

CHAPTER 3: SUBSTANTIVE SCOPE OF THE PROPOSED LEGISLATION

3.1 General

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

- a) automatic/electronic and manual/paper files;
- b) information pertaining to both natural and juristic persons;
- c) information kept by both the public and the private sector; and
- d) sound and image information.

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

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

1 Issue Paper 24.

2 Strata; Financial Services Board.

3 The Financial Services Board stated that the proposed law should be as wide as possible to prevent a situation where a number of different laws have to be passed resulting in a fragmented situation which could impact negatively on some of those laws where interpretation thereof has to take contextual considerations into consideration. The proposed law should then cover all personal information in whatever format it is held or may be distributed and should also cover all methods of collecting, distributing and processing thereof.

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

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

6 IMS Health.

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

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

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

3.2 Automatic and manual files

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

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

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

8 From the definition in the Open Democracy Bill [B67-98] of "records" as "recorded information regardless of form and medium" (cl 1(1)) it is evident that both manual and computer records were intended to be included in the scope of this Bill.

9 Article 3 of the EU Directive furthermore stipulates that the Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

10 It should however be noted that in the Electronic Communications and Transactions Act, Act 25 of 2002 (hereafter referred to as "ECT Act") paper based data bases are not included. The Act defines "electronic transactions" as follows:

"**electronic**" includes created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic, optical or any similar means;

"**transaction**" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-Government services.

11 SABC.

databases. Much information in the long-term insurance industry is, for instance, retained electronically. Such electronic data may be collected by automatic systems, such as telephonic call centres and the like, but may be manually captured by data operators on computer systems. In addition, there is a great deal of information, which is retained in paper form.

3.2.3 Caution should, in any case, be exercised when making reference to “automatic” and “manual” files. All information which is saved in files, is done so because of prior instructions given “manually”. For instance, any “automatic” electronic system will have had prior “manual” programming.¹² These phrases are therefore inappropriate. On the other hand, a “manual” file is handled by “hand” but the definition does not preclude some sort of “automatic” processing to compile a manual file.¹³

3.2.4 With current and future technological advances, there is already a substantial use of electronic and digital databases. This is likely to increase exponentially as the use of digital technologies become more pervasive. Already personal and private information is being stored in forms not provided for in current legislation. For instance, the use of biometrics (finger print scanning, retina scanning and facial image scanning) is a reality of modern life. See also the discussion on sound and image information below in para 3.3.

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

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

3.3 Sound/image information

12 LOA.

13 Liberty.

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

3.3.1 There appears to be consensus amongst respondents that the investigation should cover both sound and image information,¹⁵ given the advancement of information technology and the use of sound and image information as means of identification and verification of the interaction of individuals.¹⁶ There is clearly a lacuna in the existing guidelines and legislation in South Africa with regard to this type of information.¹⁷

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

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

3.4 Natural v juristic persons

3.4.1 In the Issue Paper the following points were made:

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

* In **Financial Mail (Pt) Ltd v Sage Holdings Ltd**²⁰ the court expressed the view that the *actio iniuriarum* should be available for a violation of the privacy of a juristic person even if one cannot, in the case of a juristic person, speak of feelings being outraged or offended. The basis for this protection is that privacy, like reputation

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

16 ENF for Nedbank.

17 The Banking Council.

18 LOA.

19 See **Motor Industry Fund Administrators (Pty) Ltd v Janit** supra at 60 (confirmed on appeal: 1995 4 SA 293 (A)) and **Financial Mail v Sage Holdings** supra 462-463; **Neethling's Law Of Personality** 32 fn 336, 68ff, 71-73; for a discussion of these cases see Chapter 2 above as well as the Nadasen submission.

20 Supra.

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

* The court in **Janit v Motor Industry Fund Administrators (Pty) Ltd**²² affirmed the view expressed in the *Sage Holdings* case that a company would be entitled to regard the confidential oral or written communications of its directors and employees as sacrosanct and would, in appropriate circumstances be entitled to enforce the confidentiality of such communications. Interestingly, in the *Janit* case, the view was articulated that the theft of confidential discussions of a board of directors constituted an unlawful invasion of their privacy and any disclosure of such information, would itself constitute an invasion of the respondent's privacy.²³

Furthermore, where another person, who was aware that the information was unlawfully obtained and that they contained private and confidential discussions of the respondent's directors, helped himself to that information, such a person thereby violated and infringed their right to privacy.²⁴

b) In the second place the Constitution sets out the applicability of the Bill of Rights to a juristic person in s 8(4) of the Constitution which states:

A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person.

c) Thirdly, in **Investigating Directorate: Serious Economic Offences ao v Hyundai Motor Distributors (Pty) Ltd ao; In re Hyundai Motor Distributors (Pty) Ltd ao v Smit NO**²⁵ it was held that juristic persons enjoy the right to privacy, but is not protected to the same extent as natural persons since juristic persons are not the bearers of human dignity. The level of justification for any particular limitation of the right would have to be judged in the light of the circumstances of each case.

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

22 1995 (4) SA 293 AD.

23 At 303.

24 At 305 B-D.

25 *Supra*.

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

3.4.2 Most respondents to the Issue Paper agreed that the investigation should be aimed at protecting both the fundamental rights of natural persons (in particular their right to privacy) and the legitimate interests of juristic persons.²⁹ In one submission³⁰ it was, however, held that the inclusion of juristic persons in this way may be unconstitutional.

3.4.3 The Commission was furthermore (in more than one submission) referred to two studies in this regard. The first was the European Commission study on the protection of the rights and interests of juristic persons with regard to the processing of personal information relating to such persons³¹ and the second an article written by S Nadasen entitled “Data Protection for

- 26 The definition of “personal information in PAIA reads as follows:
“Personal information” means information about an identifiable individual, including, but not limited to-
- a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
 - b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
 - c) any identifying number, symbol or other particular assigned to the individual;
 - d) the address, fingerprints or blood type of the individual;
 - e) the personal opinions, views, or preferences of the individual, except where they are about another individual, or about a proposal for a grant, an award or a prize to be made to another individual;
 - f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature of further correspondence that would reveal the contents of the original correspondence;
 - g) the views or opinions of another individual about the individual;
 - h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
 - i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.
- 27 Roos at 499.
- 28 The definition of “personal information” in the **Electronic Communications and Transactions Act** is based on that of **PAIA**. It is furthermore interesting to observe that the Promotion of Access to Information Act 2 of 2000 (PAIA) lists amongst the grounds on which the refusal to grant access to the records of private persons is the mandatory protection of the privacy of a third party who is a natural person. No such exclusionary provision is made in respect of juristic persons.
- 29 Internet Service Providers' Association; Liberty; Sagie Nadasan; Sanlam Life: Legal service; Financial Services Board; Neo Tsholanku, Eskom Legal department; ENF for Nedbank; SABC; LOA; The Banking Council.
- 30 IMS.
- 31 Korff D for the Commission of the European Communities *EC Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons*(Study Contract ETD/97/B5-9500/78) Final Report by Douwe Korff (contractor) (hereafter referred to as “ Douwe Korff **EC Study**”) accessed on 5/4/2004at
http://europa.eu.int/comm/internal_market/privacy/docs/studies/legal_en.pdf.

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

3.4.4 The report by Douwe Korff contains a comprehensive discussion of the international and, more specifically, the European position regarding the protection of personal information of juristic persons.

