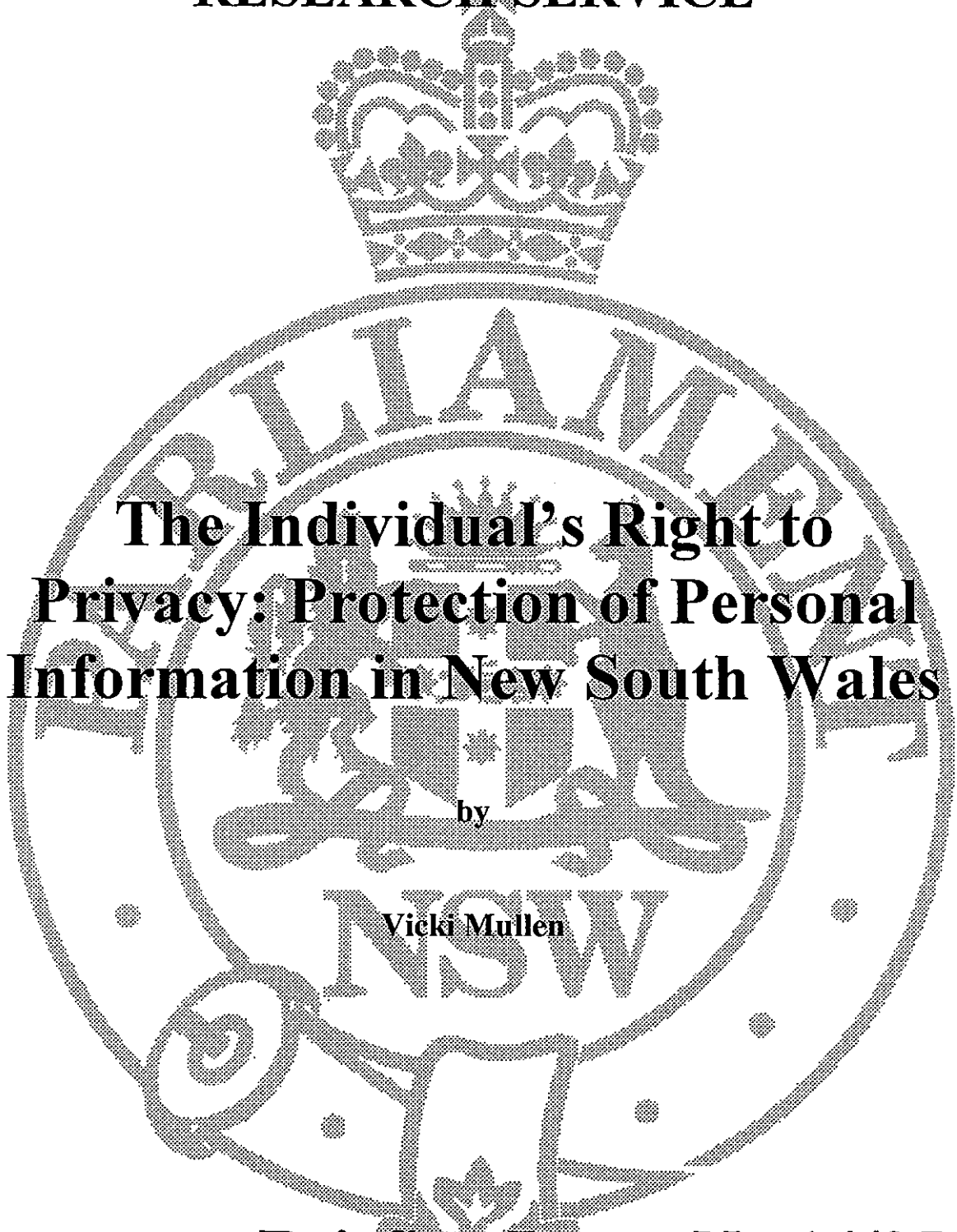
NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE



The Individual's Right to Privacy: Protection of Personal Information in New South Wales

by

Vicki Mullen

Briefing Paper No 14/95

The Individual's Right to Privacy: Protection of Personal Information in New South Wales

by

Vicki Mullen

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Dr David Clune (230 2484) Manager

Dr Gareth Griffith (230 2356) Senior Research Officer, Politics and Government

Ms Vicki Mullen (230 2768) Research Officer, Law

Ms Jan Newby (230 2483) Senior Research Officer, Statistics

Ms Marie Swain (230 2003) Research Officer, Law

Mr Stewart Smith (230 2798) Research Officer, Environment/Science

Mr John Wilkinson (230 2006) Research Officer, Economics

ISSN 1321-2559
ISBN 0 7310 5907 7

Should Members or their staff require further information about this publication, please contact the author.

April 1995

Briefing Paper is published by the NSW Parliamentary Library

CONTENTS

EXECUTIVE SUMMARY

This *Briefing Paper* discusses personal information privacy in New South Wales and the need for greater protection from misuse of such information, in particular by government agencies, in the wake of information technology advances. Competing rights in the public interest, which may conflict with personal information privacy interests, are considered. The main findings include:

- As increasing amounts and a greater variety of information about individual citizens are able and required to be held and stored by government agencies, concern has increased as to the exact and proper use of such information (page 4).

- The misuse of personal information can have serious tangible consequences for an individual. However, privacy should be protected not only as a practical or tangible matter, but also as a value that underpins human dignity (pages 4-7).

- The right of an individual to privacy is recognised and protected according to international agreements and covenants. However the current legislative protections of personal information privacy in NSW seem largely to be piecemeal and less than effective in giving enforceable privacy rights to individuals with respect to the *misuse* of personal information (pages 7-16).

- Sophisticated information technology empowers public officials to access and use information in ways that were previously impossible. The speed and ease of accessing vast amounts of information are a real threat to privacy (pages 16-18).

