

## CHAPTER TWO

### PRIVACY AND DATA PROTECTION

#### 2.1 INTRODUCTION

Throughout the Inquiry the concepts of the privacy of individuals and protection of personal data held on public Registers, particularly computerised Registers, were considered. The Committee was mindful of the considerable concern expressed in the community about the accumulation of personal information on government data bases: "... the spectre of Big Brother, and the debate about the Australia Card, are never far from the surface when the storage of government information is discussed."<sup>11</sup>

It has been argued that the development of technology with the capacity to cross-match computer files and store a wide range of personal data has not been matched in New South Wales either by legislation or the acceptance and adoption of privacy guidelines. Currently, a person who believes that their privacy has been invaded has little redress or control over how, or to whom, their information is released, or how it is used or construed. The argument for greater protection of personal data is widening as new technology expands in capability.

The Committee examined the protective measures for the privacy of individuals which exist in other countries, and reviewed the need for guidelines and legislation relating to New South Wales. Although data protection is a broad issue relating to the collection, storage and dissemination of data across a range of areas, the Committee focused on this issue only as it specifically relates to the Registry.

#### 2.2 BACKGROUND

The need to protect information which might be passed on to others without the consent of the person concerned became a matter of increasing concern in the 1960s. It was suggested then that there were three types of information about people: first, information which is private and should not be available to members of the public; second, information which is sensitive and should have limited availability; and last, information which is a matter of public record. Determining what information is sensitive or private

---

<sup>11</sup> Independent Commission Against Corruption, 1992, Vol 1, p.10

for an individual is complex and depends on subjective, cultural and societal issues. Any assessment of privacy needs to be made in light of the value of personal data to the broader interests of society. Time is also relevant, as facts or personal data which are sensitive today may not be sensitive in the future.<sup>12</sup>

The increased trans-border flow of information in the 1970s emphasised the need to ensure that similar types of data would be protected in different countries and between states. Without compatible approaches to data protection, some organisations could be reluctant to transmit data to or through countries which did not provide a degree of protection. Further, unscrupulous data users could escape the requirements of national legislation by transferring their data processing to a country which did not have data protection laws. The legislation and regulations which have developed in Europe have consequently focussed on two distinct areas, privacy regarding media coverage, and data protection measures, particularly in relation to the information processing capacity of computers.<sup>13</sup>

The first European initiative followed the 1968 Parliamentary Assembly of the Council of Europe. A Committee of Ministers was convened to:

explore the extent to which the Human Rights Convention and the domestic laws of the member states offered protection for information relating to individuals.<sup>14</sup>

The Committee of Ministers' findings indicated that there was inadequate privacy protection for individuals. The Committee resolved in 1973 and 1974 to establish principles of data protection in both the private and public sectors.

An "expert group" of the Organisation for Economic Co-operation and Development (O.E.C.D.) was convened to identify the "basic rules" for the protection of privacy for member countries.<sup>15</sup> Australia's representative to that group, the Hon Justice Michael Kirby, AC, CMG, was elected Chairman of the group. In 1980 the O.E.C.D. guidelines were adopted. That same year Australia also ratified the *International Covenant on Civil and Political Rights*, which recognises the right of an individual to privacy.

---

<sup>12</sup> Moore, 1991, p.183

<sup>13</sup> Ibid, p.185

<sup>14</sup> Ibid.

<sup>15</sup> Australian Law Reform Commission, 1980, p.23

---

The principles in the O.E.C.D. guidelines were embodied in 1984 in the British *Data Protection Act*, which attempted to create a balance between individual privacy and the free trade of information. The main objectives of the legislation were to educate the public on data protection issues and to influence and change attitudes and practices within Britain. In Britain and Europe data protection legislation has led to a wider awareness of the methods of international transmission of data.<sup>16</sup>

### 2.3 LEGISLATION AND REGULATION IN AUSTRALIA

Legal recognition of information privacy has progressed in Europe, the United States and Canada at a greater pace than in Australia. As previously stated, Australia adopted O.E.C.D. guidelines and in the same year, the *International Covenant on Civil and Political Rights* was ratified. That Covenant recognises the right of an individual to privacy. Since that time, the Privacy Committee of New South Wales has developed data protection guidelines.