3.4.5 Korff, after surveying the law and practice in some European countries, observes the following:

- (a) In some countries information protection is seen as deriving from the "right to (human) personality" or to "human dignity" or "honour" or to personal or family "characteristics" – the aim being the protection of privacy, or the private life or private sphere of individuals. From this perspective, companies and other juristic persons, not possessing human personality, human dignity or family characteristics do not require privacy or a protected private sphere. Accordingly, not only should companies or juristic persons be open to scrutiny, but the extension of information protection to them is misconceived.
- (b) However, other countries, while recognising the relationship between information protection and these classical rights, identify other "legitimate interests" affected by information processing. These interests, which are deemed worthy of protection, include the interest of everyone in "significant decisions" affecting them being taken on factual, accurate and relevant information, or the related interest in being able to challenge decisions reached on the basis of erroneous or irrelevant information. Some countries have seen the adoption of constitutional provisions which to some extent recognise information protection as a new, *sui generis* right, linked with, but distinct from, and wider, than privacy.³³

3.4.6 The international information protection instruments remain somewhat ambiguous about

32 Nadasen S "Data Protection for Companies: Privacy and More" **Insurance and Tax** Sept 2003 also submitted by Dr Nadasen as part of the submission from Sanlam Life.

33 The collection of information on race, religious-, philosophical- or political beliefs or trade union membership could affect the freedom of religion or belief, the freedom to educate one's children in accordance with one's beliefs, the freedom of association and the freedom from discrimination of both the individual and the group. The fact that information protection was increasingly seen as a *sui generis* right, related to but distinct from Articles 8 and 10 of the ECHR, was one of the main reasons for drafting a separate international legal instrument in the field: the Council of Europe Data Protection Convention. The other reason was that the Human Rights Convention is open only to Member States of the Council of Europe, whereas the Data Protection Convention was drafted in such a way as to allow non-European States too to become a party.

the nature, objects and aims of information protection.³⁴ They link information protection “in particular” with the right to privacy and freedom of expression, but they also acknowledge that these concepts do not suffice to define the interests at stake; that other interests - some of them equally fundamental in a State under the rule of law - are also affected; and that these wider interests, at least, may also pertain to juristic persons.³⁵ The ISDN Directive³⁶ gives formal expression to this increasingly explicitly recognised fact, and also confirms that, in certain contexts, a distinction between natural and juristic persons is difficult to make or justify in practice.³⁷

3.4.7 The experience of EU Member States shows that the making of an absolute distinction between natural and juristic persons (with the first being given full protection and the latter none) is difficult to defend on rational or practical grounds. Some collective bodies composed of

34 As the Explanatory Memorandum to the OECD Guidelines puts it:

“Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.” (Explanatory Memorandum, para. 31)

Thus, the Council of the OECD left it at the above acknowledgment that it might be “advisable” to extend a measure of data protection to legal persons, in some instances: the OECD Guidelines themselves do not anywhere envisage their application to legal persons, even as an option. The UN Guidelines, while still very tentative, go somewhat further in that they themselves state, in Principle 10, that: 4 The OECD Guidelines say that the data must be “complete”.

“Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.”

In Europe, there has been greater willingness to explicitly acknowledge the legitimacy of extending data protection to legal persons as such - even if the choice of whether to do so was initially left to individual States. Thus, the Council of Europe Convention stipulates, in Article 3(2):

“Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a. ...

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality.”

Article 2(a) of the EU Directive defines personal data as information relating to a natural person but similarly recognises the legitimacy of extending data protection by stipulating that:

“[the existing legislation in the Member States] concerning the protection of legal persons with regard to the processing [of] data which concerns them is not affected by this Directive” (Preamble (24)).

35 Whatever the limitations on the right to “private life” (further discussed below, at 2.3), the wider “legitimate interests” affected by unfettered data processing, noted above, are not intrinsically limited to “natural persons”: “legal persons” too have an interest in how their creditworthiness is assessed, in fairness in legal proceedings, and non-discrimination.

36 Directive 97/66/EC of the European Parliament and of the Council dated 15/12/97 concerning the This trend has culminated (for now) in the formal, mandatory extension of the ISDN Directive to such persons.

“... in the case of public telecommunications networks, specific legal regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of natural persons **and legitimate interests of legal persons**, in particular with regard to the increasing risk connected with automatic storage and processing of data relating to subscribers and users” (Preamble (7)). protection of personal data and the protection of privacy in the telecommunications sector.”

37 This trend has culminated (for now) in the formal, mandatory extension of the ISDN Directive to such persons.

“... in the case of public telecommunications networks, specific legal regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of natural persons **and legitimate interests of legal persons**, in particular with regard to the increasing risk connected with automatic storage and processing of data relating to subscribers and users” (Preamble (7)).

individuals, such as partnerships in England, lack independent juristic status but may nevertheless operate as a distinct economic entity. In other cases, eg. as regards financial transactions, information on juristic persons can be impossible to separate from information on individuals.

3.4.8 Even when juristic and natural persons can be distinguished, the distinction is, for information protection purposes, often not necessarily the most appropriate one to make. Some 'natural persons' (e.g. one-person businesses), in some respects, require less protection than other 'natural persons' (e.g. consumers), and some 'juristic persons' (e.g. religious, political, or trade union associations) require more protection than other 'juristic persons' (e.g. large corporations). Indeed, in some circumstances, some 'natural persons' may require less protection than some 'juristic persons'; and the absence of any protection for some 'juristic persons' could even, in some circumstances...breach international human rights law.

3.4.9 Therefore, three groups are identified among the Member States of the European Community, namely: states which are of the view that information protection is inherently limited to natural persons; those who are of the view that a measure of information protection should be extended to juristic persons as a matter of principle and, states which appreciate arguments in favour of the latter position but which have refrained from extending protection in this way for practical reasons.

3.4.10 Korf concludes that the crucial point for the present study is that these wider interests affected by information processing – and the corresponding guarantees in the Human Rights Convention and the general principles of Community Law – cannot be said to be inherently limited to natural persons. It was recognition of these wider issues, and in particular of the fact that the interests protected by information protection are not exclusive to natural persons (rather than a 'purely formalistic' approach), which in Europe led Austria, Denmark, Iceland, Italy, Luxembourg and Switzerland to extend their laws to juristic entities.

3.4.11 The main consideration appears to be that juristic entities as well as natural persons are affected by the increased processing of information on them, and that it is necessary to impose certain duties on persons processing information, while giving the subjects of such processing certain rights, to ensure that the processing of information on them does not harm their legitimate interests.

3.4.12 A number of distinct areas in which the extension of information protection to juristic persons has the most immediate, practical effect have been identified and they are as follows:

- a) The protection of the interests of juristic persons concerning the processing of business information by credit reference agencies and the like;
- b) The protection of the interests of juristic persons in relation to the processing of information on users and subscribers of telecommunications services;
- c) The protection of the interests of juristic persons relating to the processing of business information supplied by them to State institutions for statistical purposes;³⁸
- d) The protection of the interests of juristic persons relating to direct marketing;
- e) The protection of the interests of juristic persons concerning the processing of information which is used by public and private bodies to take decisions which 'significantly affect' them;³⁹
- f) The scope of the protection afforded to one-person businesses; and
- g) Information held by various persons and bodies which collect data, including not only financial information concerning the juristic person, but for instance the corporate strategies of those juristic persons, the number of employees employed by them, the identities of those employees, the status of those employees within the juristic person and also the financial remuneration provided to those employees.⁴⁰

3.4.13 Since the extension of information protection to juristic persons by some, but not all, Member States could be problematic, Korff recommended (a recommendation reiterated in the EU Study on the Implementation of DPD in 2001) that consideration be given to extending specific elements of the protection of the Directive to juristic persons in specific areas to all European countries.