- The community has already reacted to these threats to privacy with the development of the Australian Privacy Charter (Public Release Draft) of October 1994, as a means of raising public awareness and as a reminder to government of the need to legislate for effective protections (pages 18-19).

- The public interest will operate at times as a counter-balance to an individual's right to personal information privacy. Freedom of information laws go some way towards enshrining the public's right to know, although personal information is also protected to an extent. A constitutional implied freedom of communication with respect to political discourse has been held to exist in recent decisions of the High Court as an essential element of a representative democracy. This implied freedom could have implications, in certain circumstances, for legislative protections of personal information (pages 19-22).

- The modern challenge is to raise awareness of the increasing threat to personal information privacy, and to respond with a change in attitudes and effective legislation (pages 22-23).

1. INTRODUCTION

It has been claimed that:

> government agencies are the leading invaders of the personal privacy of citizens since they maintain the largest and most numerous personalized information systems.[1]

This *Briefing Paper* is about the protection of personal information from misuse, in particular by government agencies, and the closely related issue of data protection and security as relevant to the issue of personal information. Technological developments in information collection, dissemination, storage and management are common to both issues as a driving force behind the need to effectively regulate the security and protection of information from misuse in both the public and private sectors.

No-one lives in a vacuum in a modern society and it is inevitable that certain amounts of information concerning an individual will begin to accumulate in government data-banks from the individual's date of birth. It could be said that the less sceptical members of a democratic society will assume that a relationship of trust exists between the government and an individual in relation to the use of such information for the specific purposes of the collection only. As increasing amounts and a greater variety of information about individual citizens are able and required to be held and stored by government agencies, concern has also increased as to the exact and proper use of such information. This concern has placed the trust relationship between government and individuals under scrutiny, particularly in light of blatant breaches of this trust, that have occurred in recent times.[2]

2. INDIVIDUAL PRIVACY AND PERSONAL INFORMATION - CURRENT AND PROPOSED PROTECTIONS IN NSW

The concepts of privacy and personal information

It is recognised that on a conceptual level, 'privacy' is difficult to define due to its numerous implications. However, as a general guide, 'privacy' has been defined as

> the state of being private and undisturbed...a person's right to this...freedom from intrusion or public attention...avoidance of publicity.[3]

---

1 The Privacy Committee of New South Wales, *Privacy Law in the Information Age,* Seminar Proceedings, No 61 June 1990, p 8.

2 See the report by the Independent Commission Against Corruption, *Report on Unauthorised Release of Government Information,* August 1992.

3 *The Australian Concise Oxford Dictionary* (2nd edition), Oxford University Press, 1992, p 902.

A further definition from the Public Release Draft of the Australian Privacy Charter of October 1994 identifies privacy as a collection of rights:

> Privacy encompasses bodily (physical), territorial privacy (private space), privacy of communications (rights concerning information about a person), and freedom from unwanted surveillance. These categories sometimes overlap.[4]

On what basis, therefore, is privacy a '"value" worthy of protection'?[5] In particular, why is it considered important that personal information held by public bodies and agencies is not available for general distribution to other agencies or the public at large? The importance of privacy with respect to personal information is a difficult principle to dispute. However, it is interesting to examine some practical reasons why, even in the face of a strong public interest, individuals expect to have information about themselves protected from the prying eyes of the world. The use of personal information by parties other than the body or agency that has the legal right to hold and use the information, may impact negatively on the interests of the individual. Obvious examples of potentially adverse (depending on the user of the information) personal information would include medical and police reports, employment and criminal records, information concerning political or religious affiliations and refused licence applications. The release of such information for purposes other than the legitimate and legal purpose of collection could have severe, long-term and negative consequences for an individual.

Further, information such as addresses, telephone numbers, car registration numbers, marital status, employment status and age may be considered to be neutral information. However, again, depending on the intended use of the information, such knowledge could also be used in a way that would have negative effects for an individual. Examples of this would be age discrimination, the receipt of unsolicited material (for example, in the case of direct marketing) or even a threat to personal safety. Personal information can obviously be used in ways that have a tangible effect on an individual's life.

However, beyond the obvious desire of an individual to have personal information protected that could cause negative events to occur if released to certain bodies or parties, there is also, in a democracy, a fundamental belief in the general freedom of an individual to conduct his or her life without undue scrutiny, whether or not such scrutiny would have a negative effect. A relevant function of privacy has been identified as the provision of personal autonomy on the basis that the 'democratic principle of individuality is linked to the need for autonomy' or the desire of an individual 'to avoid being

---

4 The Charter was reproduced after an article by Cameron, J, 'Draft Australian Privacy Charter released', (1994) 1(7) *Privacy Law and Policy Reporter,* 136.

5 Wacks, R, *Personal Information, Privacy and the Law,* Clarendon Press, Oxford, 1989, p 3.

manipulated or dominated by others.'[6] Therefore, the desire of an individual for privacy with respect to personal information could be said to have a practical or tangible as well as a mental basis as relevant to an individual's sense of self. The importance of privacy has been thus described:

> A free and democratic society requires respect for the autonomy of individuals, and limits on the powers of both State and private organisations to intrude on that autonomy.
>
> Privacy is a value which *underpins human dignity* (emphasis added) and other key values such as freedom of association and freedom of speech.[7]

A further conceptual issue that should be considered is the meaning of 'personal information'. In all events the issue of what is 'personal' may be subjective and relative to a particular individual. Nevertheless, the following objective definition has been proposed:

> 'Personal information' consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him [or her] to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation.[8]

Where the collection and use of personal information by government agencies is at issue, an objective definition is essential. It would be an administrative nightmare to assess the status of information as personal or otherwise on a case by case basis. 'Personal information' has also been simply defined as 'information about an *identified* (emphasis added) person, no matter how it is stored (eg: sound, image, data, fingerprints).'[9] This definition suggests that to be 'personal', information must be capable of leading to the identification of a particular individual. Therefore, for example, general statistics of the incidence of HIV in a particular community could not be classed as 'personal information', unless those statistics in some way were capable of identifying particular individuals. This example illustrates the importance of the determination of what information should be classed as 'personal'. It could be said that most information could be easily identified as being personal or otherwise. However, there would no doubt be cases where the capacity of information to disclose the identification of an individual would be less than clear, if such capacity depended on the particular and prior knowledge of the user of the information.

