Computer technology and information privacy rights of the individual

Summary

Computerisation has greatly facilitated the storage, collection, retrieval and transfer of personal information for government functions. However, at the same time, opportunities for inappropriate unauthorised or illegal access to and use of personal information have expanded. Studies indicate that the assurances the individual seeks against such abuse and misuse can be provided by the successful application of privacy and information protection legislation. In countries such as the United States, Norway, Canada, Sweden, Britain and Australia legislative measures based on privacy and information protection principles have been instituted. As the institution of a Bill of Rights will feature prominently in a constitutional negotiation to ensure a fair and democratic South Africa, the time is now opportune to take steps to establish measures for a general privacy and information protection law. The legislative measure should consider inter alia scope and application, definitions, codes of practice, establishment of the office of privacy and information protection ombudsman, information protection principles, computer matching and data linkage, and enforcement measures.

Dr D Sing, Mr MS Bayat,
Dept of Public Administration,
University of Durban-Westville, Private Bag X54001, Durban, 4000
Sing & Bayat/Information privacy rights of the individual

“Homo sapiens, who stood at the dawn of the first material civilization at the end of the last glacial age, is now standing at the threshold of the second, the information civilization after ten thousand years.” – Yonju Masuda

“The information revolution means that I may find out everything about anything. But is also means I may learn more about you than you want me to know.” – David Bazelon

“There can be no doubt that the new technologies benefit our society by improving economy and efficiency. But these benefits come at a price. The developments in information technology have serious implications for privacy and individual liberties. Many commentators reflected on the emergence of the transparent person about whom almost everything is known and nothing that is known is forgotten.” – T Cohen

“Privacy is personality and its eclipse is also the eclipse of human rights.” – K lyer

1. Introduction

In this paper the nature and meaning of information privacy is described, followed by a discussion on the nature of information technology. Examples illustrating the impact of the abuse and misuse of information technology on information privacy are cited. This is followed by a description of information protection principles. In the latter part of the article attention is given to developments in South Africa. As a concluding thought a legislative scheme is recommended for privacy and information protection in South Africa.

2. Information Privacy

In a report on the legal protection of privacy published in the International Social Journal in 1972, it was stated as follows:

“Nearly everyone wants to keep some part of his life, his thoughts, his emotions, his activities private to himself or to chosen members of his family and friends. The extent of this private life, the area of privacy, will vary from person to person, from group to group, from society to society and vary also according to different ages, traditions and cultures. But though the area of privacy may vary the desire for privacy is universal."

The New South Wales Privacy Committee Report explains that there are

three types of privacy:

1. Territorial Privacy - an individual's interest in having a physical domain within which he can be left in solitude and tranquillity;
2. Privacy of the Person - an individual’s interests in being protected from physical harassment or subjection to indignity; and
3. Information Privacy - an individual’s interest in controlling the collection, storage and circulation of information about himself.

Therefore, it could be stated that information privacy is the social expectation that an individual:

1. will be treated fairly and accurately by information taking systems;
2. will be protected against intrusive collection of information; and
3. should have a legitimate enforceable expectation that records maintained about him will be treated as confidential.

3. Information Technology

The significance of computerization in the processing of personal information is attributable to four of its features.

1. The huge storage capacity of computers with their ability instantly to collate and produce any part of what is stored;
2. The ease with which systems can communicate with one another;
3. The extensive means available for rapid dissemination and presentation of information; and
4. The enhancement of data by cross matching it with data from other sources.

Although computerization has enabled public institutions to collect, store, process, retrieve and transfer information more efficiently, economically and comprehensively opportunities for inappropriate, unauthorised or illegal access to and use of personal information in government institution computer records have expanded. The latter development has implications for the information privacy of the individual. The dangers of increasing computerization of personal information include the possibility that inaccurate, incomplete or irrelevant data can be used as the basis for important decisions affecting the lives of the citizens. This danger was emphasized by the Privacy Protection Study Commission of the United States. It stated as follows:

"We live inexcappably, in an 'information society', and few of us have the op-

3. Ware 1979:243.
tion of avoiding relations with record keeping organizations. To do so is to forgo not only credit but also insurance, employment, medical care, education and all forms of government services to individuals. This being so, each individual has or should have a concern that the records organizations keep about him do not lead to unfair decisions about him. 7