3.4.14 In his article referred to above, Nadasen, discusses the report of Korff and then specifically considers what could constitute "appropriate circumstances" or situations in South

38 Companies are required to provide ever-increasing, detailed information on their financial, environmental and other activities, under national or Community legislation. While the need to provide such information is generally accepted (although sometimes somewhat grudgingly), concern has been raised about the proper use of such information. In particular, certain data, provided for (e.g.) statistical purposes could, in the hands of a competitor, be used to the detriment of the undertaking which provided the data, and thus affect competition. It has also been noted that the State agencies to which such data is sent are increasingly privatised, and thus have a commercial interest in using (or indeed selling) the data.

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

40 LOA.

African law (as required in the Hyundai case) which companies could rely on to protect their interests by an appeal to the protection of their privacy as it may relate to information protection. In discussing the case law, he reiterates the view that juristic persons have a right to privacy,⁴¹ but that the extent of the protection has to be judged in each case⁴² and acknowledges the fact that a company's right to privacy may be limited for several reasons.⁴³

41 **Sage Holdings Ltd ao v Financial Mail (Pty) Ltd ao** supra and **Motor Industry Fund Administrators(Pty) Ltd ao v Janit ao** supra. See discussion above.

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

43 In **Bernstein v Bester and Others NNO** supra the Court suggested that the public's interest in ascertaining the truth surrounding the collapse of a company, a liquidator's interest in a speedy and effective liquidation of a company and the creditors' and contributors' interests in the recovery of company assets could constitute a legitimate limitation to personal privacy.

Similarly, in **President of the RSA v South African Rugby Football Union** 1999 (4) SA 147 (CC) it was noted that in terms of the Commissions Act a witness before a commission may be asked questions or required to produce documents which will limit his or her right to privacy. The court cautioned that in any particular case, the questions put and the documents sought must be relevant to the scope of the commission's investigation and that the investigation must be a matter of public concern. – for the court, if the questions asked or documents requested were relevant then, “in all probability an invasion of privacy will be permissible”.

Furthermore, in **Investigating Directorate: serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit NO** supra, the court affirmed that in the proportional analysis of competing interests, in limiting the right to privacy, a balance had to be struck between the interests of the individual and that of the State, a task that lie at the heart of the inquiry into the limitation of rights.

In **Gardener v Walters aoNNO** 2002 (5) SA 796 (CC) the respondents, the joint liquidators of a public company in liquidation, had obtained orders for the issue of letters of request to the Royal Court of Jersey to recognise their appointment as duly appointed liquidators and to allow them to institute proceedings in Jersey for the investigation and recovery of the company's assets. The applicants contended, *inter alia*, that the order of the Jersey Court giving effect to the letters of request could affect their privacy. In dismissing the appeal, the court characterised the appeal to privacy as one which “ borders on the grotesque”. Not only was a proper and thorough investigation warranted, but the appeal to privacy, in the courts view, was -

‘illustrative of the attitude of so many managers of companies who seem to believe that they should be allowed to walk away scot-free from financial disasters which they have created’.

Relying on the *Bernstein* case, the court in **Shelton v Commissioner for the SARS** 2000 (2) SA 106 (E) concluded that - “...It is apparent from the judgment that the concept of privacy does not extend to include the carrying on of business activities.”

Nadasen mentions that the above statement could arguably be used to sustain the contention that, while a juristic person does enjoy a measure of privacy, that protection does not extend to include the carrying on of business activities. The Constitutional Court said the following in the *Bernstein* case -

Examples of wrongful intrusion and disclosure which have been acknowledged at common law are entry into private residence, the reading of private documents, listening to private conversations, the shadowing of a person, the disclosure of private facts which have been acquired by a wrongful act of intrusion, and the disclosure of private facts contrary to the existence of a confidential relationship. These examples are all clearly related to either a private sphere, or relations of legal privilege and confidentiality. *There is no indication that it may be extended to include the carrying on of business activities.*” [emphasis added]

Nadasen submits that the above passage lists examples of the protection of privacy which have been afforded at common law and is not a statement of law that privacy cannot be extended to include the carrying on of business. Reading the sentence within the context of the entire paragraph, it is submitted that the meaning to be ascribed is the following: there is no indication *in the common law* that it may be extended to include the carrying on of business. Furthermore, the Constitutional Court did not say that the application of the common law leads to the conclusion that “it *cannot* be extended to include the carrying on of business activities”. The Constitutional Court, it is submitted was only summarising the application of the common law to the protection of privacy.

He therefore concludes that, with respect, the court in the *Shelton* case failed to appreciate the context of the statement as it also, with respect, misconceived the import of the particular sentence, namely, an observation and not a fixed principle of law. The approach adopted in the *Shelton* case also leads to the difficult task of having to categorise where business activities end in order for an appeal to the right to privacy to be applicable.

3.4.15 Nadasen therefore concludes that the question of whether or not privacy could be extended to include the protection of the carrying on of business, must depend on the application, *in concreto*, of section 8 (4) of the Constitution.⁴⁴

3.4.16 He refers to the Korf analysis⁴⁵ referred to above and concludes that while there is no uniform approach in foreign jurisdictions, it is submitted that the Constitutional Court in the *Hyundai Motor Distributors* case has already set the basis for the recognition of the information protection of companies to be located firmly within the protection afforded to the right to privacy. However, the peculiar nature of information protection, in regard to juristic persons and as evinced by the experience of other countries, also suggest that information protection is *sui generis*, and traverses other rights in addition to that of privacy.

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

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

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

44 Admittedly, as was stated in the *Hyundai Motor Distributors* case, the privacy afforded to juristic persons can never be as intense as those of human beings. But, the Constitutional Court also asserted that this did not mean that juristic persons are not protected by the right to privacy.

45 Douwe Korf *EC Study*.

46 Michalsons for IMS Health.

47 In this respect the Commission was referred to the Ontario Commissioner who has consistently held that information about a sole proprietorship is just that: information about the sole proprietorship and not about the principal of that proprietorship. In Order 1633, former Ontario Information and Privacy Commissioner Sydney Linden wrote: "Had the legislature intended "identifiable individual" to include a sole proprietorship, partnership, unincorporated associations or corporation, it could and would have used the appropriate language to make this clear. The types of information enumerated under subsection 2(1) of the Act as "personal information" when read in their entirety, lend further support to my conclusion that the term "personal information" relates only to natural persons."

48 Michalsons for IMS Health.

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

3.4.21 The Commission was referred to the position in the United States, where a wide assortment of privacy laws are found in the individual States and at the federal level, but no national general privacy law has been enacted for the private sector.⁵⁰

3.4.22 A distinction between juristic and natural persons is furthermore found in the Privacy Act of 1974⁵¹ which only protects natural persons.⁵² Similarly, the Fair Credit Reporting Act (the "FCRA") only protects consumer credit reports⁵³ of "individuals"— it specifically excludes so called commercial credit reports⁵⁴ and by definition any entity other than an "individual".⁵⁵ A credit report generated for an application for a business loan for the same individual would not be covered. Privacy protections under the FCRA will therefore depend on whether one is asserting privacy rights over information processed in a personal or professional capacity.

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

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

49 EU Directive.

50 Eg. the Fair Credit Reporting Act (1970), the Family Educational Rights and Privacy Act (1974), and the Right to Financial Privacy Act (1978). During the 1980s, Congress passed the Privacy Protection Act (1980), the Electronic Communications Privacy Act (1986), the Video Privacy Protection Act (1988), and the Employee Polygraph Protection Act (1988). In the 1990s, Congress has passed the Telephone Consumer Protection Act (1991), the Driver's Privacy Protection Act (1994), the Telecommunications Act (1996), the Children's Online Privacy Protection Act (1998), the Identity Theft and Assumption Deterrence Act (1998), and Title V of the Gramm-Leach-Bliley Act (1999) governing financial privacy. See the discussion in the prefatory materials to the Standards for Privacy of Individually Identifiable Health Information; Final Rule. 65 F.R. 82462 (to be codified at 45 CFR Parts 160 and 164), 65 F.R. 82462 [hereinafter "HIPAA Final Rule"].