---

6 Ibid, pp 11-12.

7 The Australian Privacy Charter (Public Release Draft), op cit note 4.

8 Wacks, R, op cit note 5, p 26.

9 The Australian Privacy Charter (Public Release Draft), op cit note 4.

The definition of 'personal information' (as adopted from the *Privacy Act 1988* (Cth)) in clause 3 of the (lapsed) Privacy and Data Protection Bill 1994 (NSW) reflected these aspects so that 'personal information' was defined as 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.

International principles

The *International Covenant on Civil and Political Rights* (the 'ICCPR') was ratified by Australia on 13 August 1980.[10] This Covenant forms Schedule 2 of the *Human Rights and Equal Opportunity Commission Act 1986* (Cth). Article 17 of the ICCPR deals with the right to privacy and states:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

The effect of this international recognition of an individual's right to privacy was strengthened (to an extent) in Australia in 1991, when Australia acceded to the *First Optional Protocol to the International Covenant on Civil and Political Rights*. This enables an individual to bring a case for infringement for a right under the Covenant before the United Nations Human Rights Committee, but only 'after an individual has exhausted all available domestic remedies, or where the relevant legal processes have been unreasonably delayed.'[11] It goes almost without saying that the official right to appear before the UN Human Rights Committee is laudable. However, the exercise of this right would be (in most cases, prohibitively) expensive, particularly as the domestic legal hoops need to have been previously navigated.

In addition to Article 17 of the Covenant, privacy protection was, in the 'developed' international community, recognised as having economic importance, with the development in 1980 by the OECD of *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* as a result of the closer attention paid by this organisation to the 'social and legal consequences of the technologies which underpin

---

[10] CCH Industrial Law Editors, *Australian and New Zealand Equal Opportunity Law and Practice* (Looseleaf Service), 1991 CCH Australia Limited, para [3-715].

[11] Ibid.

modern economic development.'[12] It could be said that these guidelines have had an important and practical impact on the increased international recognition of privacy protection and have contributed to a global approach to and jurisprudence surrounding privacy laws.

> The OECD Guidelines on Privacy proved highly influential in the development of Australia's laws on that topic...[and] with some modification and development, the principles were incorporated in Pt III of the *Privacy Act 1988* (Cth).
>
> In other OECD countries, the principles have likewise formed the basis of legislation on privacy protection. They have also been adopted in the private sector, including by several multi-national corporations across national borders, as the basis of internal policy for the due protection of personal privacy in their data flows. ... It was the reduction of the economic inefficiencies of disparate treatment of the subject of privacy protection which propelled the OECD into what was, for it, the novel activity of offering guidelines for the laws and practices of Member Countries.[13]

The OECD Guidelines include basic principles on the following issues: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness and individual participation.[14]

The Privacy Committee Act 1975 (NSW)

On 2 May 1975, the Privacy Committee of NSW was established as a 'privacy ombudsman'[15] with the commencement of the *Privacy Committee Act 1975*. The functions, powers and duties of the Committee are set out in section 15 of the Act so that the Committee (under subsection (1)):

> (a) may conduct research and collect and collate information in respect of any matter relating to the privacy of persons;

---

12 Shearer, IA, 'New OECD Guidelines for the Security of Information Systems', (1993) 67(6) *The Australian Law Journal*, 460.

13 Ibid.

14 For the full text of these principles, see Volume 1 of the report by the ALRC, 'Privacy', *Report No 22*, Australian Government Publishing Service, Canberra, 1983, p 270 - 272.

15 The Privacy Committee of New South Wales, op cit note 1, p iii.

(b) may and, if directed by the Minister so to do, shall make reports and recommendations to the Minister in relation to any matter that concerns the need for or the desirability of legislative or administrative action in the interests of the privacy of persons;

(c) may make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons;

(d) may receive and investigate complaints about alleged violations of the privacy of persons and in respect thereof may make reports to complainants;

(e) may, in relation to any matter relating to the privacy of persons generally, disseminate information and undertake educational work;

(f) may, in relation to any matter relating to the privacy of persons generally, make public statements; and

(g) may, for the purposes of this Act, conduct such inquiries and make such investigations as it thinks fit.

Section 16 makes further provisions with respect to the powers and protections of the Committee so that, in relation to any inquiry or investigation conducted by it,

> the Committee shall have the powers, authorities, protections and immunities conferred on a Commissioner by Division 1 [which deals with Commissions generally] of Part II of the Royal Commissions Act, 1923, and that Act...applies to any witness summoned by or appearing before the Committee in the same way as it applies to a witness summoned by or appearing before a commissioner...

The Privacy Committee has primarily an advisory and investigatory role in the management and monitoring of privacy issues in NSW. It has never had any effective powers to enforce privacy principles on the public or private sector. The Committee has been recommending the introduction of data protection legislation since 1982.[16] The problems of the lack of effective legislation in NSW to deal with privacy breaches in relation to personal information were sharply illustrated with the exposure (as reported in 1992) by the Independent Commission Against Corruption of the widespread and corrupt

[16] The Privacy Committee of New South Wales, *Privacy and Data Protection in New South Wales, A Proposal for Legislation,* Submission to the Independent Commission Against Corruption, No 63 June 1991, p 1.

use of personal information held by certain government agencies.[17]

> The members of [the 'information exchange club'] include police officers; employees of the Roads and Traffic Authority (RTA); employees of many other local, state and federal government authorities and public utilities; private inquiry agents; debt collectors, solicitors, real estate agents, banks, credit unions and insurance companies. The common interest of club members is the trade in confidential, personal information.
>
> Personal information provided in good faith (and, frequently, under legal compulsion) by the citizens of New South Wales is being bartered and sold on a breathtaking scale. Our privacy is being sold and the proceeds of the sale are lining the pockets of the corrupt.[18]

The recommendations of the Privacy Committee (and ICAC) have been approaching realisation with the evolution of the (now lapsed) Privacy and Data Protection Bill 1994 (discussed below).

