FRONTIERS OF INFORMATION PRIVACY IN AUSTRALIA

by

Greg Tucker*

Abstract

This article reviews the very sensitive and topical area of privacy known as personal information privacy or data protection, which covers one's personal details on subjects ranging from medical and police records to religious beliefs. The various models of regulation in operation throughout the world, and the principles governing these, are reviewed and the situation in Australia examined in greater depth. The author concludes that despite some considerable efforts, there is still some way to go before Australia can boast success in developing and unifying its data protection laws.

Introduction

The Morison Report in 1973 stated:

> "Privacy may be regarded as the condition of an individual when he is free from interference with his intimate personal interests by others. It is not implied that complete freedom in this respect is anyone's moral right or that he has a legitimate claim that such complete freedom should be his legal right"[1]

Privacy is inherently difficult to define. This problem arises from its sociological and cultural underpinnings. Whilst it is clear that the concept embraces generally freedom from physical or electronic intrusions and publication of intimate details of one's private life, there are many fringe areas which may be regarded as being on the periphery of privacy.[2] The Australian Law Reform Commission in its major report took the term in its use as an "ordinary language concept"[3]

---

* BA LLM, Senior Lecturer, David Syme Faculty of Business, Monash University.

1 Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys - General No. 170/1973, p.3.

2 Prosser, in reviewing the US case law, saw privacy as falling under four torts: intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; public disclosure of embarrassing private facts about the plaintiff; publicity which places the plaintiff in a false light in the public eye; and appropriation, for the defendant's advantage, of the plaintiff's name or likeness. See Prosser, W. "Privacy" (1960) 48 *Calf. Law Rev.* 383, 389.

3 ALRC, Report on Privacy No. 22/1983, para.20.

This paper will review the area of privacy known as personal information privacy or data protection. Accordingly, there is no need to define the broader concept of privacy. No comprehensive definition of this term has emerged to date in Australia.[4]

Personal information includes: purchasing patterns; data relating to sexual preferences, religious and political beliefs; medical records; police records; and financial information; which relate to an identifiable individual or individuals.[5] Some categories of data may be regarded as more sensitive than others and merit different protection.[6]

Throughout this paper I shall refer to the person to whom the data relates as the *data subject* and the person that collects and/or uses the data as the *data controller*.

The rather cumbersome term *transborder data flow* refers to the transfer of personal information across sovereign boundaries. This is an issue of mounting importance which will be discussed later on in the paper.

Types of Regulation

There are a number of different models used to regulate the collection and use of personal data throughout the world. Each country or state may have its own version of the model. Each of these categories shall be discussed in turn. They are not necessarily mutually exclusive.

(a) Licensing

This model provides that each data controller must apply to a central authority for a licence to collect and/or use data. A licence may be granted in respect of certain categories of personal data and not others. A fee is paid for the licence on a periodic basis and the licensing authority may revoke the licence in certain circumstances which, typically, include breach of the data protection principles set down in the legislation. Of course, the impact of the withdrawal of a licence would have a devastating effect on any business. This must be regarded as the ultimate remedy rather than one which is used routinely.

One of the pioneers in personal data protection, Sweden, adopted a licensing model which to outsiders would appear to be an expensive and, at

---

4 See generally: Storey, H. "Infringement of Privacy and its Remedies" (1973) 47 *ALJ* 498; Burns, P. "Privacy and the Law: 1984 is Now" [1974] *NZLJ* 1; Swanton, J "Right of Privacy" (1974) 51 *Current Affairs Bulletin* 24; and Benn, S. "The Protection and Limitation of Privacy" (1978) 52 *ALJ* 601.

5 See OECD *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, 1980, para 1, and the *Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 108/1981, article 2.

6 This is recognised in the OECD Guidelines, OECD, Paris, 1980, para. 3(a) and the Council of Europe Convention 108/1981, Strasbourg, article 6.

times, unwieldy system. However, one must have regard to the cultural and sociological context within which these laws are put in place. In Sweden, the use of the personal identification number is widespread and the ability of government to link personal data from different files is apparent. Accordingly, the licensing of users and collectors of personal data was seen as an appropriate counter balance to the potential intrusions into the private lives of its citizens.

