

EMBARGO: FOR IMMEDIATE RELEASE

MEDIA STATEMENT BY THE SOUTH AFRICAN LAW REFORM COMMISSION

**PROJECT 124: PRIVACY AND DATA PROTECTION
(Discussion Paper – Closing date for comment: 28 February 2006)**

The South African Law Reform Commission is at present conducting an investigation entitled "Privacy and Data Protection" (Project 124). The investigation was included in the programme of the Commission at the request of the Minister for Justice and Constitutional Development.

The Minister has appointed a Project Committee for this investigation to assist the Commission in its task. The Chairperson of the Committee is Mr Justice Craig Howie. Prof Johann Neethling has been appointed as project leader and the other members are Prof Iain Currie, Ms Caroline da Silva, Ms Christiane Duval, Prof Brenda Grant, Ms Adri Grobler, Mr Mark Heyink, Ms Saras Jagwanth and Ms Allison Tilley.

The Commission hereby releases a Discussion Paper and a draft Bill for information and comment. The return date for comments is 28 February 2006.

Privacy is a valuable aspect of personality. Data or information protection forms an element of safeguarding a person's right to privacy. The essence of information protection is to provide a person with (a degree of) control over his or her personal information in instances where his or her personal information is being collected, stored, used or communicated by another person or institution.

The recognition and protection of the right to privacy as a fundamental human right in the Constitution provides an indication of its importance. It is, however, not an absolute right and in protecting a person's personal information, consideration should 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 computer and telecommunications technologies. Worldwide, the surveillance potential of powerful computer systems has prompted demands for specific rules governing the collection and handling of personal information. In addition, the use of and reliance on electronic information for aiding in all kinds of decision-making processes have reached critical levels in all walks of life. For example, the increasingly wide-spread use of on-line shopping, telebanking and electronic funds transfer services has given rise to new sources of personal information concerning a person's spending habits and lifestyles. Extensive medical records are now kept on computers by both hospital authorities and private insurers alike. Thanks to computer networking, this plethora of personal information can be accessed from many different locations and transferred amongst them easily and quickly. In addition, different information sources may be easily mixed and matched in any desirable way so as to create highly sensitive and private personal 'electronic profiles' which, apart from being used by the primary owners of the information, may be made available to anyone who is willing to pay. In reality decisions having major impacts on individuals (such as whether a loan is granted, a sensitive job is offered, or a life insurance proposal is accepted) are all too often made on the basis of these 'electronic profiles' without necessarily having confirmed their accuracy or perhaps without the knowledge of the individuals concerned.

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. Examples are the United Kingdom (Data Protection Act 1998); Canada (Privacy Act 1983 and Personal Information Protection and Electronic Documents Act, 2000), Australia (Privacy Act, 1988 and The Privacy Amendment (Private Sector) Act 2000), New Zealand (Privacy Act 1993) and most European countries. The investigation into the development of information privacy legislation for South Africa is therefore in line with international trends.

Early on it was, furthermore, 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 a history of international harmonisation efforts, and a concomitant effort to regulate transborder information flows.

In 1995, the European Union enacted the Data Protection Directive which states that countries

lacking adequate information protection law will be denied general access to personal information from these states possessing it. Privacy is therefore an important trade issue, as information privacy concerns can create a barrier to international trade. South Africa cannot afford to be denied general access to personal information from its major trading partner countries, most of which have already implemented proper information protection legislation.

The preliminary recommendations of the Commission, as set out in the Bill accompanying the Discussion Paper, can be summarised as follows:

- X The protection of personal information in the public and the private sector should be regulated in an act of general application, called the Protection of Personal Information Act, supplemented by codes of conduct for specific sectors. Both automatic and manual processing of information will be covered and identifiable natural and juristic persons will be protected.
- X The proposed Bill gives effect to eight core information protection principles which, inter alia, prescribes the following duties and obligations for responsible parties and provides for the following rights for data subjects (i.e. persons whose information is being collected):
 - * information can only be collected or stored if it is necessary for or directly related to a lawful, explicitly defined purpose and does not intrude upon the privacy of the data subject to an unreasonable extent;
 - * information must be collected directly from and with the consent of the data subject;
 - * data subjects must be informed of the purpose of any such collection and of the intended recipients of the information, at the time of collection;
 - * information must not be kept for any longer than is necessary for achieving the purpose for which it was collected;
 - * information must not be distributed in a way incompatible with the purpose for which it was collected;
 - * reasonable steps must be taken to ensure that the information processed is accurate, up to date and complete;
 - * appropriate technical and organisational measures have to be taken to safeguard the data subject against the risk of loss, damage, destruction of or

unauthorised access to personal information;

- * data subjects are allowed a right of access to their personal information and a right to demand correction if such information should turn out to be inaccurate.

- X Exceptions to the information protection principles are provided for and exemptions are furthermore possible for specific sectors in applicable circumstances. Special provision has furthermore been made for the protection of special (sensitive) personal information such as those revealing racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasions, trade union membership, health and sexual life.
- X Provision has been made for an independent Information Protection Commission with a full-time Information Commissioner to direct the work of the Commission. The Commission will be responsible for the implementation of both the new, envisaged Protection of Personal Information Act and the current Promotion of Access to Information Act 2 of 2000. Data subjects will be under an obligation to notify the Commission of any processing of personal information before they undertake such processing. Provision has also been made for investigations to be conducted by the Commission prior to commencement of the processing to establish whether it complies with the law in instances where the nature of the information being collected warrants a stricter regime.
- X 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 .
- X A flexible approach will 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.

- X 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, except under special circumstances, to countries that do not, themselves, ensure an adequate level of information protection.

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 issues raised 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. The Commission will also be organising regional workshops at which members of the Project Committee will be present to explain and discuss proposed solutions set out in the Bill and to note comments.

The manner in which the investigation will further progress will primarily depend on the response received from interested parties. Parties who would like to become involved in the investigation, be included in the Commission's mailing list or attend the forthcoming workshops are invited to submit their particulars to the Law Commission.

Comments and submissions should be addressed to:

The Secretary
SA Law Reform Commission
Private Bag X668
PRETORIA
0001

Telephone: (012) 392-9540
Fax: (012) 320-0936
E-mail: analouw@justice.gov.za
Internet: www.doj.za/salrc/index.htm

ISSUED BY THE SECRETARY, S A LAW REFORM COMMISSION, PRETORIA

DATE: 13 OCTOBER 2005

**THE CONTACT PERSON FOR ENQUIRIES IN RESPECT OF MEDIA STATEMENT IS
MS ANANDA LOUW**

TEL (012) 392 9566 (OFFICE)

analouw@justice.gov.za

EMBARGO: FOR IMMEDIATE RELEASE