The Freedom of Information Act 1989 (NSW)

It has been said that:

> The Federal FOI Act contains provisions relevant to one of the central issues common to most international and national statements of information privacy principles. I refer to the so-called 'individual participation principle' by which, to enhance the exercise of a measure of control over information about himself or herself, a record subject is guaranteed the right to have access to the records and, consequently, to correct them so far as they are inaccurate, misleading, out-of-date, incomplete or irrelevant to the legitimate purposes for which they are kept.[19]

Documents affecting *personal affairs* are protected and the right of individual participation also exists under the *Freedom of Information Act 1989* (NSW) which deals generally with public access to information held by government agencies.

Section 31 of this Act operates so that an agency must consult a person before access to a

---

17 Independent Commission Against Corruption, *Report on Unauthorised Release of Government Information*, August 1992.

18 The Privacy Committee of New South Wales, op cit note 16.

19 Transcript of speech given by The Hon Justice MD Kirby CMG, 'Privacy Protection in Australia: An Update', National Forum on Access to Information and Privacy, Department of Justice, Canada, Ottawa, Canada, 7 March 1986, pp 7-8.

document which contains information *concerning* the personal affairs of that person, is given. Subsection (2) states

> An agency shall not give access to a document to which this section applies (otherwise than to the person concerned) unless the agency has taken such steps as are reasonably practicable to obtain the views of the person concerned as to whether or not the document is an exempt document by virtue of clause 6 of Schedule 1.

Clause 6 of Schedule 1 accords the status of exempt documents to documents containing matter the disclosure of which would involve the *unreasonable* disclosure of information concerning the personal affairs of any person. A definition of 'personal affairs' is not given in the Act. It is suggested that it would be interpreted more narrowly than 'personal information' (see below). If the person concerned has the view that the document is exempt under clause 6 of Schedule 1 and the agency decides to act contrary to this view, the agency must not give access to the document without notifying the person concerned of such decision. In addition, the agency must notify the person concerned (section 31(3)):

(i) that the person has rights of review, appeal and complaint; and

(ii) of the procedures to be followed for the purpose of exercising those rights.

The agency must 'defer giving access to the document until after the expiration of the period within which an application for a review or appeal under this Act may be made or, if such an application is made, until after the application has been finally disposed of.'

In relation to the effective protection that is afforded by the NSW Act, it is interesting to consider the level of protection at a federal level. Section 41 of the *Freedom of Information Act 1982* (Cth) deals with the exempt status of documents affecting personal privacy so that, according to subsection (1):

> A document is an exempt document if its disclosure under the Act would involve the unreasonable disclosure of *personal information* (emphasis added) about any person...

On 25 October 1991, section 41 of the federal Act was amended by the *Freedom of Information Amendment Act 1991* (Cth) by omitting the words 'information relating to the personal affairs of' and substituting 'personal information about'.

'Personal information' is defined, according to section 4 of the federal Act as 'information or an opinion (including information forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.

It is suggested that the use of the words 'personal information' in the federal Act would protect more private information from disclosure under the freedom of information provisions than would the concept in the NSW Act of a 'document that contains information concerning the personal affairs of any person'.

Part 4 of the *Freedom of Information Act 1989* (NSW) deals with the right of an individual to amend certain records held by an agency. Section 39 provides that

> A person to whom access to an agency's document has been given may apply for the amendment of the agency's records:
>
> (a) if the document contains information concerning the person's *personal affairs* (emphasis added); and
>
> (b) if the information is available for use by the agency in connection with its administrative functions; and
>
> (c) if the information is, in the person's opinion, incomplete, incorrect, out of date or misleading.

As to the refusal by an agency to amend records, see sections 44-46 of the NSW Act.

Part V of the *Freedom of Information Act 1982* (Cth) deals with the amendment and annotation of personal records.

The Crimes Act 1900 (NSW)

In certain circumstances, unlawful access to and misuse of personal information by government agencies, could constitute criminal conduct.

Section 309 provides for the offence of unlawful access to data in a computer. Subsection (1) states

> A person who, without authority or lawful excuse, intentionally obtains access to a program or data stored in a computer is liable, on conviction before two justices, to imprisonment for 6 months, or to a fine of 50 penalty units or both.

Subsection (2) states that

> A person who, with intent:
>
> (a) to defraud any person; or

(b) to dishonestly obtain for himself or herself or another person any financial advantage of any kind; or

(c) to dishonestly cause loss or injury to any person,

obtains access to a program or data stored in a computer is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

It is interesting to note that the offence under subsection (2) does not require that access was made without authority or lawful excuse. Therefore the section would apply to official or legal users of particular computer data who have illegal intentions in relation to the access to the program or computer data.

Further, subsection (3) provides for the offence of intentional and unlawful access to a program or data stored in a computer, if the person obtaining access 'knows or ought reasonably to know' that such information relates to:

(a) confidential government information in relation to security, defence or inter-governmental relations; or

(b) the existence or identity of any confidential source of information in relation to the enforcement or administration of the law; or

(c) the enforcement or administration of the criminal law; or

(d) the maintenance or enforcement of any lawful method or procedure for protecting public safety; or

(e) *the personal affairs of any person (whether living or deceased)* (emphasis added); or

(f) trade secrets; or

(g) records of a financial institution; or

(h) information (other than trade secrets) that has a commercial value to any person that could be destroyed or diminished if disclosed.