There are strong indications that Sweden is moving away from it and towards a notification/registration system. The Swedish Commission reviewing the *Data Act* 1973 has recommended sweeping changes.[7]

Today this model has little support in those countries which are developing or have just developed data protection laws. Ireland, the Netherlands, Portugal and Spain have favoured registration systems.

(b) Notification and Registration

A notification or registration scheme requires the data collector to advise the central authority of the personal files it has collected or is using. However, unlike a licensing scheme, no positive assessment of the application need be made. The data controller may proceed with its activities until otherwise advised by the authority. This model places less burden on the central authority than the licensing scheme and generally requires less administration.

This model has been adopted in the United Kingdom in the *Data Protection Act* 1984. This provides for a mass registration scheme and gives the Registrar the power to deregister delinquent data controllers.[8] By contrast, the *Data Protection Act* 1988 (Ireland) provides a restricted registration scheme which is confined to specific areas of data which are generally considered to be sensitive and to warrant this protection.[9]

(c) Passive Schemes

This model requires far less formality than a licensing or registration scheme. Data controllers are not required to record formally details of their personal data files with a data protection authority. The data protection authority promotes adherence to the data protection principles amongst data controllers. Accordingly, the data protection authority, if any, must rely upon its powers of persuasion, its own investigations or public complaints for its effectiveness. The cost of this model to data controllers is substantially less than the schemes above.

Passive schemes do not always provide sanctions for non-compliance with the appropriate data protection principles. In Australia, the New South

---

7 See summaries of reports, in English, of the Swedish Commission, 1990: 61 and 1991: 21, Stockholm.

8 S.11.

9 The Act applies to all personal data kept by data controllers, but only some of this data is required to be registered. See s.16.

Wales *Privacy Committee Act,* 1975 is a passive scheme which bestows on the relevant committee an investigatory and reporting role but no enforcement capacity. A similar framework exists in South Australia.[10] The *Privacy Act* 1988 (C'lth), which operates chiefly in the federal public sector, is a passive scheme which provides for the Privacy Commissioner to institute enforcement procedures where necessary. However, annual disclosure of records of personal information held by government agencies is required under the Act.[11] The power of the Privacy Commissioner to conduct audits is an integral part of this scheme.[12]

(d) Self-regulation

Many countries have yet to enact legislation protecting personal data. Some countries have made a start, like Australia, Canada, Japan and the United States, whilst others like Malaysia, Singapore and South Korea, have yet to begin.

Self-regulation may take place concurrently with other models, working towards the same end. The Netherlands, Ireland and the United Kingdom each have a hybrid system made up of registration of personal data files and encouragement of self-regulation. The usual form of self-regulation is encouragement of data controllers by government to adopt good data protection practices. The good faith of particular industries may be evinced by the production of internal guidelines or a code of practice which provides industry-specific data protection standards.

In Australia, the federal government has urged industry to adopt the principles laid down in the Guidelines ("OECD Guidelines") published by the Organisation for Economic Co-operation and Development.[13] The *Data Protection Bill* 1991, (New South Wales) relies on this form of regulation. There is some evidence of self-regulation in Australia, for example, the standards of practice of the Australian Direct Marketing Association. However, there has been little, if any, independent assessment of such codes.

In reality, self-regulation may equal no regulation and just provide a convenient facade to hold out and proclaim that something is being done about data protection. It may be quite difficult to determine in each case whether the self-regulation is effective or nothing more than paying lip service to data protection. A recent OECD report "Privacy and Data Protection - Issues and Challenges"[14] has provided a suggested yardstick or checklist for the assessment of effective or "value added" codes. It recommends that codes include the following elements:

---

10 See Government Gazette (SA) 6 July 1989, p.6.

11 See s.14 [Information Privacy Principle 5(3)] and s.27(g).

12 Ss.27(1)(h), 28(1)(e) and 28A(g).

13 See Federal Attorney General's press release: 10 December 1984, No 180/84.

14 Tucker, G. OECD, Paris, 1992.

(i)	Form	the code should include positive statements providing a commitment to the adoption of proper data protection principles. Mere descriptive language is not sufficient;
(ii)	Substance	the code should be tailored to the particular industry or company and not merely reflect general principles of data protection. There must be some concerted attempt to apply the principles so that they become workable and applicable to the industry or company;
(iii)	Level of Detail	the code should deal with the data protection issues confronting the relevant industry or company and other interested parties;
(iv)	Transparency	the code should be written in simple language readily comprehensible to participants in the relevant industry or company;
(v)	Implementation	the code should provide for an implementation procedure within the industry or company so that there is no doubt as to the style and manner of protection offered. This may include the nomination or declaration of officers to take responsibility for this area who would have the duty to report regularly to the appropriate management body;
(vi)	Review	the code should provide for a means of review of its terms from time to time in order to make an assessment of their relevance and, where necessary, to make appropriate changes. This is a recognition that market conditions, like technological change, may alter and require a reconsideration of the terms of the code. It may include soliciting public comment which are then taken into account in the review process;
(vii)	Control	the code should be underpinned with some means of control or enforcement of its terms. This may be legislative, contractual or administrative. It should provide data subjects or other interested parties with some means of redress for a breach of the terms of the code.[15]

Data Protection Principles

Since 1980 two international instruments have dominated discussions in this area: the OECD Guidelines; and the Convention for the Protection

---

15 *Ibid.* p.53.

of Individuals with regard to Automatic Processing of Personal Data produced by the Council of Europe in 1980.[16] Although these instruments have different coverage and legal effect, the principles which they espouse are very similar. As Australia adopted the OECD Guidelines in December 1984, it is appropriate to briefly summarise the principles of personal data protection which are contained in them.

The first principle, the collection limitation principle, requires that data must only be obtained by lawful means and with the knowledge or consent of the data subject. Secondly, the data quality principle provides that only data relevant for the purpose of the collection be required by the collector of the data, and such data must be up to date, accurate and complete. Following on from this the purpose specification principle states that the purposes for which the data is gathered must be disclosed to the data subject at the time it is collected, and that such data shall only be used for that purpose or those purposes.

The fourth principle is the use limitation principle which requires that the data not be disclosed by the person who collects it to a third party without the consent of the data subject unless it is demanded by law. The security safeguards principle follows on and this sets out that the data must be protected by the collector of it, by taking reasonable security precautions against loss, destruction and unauthorised use, access, modification or disclosure of it. The openness principle, is the sixth principle and it advocates that the data subject ought to be able to readily determine the whereabouts, use and purpose of personal data relating to him or her.

The penultimate principle is the individual participation principle, which envisages that the data subjects can:

(i) obtain confirmation from the data collector that the data is held relating to them;

(ii) obtain details of such data within a reasonable time, for a reasonable charge, if any, in a reasonable manner and in an intelligible form;

(iii) be given reasons where access to such data is denied them and to be given the right to challenge such decisions, and;

(iv) challenge data relating to them and be able to have it rectified, or erased by the collector.

Finally, the accountability principle sets out that the data collector ought to be accountable for complying with the above principles.

All twenty-four of the OECD member countries have adopted the OECD Guidelines. However, the implementation by these countries of the Guidelines has not been uniform. Currently, thirteen countries have comprehensive data protection legislation covering public and private

---

16 Note that the United Nations General Assembly has adopted a resolution on data protection - see Resolution No. 45/95 of 68th plenary meeting of the General Assembly of the United Nations.

sectors.[17] Other member countries, like Australia, Canada, Japan and the United States, have laws in some sectors, but not in others. Finally, some countries, including Belgium, Greece, Italy, Switzerland and Turkey, have yet to enact any specific laws in this area.

