

SUMMARY OF PROPOSALS AND QUESTIONNAIRE

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

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

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

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

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

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

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

international trends.

Early on, it was, however, recognised that information privacy could not simply be regarded as a domestic policy problem. The increasing ease with which personal data could be transmitted outside the borders of the country of origin produced an interesting history of international harmonisation efforts, and a concomitant effort to regulate transborder data flows.

Two crucial international instruments evolved:

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

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

Although the expression of data protection in various declarations and laws varies, all require that personal information must be:

- obtained fairly and lawfully;
- used only for the specified purpose for which it was originally obtained;
- adequate, relevant and not excessive to the purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure; and
- destroyed after its purpose is completed.

These principles are known as the "Principles of Data Protection" and form the basis of both legislative regulation and self-regulating control.

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

means.

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

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

The effectiveness of data protection provisions in protecting an individual's personality rights will, however, depend largely on how they are applied and interpreted in practice. In this regard it has been argued that the rules for data protection come from three distinct perspectives, namely political, economic and technological:

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

Four models aimed at the protection of personal information can be identified. Depending on their application, these models can be complementary or contradictory. In most countries several are used simultaneously.

First of all, there is a general law that governs the collection, use and dissemination of personal information by both the public and private sectors. An oversight body then ensures compliance. This is the preferred model for most countries adopting data protecting laws and was adopted by the European Union to ensure compliance with its data protection regime.

Secondly, some countries have avoided enacting general data protection rules in favour of specific

sectoral laws governing, for example, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. A major drawback with this approach is that it requires that new legislation be introduced with each new technology - protection therefore frequently lags behind. There is also the problem of a lack of an oversight agency.

Thirdly, data protection can also be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. This is currently the policy promoted by the governments of the United States and Singapore.

Finally, with the recent development of commercially available technology-based systems, data protection has also moved into the hands of individual users. It is possible to employ a range of programs and systems that provide varying degrees of privacy and security of communications.

Governments may find that proposed measures to protect privacy meet the staunch opposition of business interests which see such safeguards as an expense and an unjustified constraint on their right to conduct their business affairs as they wish. On the other hand, business interests may be enhanced by a statutory data protection regime. Many countries, especially in Asia, have developed or are currently developing data protection laws in an effort to promote electronic commerce. These countries recognise that consumers are uneasy with the increased availability of their personal data, particularly with new means of identification and forms of transactions, and therefore that their personal information is being utilised worldwide. Data privacy laws are therefore being introduced, not from a human rights perspective, but rather as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.

It should be noted that the promulgation of data protection legislation in South Africa will necessarily result in amendments to other South African legislation, most notably the Promotion of Access to Information Act 2 of 2000 and the Electronic Communications and Transactions Act 25 of 2002. Both these Acts contain interim provisions regarding data protection in South Africa.

The preliminary proposals of the Commission can be summarised as follows:

- a) privacy and data protection should be regulated by legislation;**
- b) general principles of data protection should be developed and incorporated in the legislation;**
- c) a statutory regulatory agency should be established;**
- d) a flexible approach should be followed in which industries will develop their own codes of practice (in accordance with the principles set out in the**

legislation) which will be overseen by the regulatory agency.

The Commission is seeking feedback regarding all these proposals. Comments will be appreciated and taken into account in drafting the Data Privacy Bill.

Questionnaire:

In order to facilitate discussion, various questions have been posed throughout the document and readers are encouraged to provide feedback on all these different issues. Please note that readers do not have to limit their comments to these issues. For ease of reference a list of the questions are repeated here:

- 1) What should the scope of this inquiry be? Should the investigation include:
 - a) automatic and manual files?
 - b) information pertaining to both natural and juristic persons?
 - c) information kept by both the public and the private sector?
 - d) sound and image data?.
 - e) critical data?
 - f) personal information kept in the course of a purely personal or household activity?
[Para 1.3.12]

- 2) What are the duties of the legislature insofar as the protection of privacy in general and informational privacy in particular are concerned? [Para 3.4.4]

- 3) What is the relationship between the Constitution and the common law of privacy? Does the Constitution's conception of privacy differ from that of the common law?[Para 3.4.4]

- 4) Should a distinction be drawn between the public and the private sector in drafting privacy legislation and if so, what should these differences be. [Para 4.1.4]

- 5) Do you think that existing legal remedies provide adequate protection to consumers against the collection and sharing of information by credit bureaux that may be misleading or incorrect? What are the views of the credit bureaux regarding the principles to be embodied in the proposed legislation? [Para 4.3.14]

- 6) The Commission is interested in the views of both consumers and marketing agencies regarding direct marketing practices. Does practice indeed match theory? [Para 4.3.22]

- 7) Do patients feel comfortable in providing personal medical information to physicians, hospitals and medical aid schemes? The Commission invites comment from health authorities with regard to the following areas:
 - * genetic engineering
 - * special considerations about the needs of minors;

- * information provided to spouses, dependants, and other next of kin;
 - * public health reporting;
 - * fraud and abuse investigations. [Para 5.7.20]
- 8) Is there a need for statutory regulation in so far as financial privacy is concerned? If so, what should the nature of such regulation be ? [Para 4.3.52]
- 9) The Commission has noted that in-depth studies dealing specifically with privacy in the workplace are currently being conducted worldwide. Is there a need for such research in South Africa? [Para 4.3.61]
- 10) How should a proposed Privacy Act interact with existing legislation dealing with privacy issues for example the Promotion of Access to Information Act, the Electronic Communications and the Transactions Act and the Financial Centre Act? [Para 5.2.17]
- 11) Does the opt-out approach constitute a valid consent of the consumer? If so, why? If not, why not? What are the implications for consumers and industry if opt-out consent is allowed? [Para 5.4.23]
- 12) Should institutions be allowed to share data, and if so, under what circumstances. What should the consent requirements be in this regard? In sharing data, who is responsible for the accuracy and maintenance of the data? [Para 5.5.15]
- 13) What are the perceptions of the public regarding
- a) the current information collection practices of government?
 - a) the accuracy and maintenance of information held by government?
 - b) the benefits on the one hand and risks on the other to be derived from integrated data sharing in government. Do people recognise the available safeguards and trust them ? [Para 5.5.28]
- 14) Do readers see data profiling as a natural element of marketing practice or is it an unacceptable infringement of the individual's privacy. What should the consent requirements be? [Para 5.6.10]
- 15) Have security issues been dealt with adequately in the ECT Act or should additional provision be made for the security protection of personal data in accordance with the principles of data protection? Comment is furthermore welcomed regarding practical issues surrounding identity theft, a practice which seems to have become a major problem for

financial institutions and their customers. [Para 5.8.30]

- 16) Should all the so-called principles of data protection be incorporated in a Data Privacy Act? If so, how? The principles are:
- Principle 1: Fair and lawful processing
 - Principle 2: Openness
 - Principle 3: Collection Limitation
 - Principle 4: Use/Purpose Specification
 - Principle 5: Disclosure Limitation
 - Principle 6: Individual participation
 - Principle 7: Data Quality
 - Principle 8: Finality
 - Principle 9: Security Safeguards
 - Principle 10: Accountability
 - Principle 11: Sensitivity
- [Para 6.2.125]
- 17) Should South African privacy legislation make provision for a statutory regulatory authority? What should the level of this authority be? Where should it be housed? [Para 7.2.35]
- 18) Would it adversely affect the country's international trade if a model is adopted that is not regarded as "adequate" in terms of Article 25 of the EU Directive? If so, how? [Para 5.3.9]

The Commission invites comment on all these issues. Respondents who prefer to direct their comments at selected questions only, are welcome to do so.