The penalty for such an offence is also 2 years imprisonment or a fine of 500 penalty units or both.

Subsection (3) in particular may appear to be a wide-ranging provision. However, it has its limitations. Many of the categories from (a) to (g) in subsection (3) could have implications for the protection of personal information, and the offences under section 309

generally extend to the public and private sector. However, the offences only cover access to computer data, and not manual records. Further, subsections (1) and (3) only deal with persons who illegally access information. These subsections do not cover the event of *misuse* of information by those who have lawful access to such information. The situation of access to personal information by those who have lawful access is only dealt with by subsection (2) in cases where such a person intends to dishonestly or illegally use the information. In this instance the problem arises as to when the intent was formed. For example, a government employee may legally access certain information with legitimate intentions, and may later use such information for financial gain after the event of access.

With respect to unauthorised dealings in government information generally, the comment has been made that:

> The relevant law is riddled with gaps and inconsistencies. Possessing, handling, buying and selling government information or confidential information, is not an offence. Thirty-nine different New South Wales statutes have been identified which prohibit the unauthorised disclosure of information from different Government departments or agencies, or from particular records maintained by them. ...
>
> Despite those scattered, specific and inconsistent provisions, neither unauthorised access to government information generally, nor its unauthorised release, constitutes a criminal offence in New South Wales.[20]

The (lapsed) Privacy and Data Protection Bill 1994 (NSW)

For specific background information and for a summary of the Bill, please see the Parliamentary Library's *Bills Digest* on the Privacy and Data Protection Bill 1994 (No 13/94) by Gareth Griffith.

Even though this particular Bill has lapsed with the dissolution of the 50th Parliament, it is interesting to consider what the effect of the Bill would have been as an effective legislative response to the needs of information privacy protection in NSW.

This Bill had been criticised as not going far enough in the development of enforceable privacy rights. Clause 7 of the Bill would have established the misuse or disclosure of personal information by a public (or former) public official as a general offence for which the penalty would have been $10 000 or imprisonment for 2 years or both. Such a person would not have been guilty of an offence if the personal information was disclosed (i) in accordance with an applicable data protection code or (ii) with the informed consent of the person the subject of the information or if (iii) the personal information was contained in a public register. It is not exactly clear from the provisions of the Bill as to how an

---

[20] Independent Commission Against Corruption, op cit note 17, Volume 1, p 166.

individual and/or the Privacy Commissioner should have responded under the legislation if there was reason to suspect that an offence had been committed under clause 7, except that, according to clause 36, the Privacy Commissioner could refer a complaint for investigation or other action to any person or body considered to be appropriate in the circumstances. It is assumed that this clause would have enabled the Privacy Commissioner to notify the Police, if a complaint raised the issue of an offence under the legislation.

Under Division 2 of Part 1 of the Bill, data protection codes were to be prepared by public authorities. These codes were to conform, so far as was reasonably practicable, with the data protection principles set out in Division 4. The criticism has been made that

> The single crippling deficiency of the Bill is that the [Data Protection Principles] cannot be enforced, either by the Privacy Commissioner or (more importantly) by individuals who have suffered because of breaches of the DPPs, or by members of the public generally. The same is true of any codes of conduct based on the DPPs...
>
> The only enforcement mechanism provided in the Bill is that an 'individual who has been detrimentally affected by an alleged breach of a data protection principle...may complain to the Privacy Commissioner' (cl 23(1)). However, the Commissioner is merely empowered to report his conclusions (cl 37), but has no power to order compliance with an infringed DPP, nor award damages or any other form of compensation to the complainant. In other words, the Privacy Commissioner is a 'privacy ombudsman' with no more enforcement powers than the existing Privacy Committee.[21]

By way of contrast, the federal Privacy Commissioner under the *Privacy Act 1988* (Cth), has the power (section 52) after investigating a complaint, inter alia, to (if the complaint is substantiated) make a determination including declarations that the respondent should redress any loss or damage suffered by the complainant or, in certain circumstances, 'that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint.' Sections 54-59 of the federal Act provide for the review and enforcement of determinations made by the Commissioner under section 52.

Further criticisms that have been made of the lapsed Privacy and Data Protection Bill 1994 include:

---

[21] Greenleaf, G, 'NSW "claytons" privacy Bill legitimises data surveillance', (1994) 1(3) *Privacy Law and Policy Reporter*, 41 at 43.

- 'agencies have in effect been given a licence to write their own exemptions from the [Data Protection Principles]'[22] to the extent that data protection codes only need to conform with the data protection principles 'so far as is reasonably practicable' (see clause 11(2)); and

- clause 11(4) of the Bill would have enabled (despite the requirement under clause 11(2) for codes to conform so far as is reasonably practicable with the data protection principles) public authorities to permit under their code the disclosure of personal information to other public authorities.[23] This possibility would have had quite serious implications for data matching between government agencies.

Further, the Privacy Commissioner would have had the role of reviewing a data protection code according to clause 11. However, it is unclear whether the Commission's recommendations for amendment of a Code would be complied with by a particular public authority as, according to clause 11(5), the public authority would only be required to *consider* the findings of the review of the Code by the Privacy Commissioner. The Commissioner would have had an extremely weak role in the process of the drafting of data protection codes for public authorities, even though the functions of the Commissioner included a clear mandate under clause 22 to 'promote the adoption of, and compliance with, data protection principles and guidelines...'.

3. THE GROWING DEMAND FOR THE PROTECTION OF PRIVACY

The point has been made that a 'number of features of contemporary society presently threaten personal privacy' including the growth of the range and scope of official powers to 'intrude into the private domain', increasingly intrusive commercial practices, the increasing sophistication of surveillance and communications interception equipment and the improvements in computer and communications technology.[24] In relation to the use of personal information by government agencies, technological advances in information systems have had an enormous impact.