These basic data protection principles have been used as the basis for much of the legislation enacted since 1981. For example, the United Kingdom[18], the Republic of Ireland [19], Japan,[20] and Australia,[21] have all taken account of these principles in the legislation which they have produced. Legislative proposals have also used the OECD Guidelines as a starting point.[22]

However, these are only broad, non-industry specific principles, so that much work needs to be done on the appropriate implementation of the principles.[23] Each industry will have different demands and requirements which must be taken into account in the interpretation of these general principles. Proper industry codes of practice become useful in this situation as they can provide a linkage between the general principles of data protection and their implementation at the grass roots level. Recent European initiatives may turn attention away from the OECD Guidelines.[24]

Transborder Data Flows

The proposed directive of the European Commission concerning the protection of individuals in relation to the processing of personal data ("the draft directive") sets out a detailed general data protection model intended to be followed by its twelve member countries[25]. The draft directive, in its present form, seeks to ensure that the EC member states involved converge their laws to the high level of protection it prescribed. For example, it

---

17 Austria, Denmark, Finland, France, Germany, Iceland, Ireland, Luxembourg, the Netherlands, Norway, Portugal, Sweden and the United Kingdom.

18 *Data Protection Act* 1984.

19 *Data Protection Act* 1988.

20 *Act for the Protection of Computer Processed Personal Data Held by Administrative Organs.* 1988.

21 *Privacy Act* 1988.

22 For example, Law Reform Commission of Hong Kong. "Protection of Personal Information: The Law in Hong Kong and Options for Reform", February 1990 and the Sub-committee on Technology and Law of the Law Reform Committee of the Singapore Academy of Law "Data Protection in Singapore - A Case for Legislation" Working Paper No.1, 1990.

23 The eleven IPPs in the *Privacy Act* 1988 attempt to translate the Guidelines into functional form.

24 See Transborder Data Flows below.

25 Com (90) 314 - SYN 287, Brussels, 1990. Note that the European Parliament has proposed amendments to the draft directive resulting from the report of the Committee on Legal Affairs and Citizens Rights, European Parliament, January 1992 (the Hoon Report).

would require that the United Kingdom extend its *Data Protection Act* to encompass manual as well as automated personal data files. Current paper-based personal data files are not covered by the legislation. More particularly, countries like Belgium, Greece and Italy which lack generic data protection laws would be required to enact them in order to comply with the directive, in its final form.[26]

The potential impact of this on Australia is hard to assess. Article 24 of the draft directive sets out that European states may wish not to transfer personal data to non-European countries where protection of the data is inadequate. Adequacy is not defined. It is possible that this could lead to restrictions or prohibitions on transborder data flows from Europe. Indeed, there is substantial evidence of the use of TBDF provisions by European countries to restrict or prohibit the transfer of personal data. The extraterritorial effect of a common European standard may be to raise the level of data protection outside Europe so that trade and other matters, involving the transfer of personal data, is maintained.[27] Thus the use of TBDF provisions may no longer be dismissed as academic, the problem is no longer perceived, but real.

It is possible under the draft directive to permit the transfer where the transferee company has appropriate internal rules which are assessed to be adequate[28] This may encourage companies outside Europe to draft internal data protection guidelines or codes for their business. In this way the flow of personal information may remain unimpeded

Australia should keep developments relating to the draft directive under close scrutiny to ensure it is not caught by surprise as a new European regime evolves.

The Australian Setting

There have been a plethora of reports concerning privacy protection in Australia. In 1973 the Morison Report recommended sweeping changes in our laws to protect privacy. The Statute Law Revision Committee, Victoria, reported, in 1975, on a private member's bill called the *Information Storages Bill* 1971. In 1976, the Mann Report in Western Australia reviewed privacy laws in that state and the Australian Law Reform Commission, from 1976 to 1983, provided a wide ranging and comprehensive review of privacy laws in Australia. A sector by sector assessment of the protections and dangers relevant to data protection in Australia was provided. A draft bill accompanied the final report and some of the *Privacy Act* 1988 (C'lth) is based upon this work. More recently, in Victoria, the Legal and Constitutional Committee in its report concerning breach of confidence,[29]

---

26 See generally: Tucker, G. "International Legal Note" (1991) 65 *ALJ* 354 and 560.

27 For a summary of recent examples of TBDF see Tucker, G. OECD report "Privacy and Data Protection - Issues and Challenges" 1992, Ch VII.