51 5 U.S.C. § 552a.

52 Supra at (a)(2).

53 "Where the information concerns the subject's business history or status (i.e., is collected and provided by a commercial reporting agency for use in business transactions), of course, its communication to the user does not constitute a "consumer report" under Section 603(d). *Wrigley v. Dun & Bradstreet, Inc.*, 375 F. Supp. 969 (N.D. Ga. 1974); *Boothe*, 523 F. Supp. at 633." See Federal Trade Commission. FTC Staff Opinion – Medine-Tatelbaum. (26 July 2000), online: <http://www.ftc.gov/os/statutes/fcra/tatelbaum.htm>

54 Fair Credit Reporting Act, 15 U.S.C. § 1681a (d); *Emerson v. J.F. Shea*, 76 Cal. App. 3d 579, 143 Cal Repr. 170 (1978).; *Yeager v. TRW Inc.*, 961 F.Supp 161 (ED Texas, 1997).

55 Ibid., 15 U.S.C. § 1681a ©.

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

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

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

3.5 Public v private sector

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

3.5.2 It was argued that any legislation dealing with privacy protection is all encompassing, not just in respect of the form of the databases, but also in respect of the nature of the entities which collect personal information. As both public and private entities are affected by questions of privacy and information protection, there seems to be no reason why either sector should be excluded.⁵⁸ Consumers would be adversely affected if governmental agencies were not subject to security protection.⁵⁹⁶⁰

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

58 SABC.

59 The SABC also requires that State Owned Enterprises should have limited access, under appropriate guidelines to protect competition, with respect to databases of private sector entities where such databases could be used by State Owned Enterprises where their rights are being affected. The SABC is of the view that in order to further its interests, and consequently those of the State as the sole shareholder and the public in respect of the collection of outstanding licence fees, the SABC and its agents/ representatives should be allowed access to the databases of other entities, including the databases of pay-channels such as M-Net.

3.5.3 One commentator, however, submitted that the investigation should only focus on information kept by the private sector. It was argued that existing laws and policies provide at least a degree of protection and control over information kept by the public sector. Most of the information kept by law enforcement agencies can be regarded as sensitive information which should be kept out of the public domain. The same cannot be said about information gathered and kept by the private sector, which in most instances, is not regulated by legislation at all and is often driven by financial gain, competition and specific customer needs.⁶¹

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

3.5.5 In the Issue paper the further question was posed whether a distinction should be drawn between the public and the private sector in drafting privacy legislation and if so, what should these differences should be? ⁶²

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

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

60 LOA.

61 SAPS; See discussion on critical information below.

62 Question 4, Issue Paper 24.

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

64 LOA.

65 LOA.

66 Gerhard Loedolff, Eskom.

- * PAIA treats these two sectors similarly, with minimal material distinction. There is therefore merit in being consistent by creating new legislation that also removes as far as possible the distinction between these two sectors.^{67 68}
- * If critical information is to be included in any protection law, then, in that area, there is room to justify the distinction, on the basis that the State ought to be allowed to gather and use private information for legitimate purposes.⁶⁹

3.5.7 Other respondents, however, argued that due regard should be given to the different and differing interests which the public and private sectors have in information.⁷⁰⁷¹

- * For example, the use of medical information for the assessment of risk in cases of proposed contracts of insurance differs from the State's use of medical information to compile public health profiles or for state public health interventionist strategies.
- * The public sector is empowered by specific legislation to fulfill certain duties whilst their interest in good governance and the security of the Republic also outweighs that of the private sector. The public sector, representing Government, is furthermore entitled by certain laws to limit the privacy of the individual, eg. interception and monitoring of communications, search and seizures, etc. Entities such as private investigators have very little, if any powers to infringe the privacy of individuals. They are furthermore only accountable to their (paying) clients and not to the public in general.⁷²
- * One should recognise public interest in the public sector's retention of certain records and public access to them in cases in which retention by and availability from the private sector would be inappropriate in light of the constitutional right to privacy.⁷³
- * The private sector, on the other hand, should be allowed flexibility through the development and application of self-regulatory measures such as codes of

67 Liberty.

68 LOA.

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

70 Sanlam Life: Legal Services.

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

72 SAPS; Financial Services Board.

73 SAHA. SAHA is particularly concerned to ensure considerations of privacy should not limit transfer of records to the National Archives or provincial archives services or access to documents held by them any more extensively than strictly necessary for protection of the constitutional right to privacy.

conduct.⁷⁴ Although the two sectors are treated similarly in most national laws, there is a differentiation between the sectors in international information protection instruments. The public sector bodies are subjected to more stringent regulation than private sector bodies.⁷⁵

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

- * Many bodies from the private sector take decisions which have a profound impact upon public policy.
- * In South Africa, we do not only find a distinction between the public and private sector bodies but we also find some form of rules or legislation specific to State Owned Enterprises.⁷⁷
- * In many instances the SABC, for instance, is faced with an overlap regarding laws and regulations which apply to both the public and private sector bodies. When the SABC performs a public function in terms of the Broadcasting Act, it is on the whole also performing a commercial interest by generating revenue as a corporate entity.⁷⁸
- * There are many other State Owned Enterprises like the SABC that are faced with similar uncertainties when, for example, their activities do not fall exclusively within either of the public or private sectors. Attempts to re-categorise an entity every time a problem arises will cause undue delay and unnecessary costs for all affected entities.⁷⁹

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

74 The Banking Council.

75 SABC.

76 SABC; ISPA.

77 SABC; As an example reference was made to the SABC which is a State Owned Enterprise governed by various legislation. Further to the public law legislation, the SABC is obliged to comply with the Broadcasting Act, the IBA Act, its licence conditions, various regulations such as those prescribing local content quotas, Codes of Conduct pertaining to the broadcasting industry, as well as company law principles. In addition, the SABC is obliged to structure its business practice and model as set out in the Protocol on Corporate Governance in the Public Sector.

78 SABC.

79 SABC.

3.6 Critical information

3.6.1 Most information protection laws provide for exceptions to the information protection principles with regard to critical information, while critical information is totally exempted from the provisions of some information protection laws.

3.6.2 This position is in accordance with the EU Directive⁸⁰ which stipulates that the Directive does not apply to the processing of personal information in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

3.6.3 Article 13(1)((a)-(g) of the Directive furthermore provides for exemptions from specific privacy principles in terms of which legislative measures may be adopted to restrict the scope of the privacy principles in the indicated instances.⁸¹

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

Definition of critical information

80 Article 3 (2).

81 Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- (g) the protection of the data subject or of the rights and freedoms of others.

82 Eg, if someone would be able to hack into the JSE and bring it down for a week, it would have a far more catastrophic effect on our country than fighting a war on our borders for a couple of years.

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

3.6.6 The so-called “critical information” or “security information” should furthermore not be equated with information that is kept secure in terms of the security principle. All information should be kept secure irrespective of whether it is of a specific kind or not. Once information is classified as critical/sensitive information, it is marked accordingly and given various forms of protection - including restricting access to people with a security clearance at the appropriate level, physical protection (such as storage in approved containers of sufficient strength or meeting other security standards) and restrictions on how it may be transferred from one person to another. However, the fact that information is not classified as critical or sensitive, does not mean that it is freely available.⁸³ All personal information is subject to the privacy principles.⁸⁴

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

3.6.8 Terms used in other legislation for describing information relating to the protection of national security or the economic and social well-being of the country’s citizens are “classified information”⁸⁵ or “information kept, used, made, obtained or related to a prohibited place”,⁸⁶ as well as “intelligence/security information”.⁸⁷

83 Australian Law Reform Commission *Keeping Secrets: The Protection of Classified and Security Sensitive Information* ALRC 98 June 2004 accessed at <http://www.austlii.edu.au/other/alrc/publications/reports/98/5.html> on 2004/11/12.