Technology and personal information

It has been observed that:

> The widespread use of computers facilitates, of course, incomparably speedier and more efficient methods of storing, retrieving, and transferring information than is possible with conventional manual filing systems. To

---

[22] Ibid, p 43.

[23] Ibid.

[24] ALRC, op cit note 14, Vol 2, p 4.

> what extent...will the dictator or even the bureaucrat prove capable of resisting the temptation to abuse this power? Already there are alarming signs that the drift toward centralized data banks is inexorably posing disturbing threats to individual freedom.[25]

This warning has certainly been borne out in NSW with the exposure by ICAC of the widespread misuse of and trade in personal information by public officials of certain government agencies.[26]

> The type of information traded included addresses, silent telephone numbers, bank account and pension details, social security information, Medicare records, criminal history information and the details of people's movements in and out of the country.[27]

Wacks[28] gives a detailed analysis of specific problems that may arise in relation to personal information and information data banks generally. The following is a summary of issues identified by Wacks that should be considered in light of the information opportunities presented by the use of computerised data banks. The identification of these numerous issues and aspects of dealings in information are essential with respect to the drafting of practically effective legislation to protect and promote personal information privacy.

1. Data-collection problems

(i) Confidentiality of data - it is essential that individuals can trust the protection of highly sensitive personal information such as medical or financial records.

(ii) Consent by the data subject to the use of the data

(iii) Knowledge by the data subject of the existence of the data bank

(iv) Knowledge by the data subject of the use to which the data is being put

---

[25] Wacks, R, op cit note 5, p 178.

[26] For more detail, see Independent Commission Against Corruption, op cit note 17.

[27] *NSWPD*, 14/4/94, p 1156.

[28] Wacks, R, op cit note 5, pp 183-205.

2. Data bank system problems

(i) Security of the system

(ii) Unauthorized access to the data bank

3. Data-usage problems

(i) Incorrect or erroneous data

(ii) Relevance of data - 'A particularly insidious difficulty arises where data collected for one purpose are used for another.'[29]

(iii) Subjective data - 'The almost inevitable subjectivity that attends assessments of individual ability renders much information relating, in particular, to employees, peculiarly vulnerable to abuse.'[30]

(iv) Retention of old data

(v) Consent of the data subject to use of data - 'The individual...may at the collection stage readily consent to the giving of information of the most sensitive kind, [however] may be less willing to impart such data if he is aware that there exists some other purpose to which they could be put.'[31]

(vi) Knowledge of the data subject of the use to which the data are being put

4. Problems relating to the movement of data

(i) Linkage of data from different data bases (or what is commonly referred to as data matching which was the primary concern in the mid 1980's with the threatened introduction at a federal level of the Australia Card.)

(ii) Centralization or synthesis of data banks

(iii) Transborder data flow - 'A growing international trade in information and data-processing services ensures that data are no longer confined within national borders.'[32]

---

[29] Ibid, p 199.

[30] Ibid, p 200.

[31] Ibid, p 202.

[32] Ibid, p 204.

A Privacy Charter?

The growing demand for privacy protection in Australia has been reflected in the release of the Australian Privacy Charter (Public Release Draft) of October 1994 (attached as Appendix A), the purpose of which is to 'change the practices and processes that provide privacy protection to individuals.'[33] The Australian Privacy Charter Council, which was formed in 1992, includes 'representatives of a range of business and governmental interests, consumer groups, professional societies, civil liberties organisations and academia.'[34]

> The Charter Council's function is to develop the Australian Privacy Charter, and (in due course) associated Codes for use by industry, government and community groups. The Charter's intended audience is these groups, legislators and the Australian public.[35]

The Charter is not restricted to information privacy. It recognises individual privacy as a basic human right. This independent development no doubt intends to raise awareness in Australia of the fundamental importance of privacy which is being threatened in an increasingly technocratic society.

4. COMPETING RIGHTS

It has been stated that:

> Any claim by an individual to preserve his own integrity by ensuring respect for his privacy must be considered against similar, equally justified claims by other individuals. It must also be considered against the need to help society at large in its efforts to improve the lot of individuals within it by ensuring the efficient running of government, industry, commerce, professional activity and research. None of these can be completely ignored. Privacy is but one of a number of human rights. Privacy protection should not ignore other legitimate interests.[36]

Examples of the public interest impinging on a strict right of privacy in relation to personal information would be the compellability of a witness to give evidence in a trial, the collection of census information and the many duties of disclosure of personal

---

[33] Cameron, J, 'Draft Australian Privacy Charter released', (1994) 1(7) *Privacy Law and Policy Reporter, 136.*

[34] Ibid.

[35] Ibid.

[36] ALRC, op cit note 14, Vol 2, p 4.

information under the various tax legislation of Australia. The balance between the demands of the public interest and private interests is constantly shifting depending on the government of the day. An important shift occurred in NSW in 1989 with the enactment of the *Freedom of Information Act 1989*. At a federal level, there have been interesting constitutional developments with the recognition by the High Court of an implied constitutional right of freedom of communication in certain circumstances.

The public's right to know and freedom of information in NSW

Government data will cover a vast array of information concerning government activities and decisions, expenditures, reasons for decisions, decision-making processes, recommendations and all other information concerning the process of government. This information will frequently be directly relevant to and impact upon the conduct of an individual's or a group's daily activities both at home and at work (for example reasons for a decision to issue or refuse a licence to carry out a certain activity). Further, such information will also be directly relevant to the collective public interest and is necessary for a fully informed critique and assessment of the effectiveness of the government of the day. As a result, there has been a growing movement in the Western world in the last thirty years in favour of a legally supported public right of access to such information.[37]

Principles of personal privacy and freedom of information may conflict. However, as described above, the *Freedom of Information Act 1989* (NSW) plays a limited role in the protection of personal information, while at the same time being founded on the general philosophy of making various government information more available to the public.