The technique variously called computer-matching or computer linkage involves the electronic comparison of two or more sets of separate and unrelated records. This technique makes it possible to screen almost instantly, vast and disparate sets of personal information in search of similarities and differences. Through this technique it is possible to build up a picture of an individual citizen's life style, habits and relationships of which he knows nothing but which is used in making decisions about his military service or welfare grant. Furthermore, it makes possible for the linker to consider a lifetime of information when making a decision about a particular citizen. This information may include dated records of minor traffic offences and health problems all of which may unfairly reflect on the current situation of the individual concerned. This connection which is established between different items of information concerning a citizen, is used as the basis for passing judgement on him, a secret judgement from which there can be no appeal and which because it is based on a computer, is thought to be objective and infallible. 8

The Privacy Commissioner of Canada advocated that computer matching be challenged as a tool even to achieve desirable goals. The reason is that it violates the individual's right to prevent information from being used without his or her consent for a purpose other than for which it was collected. 9

Some examples illustrating the inappropriate, unauthorised or illegal access to and use of personal information are cited below:

1 A nursing home resident in the United States lost Government medical assistance after her bank and welfare records were matched. What the match did not reveal was that some of the money in her savings account was exempt from asset calculations because it was held in trust for burial expenses. 10

2 A man was arrested for being absent without leave from the marine Corps of the United States eleven years after he had been legally discharged. A computer matching programme found him to be absent without leave. He was held for five months before the error was corrected. 11

3 Two complaints were made to the Privacy Commissioner of the Wanga-

7 Miewald 1978:185.
8 Report 1972:419.
11 Galloway 1984:47.
nui Computer Centre concerning the misdescription of offences for which convictions had been entered. These resulted from the coding system for related or similar offences. The original text in each case was corrected to show the true nature of the offence. For example, possession of cannabis for own use instead of possession of cannabis for purpose of supply, and common assault instead of aggravated assault. Report: Wanganui Computer Center 1982:3.

iv A trainee terminal operator at the Wanganui Computer Centre admitted to making queries into the computer about his friends and relatives and verbally passing some of this information to other members of the family in the course of general conversation.12

v Early in 1986 15 000 Swedes discovered that they were unknowingly guinea pigs in a sociological survey. The project continued under three successive governments over a period of 20 years. The person numbers of most Swedes are recorded in over 100 data banks in the public and private sectors. Medical, educational, welfare, police employment and other records were accessed without consent in this secret survey.13

vi A New Orleans sculptor was afraid to travel to Mexico to meet his fiancée's grandparents. While crossing the border over the past years, he has been seized at gunpoint by U.S. police force and jailed once. The problem is that a federal computer identifies the sculptor as a fugitive because a real fugitive sometimes uses his name and social security number.14

vii The United States Privacy Journal reported that in settlement of a lawsuit the Rode Island Registry of Motor Vehicles has agreed never to sell or rent data on its 700 000 licensed drivers. Names, ages, motor vehicle details and addresses of licence holders were sold or rented to commercial mailing houses.15

These examples point to the fact that:

"Like all our tools, the computer itself is morally neutral. How it will affect us will depend on what people want to do with it, what they are able to do with it and ultimately what we shall allow them to do with it."16

4. Information Privacy Protection Principles

Studies on the subject of abuse of information technology and private interests have produced fairly general agreement that the assurances that the indi-

16 Sieghart 1976:3.
individual citizen seeks can be provided by the successful application of certain principles. Sieghart's formulation of these principles are as follows:

1. The principle of public notice – All computer systems holding personal information should be publicly known.
2. The principle of right data – Personal information held in computer systems should be accurate, complete and timely.
3. The principle of security – Personal information held in computer systems should be adequately secured against unauthorised access.
4. The principle of legitimacy – Personal processed information in computer systems should be collected and used only for legitimate purposes.
5. The principle of minimum data traffic – Personal information should pass through computer systems only to the minimum extent and for the minimum time necessary for the legitimate purpose.
6. The principle of subject verification – the data subject should be able to verify and correct all information held about him in any computer system, and discover how it has been used.
7. The principle of independent supervision – Some independent supervisory official should be able to enforce these principles fairly.

Several countries including Sweden, Norway, Netherlands, United States, New Zealand, Australia, Canada and Britain have enacted legislation based on these principles. To give effect to the principles of independent supervision, officials such as Data Protection Registrars and Privacy Commissioners who are in fact specialist ombudsmen have been appointed. Flaherty stresses the importance of such officials as follows:

"....An individual in the late twentieth century can no longer adequately protect his or her privacy without the assistance of regulatory authorities." 18

5 Developments in South Africa

In South Africa, as in other countries, a number of statutes have been introduced to compel individuals to submit certain personal information about themselves to the State. Examples of such legislation include the Statistics Act, the Income Tax Act and the Identification Act. 19

For example, Section 6 of the Identification Act, requires from every person whose name is to be included in the population register personal particulars such as a person's identity number, date and place of birth, ordinary place of

17 1976:11.
18 Canada 1984, 1985:5.
19 McQuoid-Mason 1978:160.
residence, postal address, occupation particulars as to his marriage as contained in his marriage register.