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

85 Public Audit Act 25 of 2004; National Strategic Intelligence Act 39 of 1994; Defence Act 42 of 2002; Intelligence Services Act 65 of 2002 etc.; See also the new Draft National Information Security Regulations compiled by the National Intelligence Agency.

86 Protection of Information Act, Act 84 of 1982.

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

3.6.9 The Protection of Information Act 84 of 1982 is currently the principal Act concerned with the restriction of the disclosure of information.⁸⁸ The principal mechanism by which the Protection of Information Act is currently implemented is a Cabinet-level policy document, the Minimum Information Security Standards (MISS).⁸⁹ The MISS is to be implemented by each public institution as well as some private institutions working with public ones. According to its preface the MISS “must be maintained by all institutions who handle sensitive/classified material of the Republic”.

3.6.10 Classified information is defined to be :

Sensitive information which, in the national interest, is held by, is produced in or is under the control of the State or which concerns the State and which must by reason of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.

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

3.6.12 This definition differs from that in a separate specific policy which governs information security within the South African Defence Force.⁹⁰ This more narrow military information security policy is contained in a set of South African National Defence Force Orders (SANDF/INT DIV/2/97) which applies principally to the SANDF and Armscor. Classified information is defined in terms of these orders as:

any information or material which is held by or for, is produced in or for, or is under the control of the State or which concerns the State and which for the sake of national security be exempted from disclosure and must enjoy protection against compromise. Such information is classified either Restricted, Confidential, Secret or Top Secret according to the degree of damage the State may suffer as a consequence of its unauthorised disclosure.

3.6.13 The Intelligence Services Oversight Act 40 of 1994 defines “intelligence” in sec 1 as follows:

‘Intelligence’ means the process of gathering, evaluation, correlation and interpretation of security information, including activities related thereto, as performed by the Services;⁹¹

88 See a full discussion by Klaaren J “Access to Information and National Security in South Africa” *National Security and open Government: Striking the Right Balance* Maxwell School of Citizenship and Public Affairs of Syracuse University New York 2003 695.

89 The MISS was approved by Cabinet on 4 December 1996 as “national information security policy”. See also Part II B of the PSA Regulations amended Nov 2002. New regulations are, however, being drafted by the National Intelligence Agency. Klaaren at 196.

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

Security information is not defined.

3.6.14 Various initiatives regarding the protection of critical information have been noted. The Electronic Communications and Transactions Act (the ECT Act) ⁹² provides that when information is important to the protection of national security or the economic and social well-being of the country's citizens, the Minister may declare them to be "critical databases".⁹³ The Act then sets out the special treatment that these databases will enjoy. ⁹⁴

3.6.15 While these considerations may have their value, the reality is that there have been no ministerial declarations to this effect in terms of the Act. In November 2003 the Minister of Communications awarded a tender to a consortium of Consultants to undertake an inventory of all major data bases in South Africa.⁹⁵ The purpose of this is to assist the Minister to -

- (a) put in place regulations, with respect to the development, maintenance, validity, integrity and security of these databases and related systems,
- (b) review progress and compliance on an ongoing basis,
- (c) refine policy, legislative and regulatory requirements where appropriate; and
- (d) ensure that databases and information, in the Republic of South Africa, that could negatively impact on companies and citizens, are developed, maintained and secured to meet appropriate standards.⁹⁶

and the Intelligence Division of the South African Police Service; Agency is defined as follows: 'Agency' means the National Intelligence Agency referred to in section 3 of the Intelligence Services Act, 1994 (Act 38 of 1994). Act 38 of 1994 replaced by Intelligence Services Act 65 of 2002.

92 Sec 53 of Act 25 of 2002.

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

53. The Minister may by notice in the Gazette -

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

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

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

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

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

3.6.17 It is therefore unsure what the effect of the ECT Act will be,⁹⁸ especially since sec 55 dealing with the management of critical databases also provides as follows in sec 55(3):

This Chapter must not be construed so as to prejudice the right of a public body to perform any function authorised in terms of any other law.

3.6.18 The Minister for Intelligence Services furthermore launched the Classification and Declassification Review Committee in February 2003 with the aim to develop criteria for the management of the protection of classified information and the access of information that has been declassified. The Review Committee adopted the following terms of reference:

- * To scrutinise existing legislation, regulations, policies and procedures relating to the classification and declassification as well as custody of sensitive information;
- * To study international practices in respect of legislation, practices etc.
- * To examine the practical application of the above in respect of facilities and controls in various government departments;
- * To study policies and practices in the private sector (eg banks, financial institutions, construction and service industries);
- * To examine the storage of sensitive information; and
- * To formulate recommendations regarding amendments to legislation, policies and procedures, especially with regard to the harmonisation of legislation, policies and standards.

3.6.19 Existing legislation will be reviewed to ensure a synergy and that it meets with Constitutional obligations. A clear policy and guidelines for classification and declassification is needed to manage the protection as well as access of critical information.

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

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

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

3.6.21 The National Strategic Intelligence Act 39 of 1994 provides in sec 6 that the Minister (member of cabinet designated by the President to assume the responsibility for intelligence services as contemplated in sec 209 (2) of the Constitution) may, after consultation with the Joint Standing Committee on Intelligence, and in consultation with the relevant Government Departments affected, make regulations regarding inter alia the protection of information and intelligence. Draft regulations in this regard, intended to replace the MISS, are being discussed at present.

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

Full exclusion of critical information from privacy legislation

3.6.23 In so far as the question regarding the possible exclusion of critical information from the privacy legislation is concerned, it is interesting to note that countries in Europe have made limited use of the possibility to fully exclude critical information from their information privacy

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

100 A similar argument was posed by Liberty.

101 See also ENF for Nedbank.

laws.¹⁰² Denmark, Ireland, the UK (for national security)¹⁰³ and Spain are exceptions to this rule. They are the countries that have complete or almost complete, and in practice unchallengeable, exemptions from the information principles, the exercise of data subject rights, notification and enforcement.

Separate laws excluded

3.6.24 Some countries subject some or most processing in the areas listed to separate laws.¹⁰⁴ This does not, however, necessarily mean that they are not subject to a regime which is compatible with the principles of the Directive. Processing in connection with defence, security services, police matters etc is subject to special laws or rules which, in turn, must conform to the basis principles in the information protection law. See for instance the Netherlands, Italy, Luxembourg, Germany, Portugal, Sweden.

3.6.25 This is not to say that processing for the kinds of purposes mentioned above and which is subject to the national laws implementing the Directive does not benefit from extensive exceptions and exemptions within those laws. As is clear from Art 13(1) paras (a) -(g) the Directive expressly allows for exemptions and restrictions for the information protection principles, i.e. Art 6(1); the informing-requirements imposed on controllers under Arts. 10 and 11(1); the right of access, rectification or erasure (Art 12); and the duty to publicise details of processing operations (Art 21) with regard to such processing.¹⁰⁵

3.6.26 However, the Directive does impose two conditions in this respect: such exemptions or restrictions must be provided for in “legislative measures” and they must be “necessary” to safeguard the public interest in question. In terms of the Directive, compliance with these

102 Korff D *Comparative Summary of National Laws* EC Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49) Human Rights Centre Cambridge September 2002 (hereafter referred to as “Korff *Comparative Study*”) at 142.

103 Sec 28 stipulates as follows:

28. - (1) Personal data are exempt from any of the provisions of -

(a) the data protection principles,

(b) Parts II, III and V, and

(c) section 55,

if the exemption from that provision is required for the purpose of safeguarding national security.