> It is sometimes suggested that there is a conflict between the aims of privacy protection and those of freedom of information. It is more accurate to speak of occasional tensions between them as the balance between the principle of the widest possible access to government-held information and the principle of limiting the use and disclosure of information about individuals is worked out in particular cases. ... Both in the United States and in Australia FoI developed wider objectives concerned with government accountability and participation in decision making, but FoI continues to have an important role to play in achieving privacy objectives.[38]

It is therefore interesting to note that clause 51 of the (lapsed) Privacy and Data Protection Bill 1994 (NSW) specifically stated that nothing in the Bill would require or

---

[37] In the context of the *Freedom of Information Act 1982* (Cth), for a brief history of the freedom of information movement in Australia, see Bayne, P, *Freedom of Information*, The Law Book Company Limited, 1984, p 4.

[38] Fraser, R, 'Freedom of Information and Privacy: Some Recent Developments and Issues', (1994) 54 *Freedom of Information Review*, 74.

permit information to be disclosed in contravention of the *Freedom of Information Act 1989*. This would suggest that it was contemplated that the *Freedom of Information Act 1989* would have provided the individual with a higher level of protection of personal information privacy in certain circumstances than the proposed Privacy and Data Protection Bill 1994 (for example, compare the operation of clause 7 of the Bill and its exemptions and section 31 of the *FoI Act*). This would have been a curious feature of legislation of which the primary focus was the protection of information privacy.

In NSW:

> Access to personal records, privacy and its connection to FoI is an issue to be addressed arising out of the proposed NSW Privacy and Data Protection Bill currently being examined by a Parliamentary Select Committee, due to report in 1995.[39]

Unfortunately, the Committee was dissolved before it could report.[40]

The constitutional implied right of freedom of communication

Two cases of the High Court in 1992[41] established that 'there is to be drawn from the doctrine of representative government which forms part of the fabric of the Constitution a fundamental implication of freedom of political communication and discussion.'[42] Both of these cases were concerned with the validity of federal legislation. In 1994, the constitutional implication of freedom of political communication and discussion was further developed with respect to its relationship with the law of defamation in the cases of *Theophanous v Herald & Weekly Times*[43] and *Stephens v West Australian Newspapers Ltd*[44]. These cases have been described as 'constitutionalising' Australia's defamation laws 'by establishing a defence, derived from the Constitution, which applies where the defamatory publication is a matter of political discussion.'[45] It is not proposed to go

---

39 Smith, B, 'Parliament and FoI in NSW', (1994) 54 *Freedom of Information Review*, 79 at 83.

40 For a discussion of the relationship between the federal *Privacy Act 1988* and the *Freedom of Information Act 1982*, see Bayne, P, 'Privacy dimensions of administrative law', (1995) 69 *The Australian Law Journal*, 13 at 17. See also Fraser, R, op cit note 38.

41 *Nationwide News Pty Limited v Wills* (1992) 177 CLR 1 and *Australian Capital Television Pty Limited v The Commonwealth* (1992) 177 CLR 106.

42 *Theophanous V Herald & Weekly Times Ltd and Another* (1994) 124 ALR 1, per Deane J at 44.

43 (1994) 124 ALR 1.

44 (1994) 124 ALR 80.

45 Walker, S, 'The Impact of the High Court's Free Speech Cases on Defamation Law', (1995) 17(1) *The Sydney Law Review* 43.

into the details of these key constitutional decisions. However, it is interesting to note that an implied freedom of communication with respect to political discourse, may act as a competing right to a right of privacy with respect to personal information. This is particularly relevant to a politician's right of privacy. For example, it is arguable that the validity of provisions of freedom of information or privacy laws in Australia preventing (in certain circumstances) the disclosure of personal information concerning a politician could possibly be challenged as breaching the implied constitutional right, if such information had political importance or implications. With respect to the 1992 cases, it has been commented that:

> A deleterious impact on the development of a right to privacy would occur if a general constitutional right to freedom of expression and communication developed without the counter-balancing right to privacy.
>
> At another level, the decisions raise the general issue of whether there is a need for more certainty in the protection of fundamental human rights in our law. At this level the decisions are helpful in generating debate about whether there is the need for a Bill of Rights or whether it is appropriate that the judiciary, on a case-by-case basis, imply these in the Federal Constitution.[46]

5. CONCLUSION

There is no doubt that the privacy of individuals is under increasing threat in a technology-driven and commercially aggressive society. A solution to the misuse of personal information by government agencies should involve clear and effective legislative safeguards. A change in the culture of those who have access to and use such information is also imperative, so that personal information privacy is a standard high priority. In addition, public awareness of privacy issues needs to be raised so that the 'guardians' of personal information are more aware of their duties and individuals are more aware of the extent of their privacy rights under existing privacy and freedom of information laws.

It would be a rare individual who would be aware of the full extent of personal information held by public (or private) agencies or bodies and the exact use of such information. It could be said that most individuals would assume that personal information is always dealt with in a confidential and legal manner. Such trust in various agencies should be supported by clear legislation and standard codes of practice and not simply left to the particular practices of a particular agency.

The federal Privacy Commissioner, Mr Kevin O'Connor captured the essence of the modern challenge of protection of privacy and personal information when he stated:

---

[46] Tucker, G, 'Privacy Protection and the High Court', (1993) 67 (1 & 2) *The Law Institute Journal*, 69.

Privacy supports people in relation to their personal development and the way they deal with others. It's crucial in relationships of candour such as with doctors, banks and solicitors and it's very important in promoting respect between individuals for each other. Those values are broadly recognised in the society and the challenge is to give expression to them in these new environments.[47]

[47] 'BSEG's' Mysterious Proposal for Info Privacy', (1995) 108 *Communications Update*, 4.