The Identification Act poses a particular threat to a person's privacy by the State, as it allows the Director-General for Home Affairs to furnish information to any state department, local authority or statutory body for any other purposes, and to any other person (who makes written application and pays the prescribed fees) provided the Director-General is satisfied that it is in the interest of the person registered to furnish the particulars. However, the person registered is not required to consent to the disclosure nor is he informed as to who has received the information. 20

Provisions exist in the Statistics Act, the Income Tax Act and the Identification Act that prohibits the disclosure of information by officials outside the course of their official duties. 21

For example, Section 4(1) of the Income Tax Act, 1962, states that “every person employed in carrying out the provisions of this Act shall preserve and aid in preserving secrecy with regard to all matters that may come to his knowledge in the performance of his duties in connection with these provisions and shall not communicate such matter to any person whatsoever other than the taxpayer concerned or his lawful representative nor suffer or permit any such person to have access to any records in the possession or custody of the Commissioner except in the performance of his duties under this Act or by order of competent court.”

Somewhat similar provisions exist in the Public Service Act, 1984. A public servant is guilty of misconduct if he “without first having obtained the permission of his head of department, discloses, otherwise than in carrying out his official duties, information gained by or conveyed to him through his employment in the public service, or uses that information for any purpose other than for carrying out his official duties, whether or not he discloses that information.” Apart from the limited protection given in certain statutes to personal information South Africa lacks a general privacy and information protection legislation.

Formal steps have already been taken in South Africa to find legislative and administrative measures for protecting the information privacy of the individual. The most recent step was taken in January 1987 when the South African Law Commission was requested by the Director-General of National Education to institute a thorough investigation into “the way in which the right to privacy and reputation of the individual are protected by the legal system within the context of the computer.” 22

The African National Congress in its Bill of Rights for a Democratic South

20 McQuoid-Mason 1978:197.
21 McQuoid-Mason:197.
Africa makes provision for the right to privacy of the individual citizen. The provisions are as follows.\(^\text{23}\)

i. No search or entry shall be permitted except for reasonable cause as prescribed by law and as would be acceptable in an open and democratic society.

ii. Interference with private communications, spying on persons and the compilation and keeping of secret files about them without their consent, shall not be permissible save as authorised by law in circumstances that would be acceptable in an open and democratic society.

6. Conclusion

It is certain that the institution of a Bill of Rights will be promised in any constitutional negotiation to ensure a just and democratic South Africa. Any legislative measure to protect and promote the information privacy rights of the individual should take cognisance of the following aspects:

a. Scope and Application

The goal should be the protection of information privacy and not merely information protection. Consideration should be given to whether the legislation will apply only to the public sector or to the private sector as well.

b. Definitions

Attention must be given to the most important definition, namely that of 'personal information'.

c. Information protection principles

The principles should be the centre-piece of the legislation. The success of the legislation will depend to a large extent on how these principles are framed. As statements of principle they will necessarily be expressed in broad terms.

d. Codes of practice

There should be provision for the development of Codes of Practice set for application to specific types of records and public authorities and new forms of technology.

\(^{23}\) Robertson 1991:229.
e Computer Matching and Data Linkage

Programmes which involve data matching using the records of more than one public authority should be reported to the Privacy and Information Protection Ombudsman.

f Transborder Data Flows

The legislation should address the issue of transborder data flows by requiring that data should only be transferred out of a country where the transfer is required by law, or treaty or where the receiving party can ensure equivalent data protection.

g Enforcement: Offences and Remedies

The legislation should create a limited range of offences for the most serious and wilful breaches of information protection principles.

h Establishment of the Office of the Privacy and Information Protection Ombudsman

This Office should be funded by statutory appropriations.

i Functions and powers of Ombudsman

The ombudsman should be given advisory and investigatory powers.

j Review by Parliament

Provision should be made for the establishment of a Parliamentary Joint Committee to monitor and review the exercise by the Ombudsman of his powers and functions.
GALLOWAY JL

INTERNATIONAL COMMISSION OF JURISTS

MCQUOID-MASON DJ
1978. The law of privacy in South Africa. Cape Town: Juta and Company Ltd.

MIEWALD RD

NEW SOUTH WALES PRIVACY COMMISSIONER
1983/84. Reports. Canada.

PITT DC AND SMITH BC (ed.)

REGAN PM

ROBERTSON M (ed)

SIEGHART P

SOUTH AFRICAN LAW COMMISSION

WANGZANUI COMPUTER CENTRE PRIVACY

WARE HW