(2) Subject to subsection (4), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions mentioned in subsection (1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact.

(3)-(12).....

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

105 Korff *Comparative Study* at 142.

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

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

3.6.27 Apart from the very wide exemption with regard to processing for the purpose of safeguarding national security,¹⁰⁶ the law in the UK includes a series of more limited exemptions for personal information processed in relation to crime and taxation matters, health, education and social work etc. Most of these exemptions are limited to what is referred to as “subject information provisions” ie informing-requirements and the data subject access requirements, but the crime and taxation exception extends to the “fair processing” principle.¹⁰⁷

3.6.28 The main point to be made about these exceptions is, however, that they all only apply to the extent that the full application of the provision from which they allow derogations “would be likely to prejudice” the matters concerned.¹⁰⁸ This means that the courts and the information

106 See footnote 102 above.

107 Korff *Comparative study* at 144; Section 29 (1) and (3) of the UK Data Protection Act 1998. Section 29 (1) reads:

‘Personal data processed for any of the following purposes-

- (a) The prevention or detection of crime
- (b) The apprehension or prosecution of offenders

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and Section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.’

Data Protection Principle 1 covers fair and lawful processing of data and the requirement to provide information to data subjects (Data Protection Notices on Applications and Agreements); Schedules 2 and 3 cover the conditions for processing and the conditions for processing sensitive data; Section 7 deals with the provision of information (subject access) to data subjects regarding the identity of the data controller, the purpose of the processing and the recipients of the data. The non-disclosure provisions relate to subject access.

Section 29 (3) reads:

‘Personal Data are exempt from the non-disclosure provisions in any case in which: -

- (a) The disclosure is for any of the purposes mentioned in subsection (1), and
- (b) The application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.’

108 The Information Commissioner also warned the Home office that the new powers enabling law-enforcement and intelligence agencies to demand the communications records of British telephone and internet users may breach human rights law because website, email or phone logs available strictly for national security investigations can be accessed by police or intelligence officers for more minor cases such as public health and tax collection. The law states that access to this information by law-enforcement agencies should only be on the grounds of national security or for investigating crime related directly or indirectly to national security. Stuart Millar, technology correspondent *The Guardian* July 31, 2002 accessed at

<http://www.guardian.co.uk/guardianpolitics/story/0,3605,765917,00.html> on 2002/08/02.

protection authority are able to assess the necessity of any such exceptions and their application in practice, in accordance with the Directive.¹⁰⁹

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

The Commissioner takes the view that, for any of these three exemptions to apply, there would have to be a substantial chance rather than a mere risk that in a particular case the purposes (crime prevention and -detection and taxation) would be noticeably damaged. The information controller needs to make a judgment as to whether or not prejudice is likely in relation to the circumstances of each case”.

3.6.30 In New Zealand sec 57 provides that nothing in principles 1-5 and 8-11 applies in relation to information collected, obtained, held or disclosed to, an intelligence organisation. Principles 6 and 7 deal with access to personal information and correction of personal information.

3.6.31 In the USA law enforcement agencies have immunity from almost every significant restriction in the Privacy Act.¹¹¹ In so far as national security is concerned, a system of records that is maintained by the CIA may be generally exempted from the Privacy Act’s access and amendment provisions as well as from the provision that the information should be collected directly from the data subject as far as possible.

South Africa

3.6.32 In South Africa, most respondents who commented on this issue agreed that it would be premature at this stage, to exclude critical data bases from all the information protection principles.¹¹²

3.6.33 Respondents reiterated the view of the Commission that the more critical the information, the more important it may be to ensure that the personal information collected is

109 Korff *Comparative study* at 144.

110 Korff *Comparative study* at 145.

111 Roos 1998 *THRHR* at 525.

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

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

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

3.6.35 A few respondents, however, felt that critical information should be excluded.¹¹⁶ It was stated that, without wishing to minimize the importance of a citizen's right to privacy, this country faces other issues, for example, that of crime, which must at least for the moment, take precedence. Accordingly, critical information must be excluded from the information protection laws altogether.¹¹⁷

3.6.36 This idea was further elaborated on by the SAFPS who wants to be excluded from the Act.¹¹⁸ It was therefore submitted that although the legislature should provide a measure of protection of privacy in general and informational privacy in particular, such protection must specifically exclude any requirement on the provision to consumers of information related to fraudulent activity and crime in general irrespective of whether such information is held by public or private bodies and organisations.

113 Vodacom; SABC; ENF for Nedbank.

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

115 The Internet Service Providers' Association.

116 Soc of Adv Natal; SAFPS; SAPS.

117 Soc of Adv Natal. The SAPS argued that full effect must be given to the Constitution in respect of privacy relating to data, but that proper limitations, as recognised in democratic societies which allow crime detection, investigation and intelligence functions, must be recognised and protected in the process.

118 Fraud Prevention databases would be able to continue to operate using a variety of data matching techniques (including address based systems and systems that use fuzzy matching techniques) to identify crime, without being constrained by arguments that such processing is unfair. These sophisticated data matching techniques are key tools in the fight against organised financial crime.

* Fraud prevention services and commercial organisations would not be required to provide details of the fraud and crime prevention processing they undertake to consumers as this would alert criminals and tip them off, save as allowed for in terms of the Promotion to Access of Information Act.

* Fraud prevention services and commercial organisations should be required to advise subjects implicated in fraud cases that data about them had been filed on fraud prevention databases.

* Consumers would not have a right of subject access to fraud prevention data as this would alert criminals to the possibility of apprehension and prosecution, would compromise investigations and lead to a different pattern of attack probably from a new location.

* Fraud prevention systems should not be open to public inspection.

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

3.6.38 In order to follow this route the legislation dealing with these matters will have to be harmonised. There are currently numerous acts involved. Some examples are:¹²⁰

- * Section 104 of the *Defence Act* 42 of 2002 deals with the improper disclosure of information;
- * Sec 11A of the *Armaments Development and Production Act* 57 of 1968 deals with the prohibition of disclosure of certain information;
- * Sec 4 of the *National Key Points Act* 102 of 1980 deals with the furnishing of information to the Minister;
- * The *Protection of Information Act* 84 of 1982 is a broad based act providing for the restriction of the disclosure of information.
- * Section 4 and 5 of the *Intelligence Services Oversight Act* 40 of 1994 deals with access to intelligence, information and documents and secrecy of information.
- * *National Strategic Intelligence Act* 1994 provides for the protection of information and intelligence.
- * Section 41 of the *Promotion of Access to Information Act* 2 of 2000¹²¹ deals with the national security ground of refusal to access to information.¹²²
- * Sec 56 of the *ECT Act* 2002 deals with the restrictions on the disclosure of information.
- * Sec 35 of the *Regulation of Interception of Communications and Provision of Communication-related Information Act* 70 of 2002 deals with the manner in and periods for which the information at the relevant centres should be kept.

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

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

121 See also discussion below.

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

3.6.39 The Commission therefore proposes that -

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

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

3.7 Sensitive information (special personal information)

3.7.1 The EU Directive lays down additional conditions (over and above the usual criteria for making processing lawful) for the processing of so-called “special categories of information (usually referred to as sensitive information).¹²⁴

3.7.2 Most European countries agree on the main categories of information to be regarded as sensitive information (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and information concerning health or sex life), but some add further categories (information on debts, financial standing, criminal convictions and the payment of welfare benefits).