APPENDIX A

The Australian Privacy Charter (Public Release Draft) October 1994

(Page 18)

THE AUSTRALIAN PRIVACY CHARTER (PUBLIC RELEASE DRAFT) OCTOBER 1994

PREAMBLE

The meaning of 'privacy'

Australians value privacy, and recognise that it is under ever-increasing threat. They expect that their rights to privacy be recognised and protected.

Privacy encompasses bodily (physical) privacy, territorial privacy (privacy space), privacy of communications, information privacy (rights concerning information about a person), and freedom from unwanted surveillance. These categories sometimes overlap.

'Privacy' is a term widely used to refer to an accepted group of related rights. These rights are accepted nationally and internationally. This Charter enumerates those rights as 'privacy principles'.

Privacy Principles comprise both the rights that each person is entitled to protect, and the obligations of organisations and others to respect those rights.

Personal information is information about an identified person, no matter how it is stored (eg: sound, image, data, fingerprints).

Privacy is important

A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both State and private organisations to intrude on that autonomy.

Privacy is a value which underpins human dignity and other key values such as freedom of association and freedom of speech.

Even those privacy protections and limitations on surveillance that do exist are being progressively undermined by technological and administrative changes. New forms of protection are therefore required.

Interferences with privacy must be justified

Privacy is a basic human right and the reasonable expectation of every person. A desire for privacy does not mean a person has 'something to hide'. People who wish to protect their privacy should not be required to justify their desire to do so.

The maintenance of other social interests (public and private) justifies some interferences with privacy and exceptions to these Principles. The onus is on those who wish to interfere with privacy to justify doing so. The Charter does not attempt to specify where this may occur.

Aim of the Principles

The following Privacy Principles are a general statement of the privacy protection that Australians should expect to see observed by both the public and private sectors. They are intended to act as a benchmark against which the practices of business and government, and the adequacy of legislation and codes, may be measured. They inform Australians of the privacy rights that they are entitled to expect, and should observe.

The Privacy Charter does not attempt to specify the appropriate means of ensuring implementation and observance of the Privacy Principles. It does require that their observance be supported by appropriate means, and that appropriate redress be provided for breaches.

PRIVACY PRINCIPLES

1. Justification and exceptions

Technologies, administrative systems, commercial services or individual activities with potential to interfere with privacy should not be used or introduced unless the public interest in so doing outweighs any consequent dangers to privacy.

Exceptions to the Principles should be clearly stated, made in accordance with law, proportional to the necessities giving rise to the exception, and compatible with the requirements of a democratic society.

2. Consent

Individual consent justifies exceptions to some Privacy Principles. However, 'consent' is meaningless if people are not given full information or have no option but to consent in order to obtain a benefit or service. People may revoke their consent.

In exceptional situations the use or establishment of a technology or personal data system may be against the public interest even if it is with the consent of the individuals concerned.

3. Accountability

An organisation is accountable for its compliance with these Principles. An identifiable person should be responsible for ensuring that the organisation complies with each Principle.

4. Observance

Each Principle should be supported by necessary and sufficient measures (legal, administrative or commercial) to ensure its full observance, and to provide adequate redress for any interferences with privacy resulting from its breach.

5. Openness

There should be a policy of openness about the existence and operation of technologies, administrative systems, services or activities with potential to interfere with privacy.

Openness is needed to facilitate public participation in assessing justifications for technologies, systems or services; to identify purposes of collection; to facilitate access and correction by the individual concerned; and to assist in ensuring the Principles are observed.

6. Freedom from surveillance

People have a right to conduct their affairs free from surveillance or fear of surveillance. 'Surveillance' means the systematic observation or recording of one or more people's behaviour, communications, or personal information.

7. Privacy of communications

People who wish to communicate privately, by whatever means, are entitled to respect for privacy, even when communicating in otherwise public places.

8. Private space

People have a right to private space in which to conduct their personal affairs. This right applies not only in a person's home, but also in the workplace, the use of recreational facilities and public places.

9. Physical privacy

Interferences with a person's privacy such as searches of a person, monitoring of a person's characteristics or behaviour through bodily samples, physical or psychological measurement, are repugnant and require a very high degree of justification.

10. Anonymous transactions

People should have the option of entering transactions which do not require them to identify themselves.

11. Collection limitation

The minimum amount of personal information should be collected, by lawful and fair means, and for a lawful and precise purpose specified at the time of collection. Collection should not be surreptitious. Collection should be from the person concerned, if practicable.

At the time of collection, personal information should be relevant to the purpose of collection, accurate, complete and up-to-date.

12. Information quality

Personal information should be relevant to each purpose for which it is used or disclosed, and should be accurate, complete and up-to-date at that time.

13. Access and correction

People should have a right to access personal information about themselves, and to obtain corrections to ensure its information quality.

Organisations should take reasonable measures to make people aware of the existence of personal information held about them, the purposes for which it is held, any legal authority under which it is held, and how it can be accessed and corrected.

14. Security

Personal information should be protected by security safeguards commensurate with its sensitivity, and adequate to ensure compliance with these Principles.

15. Use and disclosure limitations

Personal information should only be used, or disclosed, for the purposes specified at the time of collection, except if used or disclosed for other purposes authorised by law or with the meaningful consent of the person it is about (if in the public interest).

16. Retention limitation

Personal information should be kept no longer than is necessary for its lawful uses, and should then be destroyed or have identifiers permanently removed.

17. Public registers

Where personal information is collected under legislation and public access is allowed, these Principles still apply except to the extent required for the purpose for which public access is allowed.

18. No disadvantage

People should not have to pay in order to exercise their rights of privacy described in this Charter, nor be denied goods or services or offered them on a less preferential basis for wishing to do so. The provision of reasonable facilities for the exercise of privacy rights is part of the normal operating costs of organisations.