles are, however, not regarded as necessarily detrimental to the data subject. On the latter point, the EU Commission seems to have been of the opinion that simply sending a commercial brochure to a list of persons selected by computer does not significantly affect the persons for the purposes of Art. 15(1). Also, other commentators view advertising (or at least certain forms of advertising) as too trivial to be significant.³⁴⁵

5.7.17 The prohibition against automated decision making is set out in article 42 of the Dutch Personal Data Protection Act, 2000, section 12 of the UK Data Protection Act, 1998 and since the implementation of the Directive, most of the other European countries. However, no similar provision has been made in the Australian³⁴⁶ and Canadian³⁴⁷ legislation.

5.7.18 The Commission's preliminary views regarding profiling can be summarised as follows:

a) There is no objection to the compiling of statistical information and profiles

³⁴⁴ Bygrave Computer Law and Security Report 2001 at 8.

³⁴⁵ Nevertheless, some forms of advertising have at least a potential to significantly affect their targets. For instance, the cybermarketing process outlined above could plausibly be said to have a significant (significantly adverse) effect on the persons concerned if it involves unfair discrimination in one or other form of "weblining" (e.g. the person visiting the website is offered products or services at a higher price than other, assumedly more valuable consumers have to pay, or the person is denied an opportunity of purchasing products/services that are made available to others).

³⁴⁶ Privacy Amendment (Private Sector) Bill 2000.

³⁴⁷ Personal Information Protection and Electronic Documents Act 2000 (Bill C-6).

of personal information, provided it is not possible to trace the information to an identifiable data subject.

- b) The legitimate interests of business should be appropriately accommodated. In ordinary circumstances marketing profiles should not be regarded as detrimental to a data subject. Marketing practices are currently being dealt with in the ECT Act³⁴⁸ as well as in the National Credit Bill.³⁴⁹
- c) The ordinary principles, exceptions, exclusions and exemptions set out in Chapter 3 and 4 of the Bill are applicable as is Chapter 7 dealing with sector specific codes of conduct.
- d) Section 39 (1) (k) and section 40 (3) of the proposed Bill furthermore already makes provision for the supervision of information matching legislation.
- e) Restrictive measures need to be put in place that will ensure that data subjects are not unreasonably affected to their detriment by the profiling of their personal information.

5.7.19 The conclusion of the Commission is therefore that a section should be included in the proposed Act to provide for the prohibition of unreasonable automated decision making since its exclusion will deprive data subjects of a significant counterweight to the ongoing expansion, intensification and refinement of automated profiling practices. Comment is invited as to whether a specific section similar to sec 45 of the ECT Act should be included in the information protection legislation.

³⁴⁸

Section 45 of the Electronic Communications and Transactions Act, 25 of 2002 reads as follows:

45. Unsolicited goods, services or communications

(1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer-

- (a) with the option to cancel his or her subscription to the mailing list of that person; and
- (b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89 (1).

(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89 (1).

³⁴⁹

See in this regard Part C Credit Marketing Practices (clauses 73-77) of the NCB.

5.7.20 The legislative enactment of this provision will read as follows:

**CHAPTER 10
MISCELLANEOUS**

Automated decision making

93. (1) *Subject to subsection 2, no one may be subject to a decision to which are attached legal consequences for him or her, or which affects him or her to a substantial degree, where this decision has been taken solely on the basis of the automated processing of personal information intended to provide a profile of certain aspects of his or her personality or personal habits.*

(2) *The provisions of subsection (1) do not apply where the decision referred to therein:*

- a) *has been taken in connection with the conclusion or execution of a contract, and*
 - (i) *the request of the data subject in terms of the contract has been met; or*
 - (ii) *appropriate measures have been taken to protect the data subject's lawful interests; or*
- b) *is based on a law or code of conduct in which measures are laid down for protecting the lawful interests of data subjects.*

(3) *Appropriate measures, as referred to under subparagraph 2(a), must be considered as taken where the data subjects have been given the opportunity to put forward their views on the decisions as referred to under subsection (1).*

(4) *In the case referred to under subsection (2), the responsible party must inform a data subject about the underlying logic of the automated processing of the information relating to him or her.*

Comment is invited.