3.7.3 In the document ‘Privacy Online: A Report to Congress (June 1998)’, the U.S. Federal Trade Commission also expressed their concern that information of a much more personal nature, such as race, health, financial standing, sexual orientation, is collected, frequently without any indication of how this information is subsequently to be used. In particular, the disclosure of such information to other parties must be controlled, if not prevented altogether. Very stringent rules should apply to processing sensitive information. In principle, such information should not be

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

124 Article 8(1) of the EU Directive provides as follows:

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

processed, however, derogation from the principle should be tolerated under very specific circumstances, such as:

- *where the data subject has given explicit consent to process sensitive information but then only in respect of the purpose for which consent has been given; and
- *the processing of sensitive information as mandated by law but then only to the extent that legitimate general public interest or state security outweighs the invasion of the privacy of an individual.

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

3.7.5 In principle the processing of sensitive information is therefore a cause for concern worldwide and therefore often subject to certain listed exceptions. These exceptions are usually set out in ways corresponding to the ones listed in the Directive.¹²⁵

125 Article 8(1) of the EU Directive provides as follows:

The processing of special categories of data

1.

2. Paragraph 1 shall not apply where:

- (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
- (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law insofar as it is authorized by national law providing for adequate safeguards; or
- (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
- (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
- (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of

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

3.8 Household activity

3.8.1 In the Issue Paper it was stated that the legislation will not cover personal information kept by a natural person in the course of a purely personal or household activity.

3.8.2 Mixed reaction was received on this question. Some respondents agreed with the Commission's preliminary view.¹²⁶ The Commission was, however, requested to explain, by way of examples, the exact meaning of information kept "*in the course of a purely personal or household activity*" since the phrase seems superficially to require exclusion but it was felt that it is rather vague.¹²⁷

3.8.3 It was pointed out that all types of information have a conceivable commercial value. For instance, names and postal addresses can be valuable for direct marketing. In modern society, even the number of socks a person has, their colours, sizes, and so on, also is potentially of enormous economic value.¹²⁸

3.8.4 Although this may be true, it is, however, important to note that some confusion can be prevented if one takes into account that it is not the nature of the information that is at stake here, but rather the use to which it is put by the collector. A directory of telephone numbers and addresses of friends or acquaintances kept for personal use at home, should therefore not be considered to be processing of personal information and need not be regulated by an information protection law.¹²⁹

general application may be processed.

126 LOA.

127 Financial Services Board.

128 LOA.

129 Roos 1998 *THTHR* at 523.

3.8.5 However, household information is growing exponentially in the modern world, and it is, of course, not always easy to determine when such information is purely for private use, or when there is economic potential, or potential for abuse,¹³⁰ but that will be a factual question.

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

3.9 Anonymised/de-identified information

3.9.1 The view was posed that "anonymised/de-identified information" should be exempt from the privacy legislation if it has been audited and proved to be unable to be re-identified. This is key to ensuring that compliance costs are kept to a minimum by business.¹³¹

3.9.2 The ability to identify a person - or reasonably ascertain a person's identity - from a piece of information is the key component that makes the information personal information.

3.9.3 Existing legislation and guidelines in use in South Africa do not adequately address the distinction between identifiable and non-identifiable information about individuals. Since the legislation makes no specific reference to de-identified information, it tends to treat all information about individuals as identifiable information, with corresponding tight restrictions on access to and processing of the information. Examples are:

- * The National Health Bill (latest available version, published November 2003, section 16) which makes very limited reference to circumstances under which patient records used contain 'no information as to the identity of the user concerned', but does not provide a description of what this means in practice.
- * The definition of 'personal information' used in the Promotion of Access to Information Act and other legislation, and
- * the definition of 'personal health information' in a recent report by the Council for Medical Schemes are so wide that it could be very difficult to de-identify information.¹³²

130 LOA.

131 IMS.

132 It was argued that the definitions of anonymised and de-identified data used in Issue Paper 24, reflect an important improvement on other legislation and guidelines, which do not provide any such definitions. These definitions will be very

3.9.4 It was pointed out¹³³ that the proposed legislation could address the issue of the differences in requirements for dealing with identifiable and de-identified information about individuals more effectively than has been the case up to now in South Africa legislation and guidelines.

3.9.5 This issue is of particular concern in public health research, which typically requires access to de-identified information from multiple patients. In the absence of guidelines in the legislation, there is a tendency to assume that access to all information on individuals requires specific consent, which is virtually impossible, especially in the case of large studies. Moreover, where information is de-identified, an argument could be made that the potential benefits of obtaining access to information for public health research far outweigh the small potential risk to individuals of using their information for such studies, but the current state of legislation makes it difficult to sustain such an argument. The collection and use of profiles and statistical information that are valuable for the purposes of monitoring issues of public health and safety, the conduct of medical research, epidemiological research and professional quality assurance programs: all of which contribute to an effective and accountable commercial environment, should not be undermined.

3.9.6 However, the Commission was referred¹³⁴ to the work done by Sweeney and Samarati that show that information can indeed be used in non-obvious ways to identify (some) individuals about whom ‘anonymous’ information has been recorded. The question was therefore posed whether such non-obvious techniques are ‘reasonably foreseeable’, given the fact that they have been reported in the scientific literature?

3.9.7 In practical and technical terms one would furthermore have to ensure that the definition of “processing” must not be interpreted so broadly as to capture the process of de-identifying information.¹³⁵ It was argued¹³⁶ that since “removal” may be interpreted as being interchangeable with “deletion”, a very strong case on the surface exists for the action of “de-identification” to be captured by the definition of “data processing”. This is obviously "at odds" with 'protecting'

useful in addressing issues related to de-identified and anonymised data even before the proposed Act comes into force, including the problem of definitions referred to above. The proposed Act will be even more helpful in this regard if the issues highlighted above are addressed in a way which can also be applied in the interpretation of related legislation.

133 Medical Research Council.

134 Prof Martin Olivier.

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

136 IMS.

personal information, given that the intention of the proposed legislation is to protect the privacy of the individual - not to hamper processes that enhance that right to individual privacy. Anonymisation enhances privacy of the individual and it should be able to be actively pursued by organisations that may collect personal information.

3.9.8 The question is therefore whether consent must be given for the de-identification of personal information to occur (i.e. consent to remove identifying details). **Comment is invited on this issue.**

3.9.9 In the USA the rules made under the Health Insurance Portability and Accountability Act of 1996 (the "HIPAA") have been brought into force¹³⁷. The HIPAA will apply to "individually identifiable health information". The definition of "health information" excludes professional provider information, as it applies only to information about the individual receiving health care. Once information has been de-identified – anonymised – it is deemed no longer to be identifiable health information and may be disclosed without restriction. However, if codes or other record identification methods are disclosed and allow subsequent re-identification of the information, or if the information is in fact re-identified, the previous restrictions apply. HIPAA is noteworthy amongst privacy statutes for setting out (at some length) standards and methods of how de-identification is to be undertaken.

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

3.10 Professional information (including provider information)¹³⁸

3.10.1 A submission was received on Issue Paper 24¹³⁹ proposing that "professional information" should be excluded from the proposed privacy legislation and that "provider information" should be recognised as a part of professional information.

137 Notwithstanding industry opposition, the rules came into effect on April 14, 2001, although most entities have two years in which to comply. See U.S. Department of Health and Human Services "Protecting the Privacy of Patients' Health Information" *HHS Fact Sheet*, 9 May 2001.

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

139 IMS.

3.10.2 "Professional information" was defined as:

- (a) the name, title, contact information, identifying code and professional designation of an identifiable individual , and
- (b) information describing the activities and transactions the individual has engaged in carrying out those responsibilities, including a description of those responsibilities when it is used for the purpose of describing the professional or official responsibilities of the individual".

3.10.3 The importance of this interpretation is that a distinction is drawn between information relating to the performance of the individual in their professional, official or business capacity where the information has the potential to influence public interest, national security and public health and safety and the same individual in their personal or private capacities.

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

3.10.5 It was furthermore proposed that in the health sector the definition of personal health information should be drafted to ensure that information about the employment and business responsibilities, activities and transactions of individual health service providers is not included. This type of information may be used to objectively assess the quality of provider services and should be considered professional in nature rather than personal health information.

