

SUMMARY OF PRELIMINARY RECOMMENDATIONS

Privacy is a valuable aspect of personality. Data or information protection forms an element of safeguarding a person's right to privacy. It provides for the legal protection of a person in instances where his or her personal information is being collected, stored, used or communicated by another person or institution.

In South Africa the right to privacy is protected in terms of both our common law and in sec 14 of the Constitution. The recognition and protection of the right to privacy as a fundamental human right in the Constitution provides an indication of its importance.

The constitutional right to privacy is, like its common law counterpart, not an absolute right but may be limited in terms of law of general application and has to be balanced with other rights entrenched in the Constitution.

In protecting a person's personal information consideration should, therefore, also be given to competing interests such as the administering of national social programmes, maintaining law and order, and protecting the rights, freedoms and interests of others, including the commercial interests of industry sectors such as banking, insurance, direct marketing, health care, pharmaceuticals and travel services. The task of balancing these opposing interests is a delicate one.

Concern about information protection has increased worldwide since the 1960's as a result of the expansion in the use of electronic commerce and the technological environment. The growth of centralised government and the rise of massive credit and insurance industries that manage vast computerised databases have turned the modest records of an insular society into a bazaar of information available to nearly anyone at a price.

Worldwide, the surveillance potential of powerful computer systems prompt demands for specific rules governing the collection and handling of personal information. The question is no longer whether information can be obtained, but rather whether it should be obtained and, where it has been obtained, how it should be used. A fundamental assumption underlying the answer to these questions is that if the collection of personal information is allowed by law, the fairness, integrity and effectiveness of such collection and use should also be protected.

There are now well over thirty countries that have enacted information protection statutes at national or federal level and the number of such countries is steadily growing. The investigation into the possible development of information privacy legislation for South Africa is therefore in line with international trends.

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

transmitted outside the borders of the country of origin produced an interesting history of international harmonisation efforts, and a concomitant effort to regulate transborder information flows.

Two crucial international instruments evolved:

- a) The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and
- b) the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.

These two agreements have had a profound effect on the enactment of national laws around the world, even outside the OECD member countries. They incorporate technologically neutral principles relating to the collection, retention and use of personal information.

Although the expression of information protection in various declarations and laws varies, all require that personal information be dealt with according to specific principles known as the "Principles of Information Protection" which form the basis of both legislative regulation and self-regulating control.

Some account should also be taken of the UN Guidelines as well as the initiative of the Commonwealth Law Ministers in this regard. In both instances countries are encouraged to enact legislation that will accord personal information an appropriate measure of protection, and also to make sure that such information is collected only for appropriate purposes and by appropriate means.

In 1995, the European Union furthermore enacted the Data Protection Directive in order to harmonise member states' laws in providing consistent levels of protection for citizens and ensuring the free flow of personal data within the European Union. It imposed its own standard of protection on any country within which personal data of European citizens might be processed. Articles 25 and 26 of the Directive stipulate that personal data should only flow outside the boundaries of the Union to countries that can guarantee an "adequate level of protection".

Privacy is therefore an important trade issue, as information privacy concerns can create a barrier to international trade. Considering the international trends and expectations, information privacy or data legislation will ensure South Africa's future participation in the information market, if it is regarded as providing "adequate" information protection by international standards.

It should be noted that the promulgation of information protection legislation in South Africa

will necessarily result in amendments to other South African legislation, most notably the Promotion of Access to Information Act 2 of 2000, the Electronic Communications and Transactions Act 25 of 2002 and the, still to be enacted, National Credit Bill [B18-2005]. All these Acts contain interim provisions regarding information protection in South Africa.

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

- a) Privacy and information protection should be regulated by a general information protection statute, with or without sector specific statutes, which will be supplemented by codes of conduct for the various sectors and will be applicable to both the public and private sector. Automatic and manual processing will be covered and identifiable natural and juristic persons will be protected [**Chapter 2, clauses 3-6**].
- b) General principles of information protection should be developed and incorporated in the legislation. The proposed Bill gives effect to eight core information protection principles, namely processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, individual participation and accountability. Provision is made for exceptions to the information protection principles [**Chapter 3, Part A, clauses 7-23**]. Exemptions are furthermore possible for specific sectors in applicable circumstances [**Chapter 4, clauses 32-33**]. Special provision has furthermore been made for the protection of special (sensitive) personal information [**Chapter 3, Part B, clauses 24-31**].
- c) A statutory regulatory agency should be established. Provision has been made for an independent Information Protection Commission with a full-time Information Commissioner to direct the work of the Commission [**Chapter 5, Part A, clauses 34-46**]. The Commission will be responsible for the implementation of both the Protection of Personal Information Act (see Annexure B) and the Promotion of Access to Information Act, 2000. Data subjects will be under an obligation to notify the Commission of any processing of personal information before they undertake such processing [**Chapter 6, Part A, clauses 47-51**] and provision has also been made for prior investigations to be conducted where the information being collected warrants a stricter regime [**Chapter 6, Part B, clauses 52-53**].
- d) Enforcement of the Bill will be through the Commission using as a first step a system of notices where conciliation or mediation has not been successful. Failure to comply with the notices will be a criminal offence. The Commission may furthermore assist a data subject in claiming compensation from a responsible party for any damage suffered. Obstruction of the Commission's work is regarded in a very serious light and constitutes a criminal offence [**Chapter 8, clauses 63-87 and Chapter 9, clauses 88-92**].

¹
Bill

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

- e) A flexible approach should be followed in which industries will develop their own codes of conduct (in accordance with the principles set out in the legislation) which will be overseen by the regulatory agency. Codes of conduct for individual sectors may be drawn up for specific sectors on the initiative of the specific sector or of the Commission itself. This will include the possibility of making provision for an adjudicator to be responsible for the supervision of information protection activities in the sector. The Commission will, however, retain oversight authority. Although the codes will accurately reflect the information protection principles as set out in the Act, it should furthermore assist in the practical application of the rules in a specific sector [**Chapter 7, clauses 54-62**].

- f) It is the Law Commission's objective to ensure that the legislation provides an adequate level of information protection in terms of the EU Directive. In this regard a provision has been included that prohibits the transfer of personal information to countries that do not, themselves, ensure an adequate level of information protection [**Chapter 10, clause 94**].

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