The Commonwealth *Privacy Act 1988* outlined data protection principles to be applied in relation to information collected and stored by Commonwealth government organisations. However, as recently as August 1992, the Independent Commission Against Corruption noted that:

There is no established legal definition of the right to privacy. It is nonetheless acknowledged as an essential element of individual freedom and human dignity.<sup>17</sup>

#### 2.3.1 The Commonwealth *Privacy Act 1988*

The Commonwealth *Privacy Act 1988* was introduced to address privacy concerns relating to the collection and handling of personal information by Commonwealth government agencies and employees of those agencies. Specifically, the Act includes the following eleven principles:

---

<sup>16</sup> Moore, 1991, p.184

<sup>17</sup> Independent Commission Against Corruption, 1992, p.176

---

personal information shall not be collected or made available unless it is collected for a purpose that is lawful and directly related to and necessary for a function, purpose or activity of the collector;

the collector of personal information should take steps to ensure that the individual concerned is aware of the purpose for which data is collected, whether the collection is authorised or required under law, and to which agencies the information is usually disclosed;

where a collector solicits personal information for inclusion in a generally available publication or record, the data is relevant to the purpose for collection, complete and up to date, and that the collection of the data does not unreasonably intrude into the personal affairs of the person concerned;

a keeper of a record containing personal information shall ensure that reasonable security safeguards are used to protect that information from loss, unauthorised access, use, modification, disclosure or other misuse;

a record-keeper should maintain records which specify for each record its nature, purpose, class of individual, period retained, who has access and the steps required to gain access;

a keeper of a record containing personal information should give access to the individual concerned, except where refusal is authorised under Commonwealth legislation;

specific steps be followed when alteration or deletion of records containing personal information occurs and that such steps consider: the purpose of the collection of the data and legislative provisions concerning accuracy;

the record-keeper must check the accuracy of personal information before its use;

a keeper of a record containing personal information should ensure that the data is only used for the purpose for which the information is relevant;

a record-keeper should ensure that the use of personal information is limited to the purpose for which it was obtained, except under specified circumstances; and

a record-keeper shall not disclose records containing personal information except under specified circumstances.

At the time the legislation was adopted, provision was made to ensure that some data protection principles applied to data collected prior to the implementation of the Act. Data protection principles number one, two, three, ten and eleven of the Act were designed to apply both to the collection process and access to data collected after the commencement of the Act.<sup>18</sup> In this way data collected by Commonwealth agencies before and after the implementation of the Act was protected.

### 2.3.2 Privacy Committee of New South Wales

The *Privacy Committee Act 1975* established the Privacy Committee of New South Wales which commenced operations on 2 May 1975. As a statutory Committee, independent of government, the Privacy Committee of New South Wales acts as a privacy ombudsman and conducts research and educational work on the issue of privacy.

The Privacy Committee of New South Wales has developed eleven data protection principles. In developing the principles, the Privacy Committee drew on a number of guidelines from international organisations, including the O.E.C.D.'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*; the Council of Europe's *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)*; and the European Commission's *Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data (1990)*. The principles are also based on the Information Privacy Principles contained in the Commonwealth *Privacy Act 1988*.<sup>19</sup>

The privacy principles developed by the Privacy Committee of New South Wales vary in a minor way from those contained in the Commonwealth *Privacy Act, 1988*. They include a number of additions which are said to take into account recent international developments in data protection, particularly from the European Commission.<sup>20</sup> In

---

<sup>18</sup> *Privacy Act 1988*, principles 1, 2, 3, 10 & 11 to apply to information collected prior the commencement of the Act to and principles 4 - 9 to apply to information collected after the commencement of the Act.

<sup>19</sup> Organisation for Economic Co-operation and Development, 1981

<sup>20</sup> Submission 64. Part B. Privacy Committee of New South Wales, p.69

---

particular, an amendment has been made to Principle 4, Principles 8 and 9 have been merged and an additional Principle 11 included. The last principle, number 11, seeks to ensure that information related to ethnic/racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life should not be disclosed without the written consent of the individuals concerned. These principles are appended to the Report in Appendix 3. The variations from and additions to the principles in the *Privacy Act, 1988* are highlighted in italics.

In October 1992, at the International Data Protection and Privacy Commissioners' Conference held in Sydney, the Executive Member of the Privacy Committee of New South Wales was critical of the failure of organisations and government bodies within New South Wales to adopt privacy principles. The Privacy Committee of New South Wales is an advisory body with no power to implement its privacy and data protection guidelines. It appears that the guidelines from the advisory body have not been widely adopted throughout New South Wales.