3.10.6 It is certainly difficult to discern how an individual prescription can constitute personal information about the physician who wrote it. While it can be revealing with regard to the patient – the nature of an illness or condition, for instance, and perhaps its severity – it discloses little or nothing about the physician as an individual. The prescription is not, in any meaningful sense, "about" the physician.¹⁴¹ It does not tell us how he goes about his activities. Indeed, a prescription

140 For example, when a business negotiates a contract with a supplier, the business' staff and those of the supplier will prepare notes on the progress of the negotiations, setting out, amongst other matters, the position of the respective parties to the contract, comments on the negotiations etc. All of this information is provided in the individuals' professional capacity as a representative of the business. It is a business-to-business transaction. Any recorded information about the individual's views, or perspective on the proposed business arrangement is created and used solely because the individual represents a potential business partner – it bears no relation to the individual as an individual person. Rather it is important to business as it reflects the corporate position of the company they represent.

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

is not normally treated as personal information about himself or herself by the prescribing physician. The patient is not enjoined to secrecy, remaining entirely free to show it to anyone at will, or to leave it unattended in a public place.¹⁴²

3.10.7 It was argued that with the exclusion of "professional information" from the definition of "personal information" in information protection legislation, an individual's rightful expectation of personal privacy is met whilst ensuring that the individual remains accountable to society in their capacity as an employee, worker, public officer, government official or professional.

3.10.8 It was furthermore argued that provider information forms part of professional information. IMS Health Canada and USA use prescription sales information and various statistical methods to produce provider information in the form of estimates of normative prescribing patterns of physicians, as well as estimates respecting individual physicians' prescribing patterns. After tracking prescription trends, IMS Health Canada and USA then make the information available under strict contractual arrangements to pharmaceutical companies, health professional bodies, government, medical researchers and patient advocacy groups for a variety of purposes. These purposes provide a multitude of benefits to the health sector which enable the sector to provide more efficient, effective and transparent services.¹⁴³

3.10.9 IMS Health Canada only discloses estimates respecting an individual physician's prescribing patterns with the express consent of the individual prescriber; otherwise, provider information is disclosed only in aggregate form. In the aggregate format, actual prescribing activity of individual prescribers is not identified – rather, prescribers are assigned a number that depicts the average prescribing activity of members of the entire group

3.10.10 The public benefits that flow from access to provider information, including improving the efficiency of the health care system, clearly militate in favour of allowing wide access to this information.

3.10.11 Medical research, quality assurance of government health programs, efficient monitoring of healthcare funding requirements and fraud prevention all require that some health information be accessible. Prescription records, which neither identify a patient nor reveal the

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

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

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

3.10.12 The Commission has already proposed that de-identified information be excluded from the ambit of the Act.¹⁴⁴ This exemption will most probably provide the necessary relief sought in so far as provider information is concerned. It is, however, the Commission's preliminary opinion that professional information should be included in the definition of personal information in so far as it would be applicable. See also the discussion on juristic persons above. It is furthermore of importance to note that the Commissioner may authorise the processing of personal information under specified circumstances. See Chapter 4 below for a discussion of exemptions from the information principles.

3.11 Conclusion

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

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

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

3.11.3 Provision will also be made for responsible parties to approach the Commissioner for exemptions from specific information principles under specified circumstances. See Chapter 4 of the Bill below.

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

CHAPTER 2
GENERAL APPLICATION PROVISIONS

Application of this Act

3. This Act applies to-

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

144 See para 3.9 above.

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

146 "**personal information**" means information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to-

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- (b) information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
- (c) any identifying number, symbol or other particular assigned to the person;
- (d) the address, fingerprints or blood type of the person;
- (e) the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
- (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g) the views or opinions of another individual about the person;
- (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
- (i) the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
- (j) but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years;

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

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

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

Comment is invited in all instances.

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

Exclusions

- 4. This Act does not apply to the processing of personal information -
 - (a) in the course of a purely personal or household activity;
 - (b) that has been de-identified to the extent that it cannot be re-identified again;
 - (c) that has been exempted from the application of the information principles in terms of sec 33.¹⁵⁰

Saving

-
- 147 "record" means any recorded information -
 - (a) regardless of form or medium; and includes any -
 - (i) writing on any material;
 - (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment (whether hardware or software or both), or other device; and any material subsequently derived from information so produced, recorded or stored;
 - (iii) label, marking, or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
 - (iv) book, map, plan, graph, or drawing;
 - (v) photograph, film, negative, tape, or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced;
 - (b) in the possession or under the control of a public or private body, respectively;
 - (c) whether or not it was created by a public or private body, respectively; and
 - (d) regardless of when it came into existence;
 - 148 "responsible party" means the natural person, juristic person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
 - 149 The responsible parties referred to are prohibited from processing personal information, unless they designate a person or body in South Africa to act on their behalf in accordance with the provisions of this Act. For the purposes of application of this Act and the provisions based upon it, the said person or body shall be deemed to be the responsible party.
 - 150 Once the harmonisation of the legislation has taken place as recommended above in para 3.6.39 of the Discussion Paper, section 4 may read as follows:
 - 4. *This Act does not apply to the processing of personal information -*
 - (a) *in the course of a purely personal or household activity;*
 - (b) *that has been de-identified to the extent that it cannot be re-identified again;*
 - (c) *by or on behalf of the intelligence or security services referred to in theAct;*
 - (d) *for the purposes of implementing the police tasks defined in the Act;*
 - (e) *by the armed forces in terms of theAct with a view to deploying or making available the armed forces to maintain or promote the international legal order.*

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

This Act binds the State

6. This Act binds the State.

Comment is invited in all instances.

3.11.5 A final point to note in so far as the scope of the inquiry is concerned is, however, that although the primary focus of this investigation is that of data or information privacy, this area is also closely linked to other privacy concerns such as bodily privacy, territorial privacy, communications privacy and surveillance.¹⁵¹

3.11.6 As was stated in the Issue Paper it is clear that information privacy overlaps with all of these other privacy concerns in so far as problems of regulating the processing of the information gained as a result of intrusions (where those intrusions have been lawful) are concerned. One would need a good understanding of all of these areas to ensure that all rights likely to be affected or covered by any information privacy legislation are acknowledged and addressed. Proposed legislation will therefore have to be closely linked to legislation already in place in those areas and may even have to address problems where an area has not been regulated yet.

151 The Victorian Law Commission in Australia has recently published an Information Paper entitled "Privacy Law: Options for Reform" *Information Paper* 2001 available at www.lawreform.vic.gov.au. In this paper they briefly explored the meaning of the right to privacy and the challenges of the new technological age and then went on to examine five key dimensions of privacy which are recognised by their existing laws in order to determine which of those areas their Commission's work should focus on. These areas are the following:

- (a) bodily privacy: intrusions into a person's body, for example through DNA testing; biometric identification (hand scanning), drug tests, frisking of people, psychological testing of employees, blood tests from people suspected of carrying an infectious disease, and genetic testing (genetic privacy) by for instance insurance agencies. Intrusions are usually to obtain information about an individual.
- (b) territorial privacy: intrusions into a person's physical space, for example a home or business premises, using telephones and faxes for unsolicited tele-marketing, listening devices, concealed cameras, sensors, surveillance of e-mail and Internet browsing activity.
- (c) information privacy: access to information held by Government or private sector organisations, for example mailing lists, credit bureaux and information contained on public registers such as the electoral roll.
- (d) communications privacy: interception of private communications, for example telephone calls and e-mails; and
- (e) surveillance: use of surveillance devices, for example video cameras in public (shops, hospitals, streets) and private places.