### 2.3.3 Data Protection Bill 1992

No privacy or data protection legislation has been enacted in New South Wales. There was in 1992 a Data Protection Bill "lying on the table" before the New South Wales Parliament, introduced as a Private Member's Bill by Mr A A Tink, MP. In evidence before the Committee, Mr Tink indicated that the Bill differed from the Commonwealth *Privacy Act 1988* in a number of sections.<sup>21</sup> Further, Mr Tink said that the Bill "sets out some proposals for criminal provisions relating to the offering for sale or selling of information in a way that ... I (would) describe as corrupt." He also indicated that the Bill incorporates data protection principles based on those developed in Europe and that the Bill is "essentially educative rather than punitive."<sup>22</sup>

### 2.3.4 Independent Commission Against Corruption

In the report of the Independent Commission Against Corruption, *Unauthorised Release of Government Information*, comment is made on the *New South Wales Data Protection*

---

<sup>21</sup> Evidence. Tink, 30.7.92, p.67. Sections 1, 2E, 2F, 2G, 3B, 3C, 4A-D, 5B, 7, 9 and 11 of the *Data Protection Bill 1992* were indicated to be different.

<sup>22</sup> Evidence. Tink, 30.7.92, p.61

---

*Bill 1992*. The view expounded in that Report is that the Bill relates to offences and persons who disclose, supply or handle information without authorisation.<sup>23</sup>

Among the issues examined in the Report were the accuracy of data; the standard of privacy to be adopted; determining the "public good"; consistency of data collection; ownership of data; and legislation.<sup>24</sup> Relevant recommendations concerned:

- . the development of a policy in respect of what government information is to be publicly available, and what protected;
- . the release of publicly available information;
- . security and access to government information storage and retrieval systems;
- . removing the restrictions proposed in the *Data Protection Bill 1992*; and
- . consistent application of legislation.

Whilst the unauthorised use of government information is an important issue, detailed examination of the issue was beyond the scope of the Terms of Reference before the Committee.

## 2.4 THE REGISTRY AND DATA PROTECTION PRINCIPLES

The New South Wales Law Reform Commission's Report, *Names: Registration and Certification of Births and Deaths* was prepared in 1988, the same year that the Commonwealth *Privacy Act 1988* was enacted. Without clear principles to govern the recording, storage of and access to records of births, deaths and marriages, the Commission sought guidance from three sources. These included the *Guidelines for the Operation of Personal Data Systems* propounded by the Privacy Committee of New South Wales, privacy guidelines stated by the Australian Law Reform Commission in its *Report on Privacy* and principles gathered from freedom of information legislation from Victoria

---

<sup>23</sup> Independent Commission Against Corruption, 1992, pp.173-174

<sup>24</sup> Ibid. p.176

---

and the Commonwealth.<sup>25</sup> The New South Wales Law Reform Commission formulated three principles for general application, viz:

- . only the minimum personal data necessary should be sought and recorded;
- . care should be taken to ensure the accuracy of all information recorded; (and)
- . access to the information should be consistent with the socially accepted purposes of the Register.<sup>26</sup>

The Commission indicated in its Report that the Registry generally followed these principles. It also determined that, while only the minimum personal data should be recorded, all data that was currently recorded served a range of useful purposes.

Evidence before the Social Issues Committee addressed the tension among principles of privacy, freedom of information and the use of information in the public interest.<sup>27</sup> Issues raised concerned the accuracy of data held, the need for the subject of an entry to be able to access and verify data, the protection of privacy and the use of personal data for commercial purposes. These issues are discussed in Chapter 4 of the Report.

The Committee considered the data principles outlined in the Commonwealth *Privacy Act 1988*, *New South Wales Data Protection Bill 1992* and the data protection principles of the Privacy Committee of New South Wales. The principles within these documents were considered in relation to the data collected and data made available for research and to the public. The Committee considers that it is a priority for New South Wales that data protection principles be enacted in legislation.

---

<sup>25</sup> Privacy Committee of New South Wales, Paper No.31; Australian Law Reform Commission 22, Privacy, AGPS, 1983; *Freedom of Information Act 1982* (Vic) and *Freedom of Information Act 1982* (Australia).

<sup>26</sup> NSW Law Reform Commission, 1988, para 4.3, p.25

<sup>27</sup> Evidence. Rose, 18.9.92

---



**Recommendation 1:**

- . That data protection principles be enacted in New South Wales in legislation, as a priority.

---