28 See article 25 of the draft directive.

29 "Privacy and Breach of Confidence" Report no. 40/1990.

recommended substantial revision of privacy laws and, in South Australia, the Report of the Select Committee of the House of Assembly on Privacy was produced in 1991. Finally, the Privacy Committee of New South Wales has just provided a report to the Independent Commission Against Corruption.[30]

There exists a curious lack of debate concerning the constitutional position in Australia in relation to the protection of personal information. The scope of the ALRC's reference on privacy was limited to the federal public sector rather than Australia as a whole however, reference was made to the possibility of extending the proposals to the States.[31] Although it is beyond the scope of this article, there would seem to be a good argument that the federal parliament has jurisdiction to enact privacy legislation to cover the whole field of privacy.[32] For example, the external affairs power seems to provide such a nexus. The decisions in *Koowarta* v *Bjelke-Peterson & Ors*[33] and *Commonwealth v Tasmania*[34] may support this proposition.

The Australian government could rely upon a number of international instruments to this end. Australia is a party to the International Covenant on Civil and Political Rights and, pursuant to this, Australia has undertaken to take appropriate legislative measures to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.[35] The adoption in 1984 of the OECD Guidelines provides a further international link. Finally, the General Assembly of the United Nations, in December 1990, passed a resolution on data protection.[36] This resolution is expressed to apply to member countries as well as the organisation itself. At present, federal parliament has left privacy matters to be dealt with jointly between the governments around Australia. The recent amendment to the *Privacy Amendment Act* 1990 regulating consumer credit reporting throughout Australia, sought to rely on the corporations power and the telecommunications power under the federal constitution. Accordingly, no evidence exists that the federal government wishes to cover the field in this area by attempting to invoke the external affairs power. Uniformity throughout Australia will be difficult to achieve under these conditions.

---

30 "Privacy and Data Protection in New South Wales: A Proposal for Legislation." Report no. 63/1991.

31 ALRC, *Privacy* No 22, AGPS, 1983 vol 2, para 1396.

32 See generally: Hughes, G. *Data Protection in Australia,* The Law Book Co, 1991 Ch.3; Tucker, G. *Information Privacy Law in Australia,* Longman Cheshire, 1992 pp. 61 - 68.

33 (1981-2) 153 CLR 168.

34 (1984-5) 158 CLR 1.

35 See article 17.

36 No. 45/95 of the 68th plenary meeting of the General Assembly.

(a) State and Territory Legislation

(i) The Australian Capital Territory

A Privacy Unit has been in existence for several years in the ACT. It performs an educational role for the Territory government as well as acting as a watchdog in the area and forwards matters within the jurisdiction of the *Privacy Act* 1988 (C'lth) to the federal Privacy Commissioner.

(ii) New South Wales

The Privacy Committee of New South Wales was established by legislation in 1975 following the report of the Morison Committee. This Committee emerged during a strong surge of privacy reform in Europe. The regime, however, does not follow its European counterparts, rather it sets up an advisory body to oversee privacy in general in that state. The Committee has taken a very active role and produced many publications and raised many privacy issues. It has played a de facto role as a national educator in privacy issues in the past.[37]

The Committee produced a reform proposal in its recent report to the Independent Commission Against Corruption.[38] This proposal advocates the implementation of a passive structure with a privacy committee presiding over it. This proposal has been taken a step further and is largely contained in the *Data Protection Bill* 1991 currently before the NSW parliament.

The bill deals with privacy protection generally but most of its provisions deal with data protection issues specifically. The bill may be broken into four components: penal provisions; regulation of the public sector; regulation of the private sector; and the powers of the privacy committee.

The penal provisions focus on the unlawful transfer and use of personal data held by public sector. For example, there are offences created for soliciting the disclosure of personal data;[39] obtaining such information from a public employee where the recipient knows, or ought to know, that the employee is guilty of an offence where the recipient uses or discloses the information;[40] and a general offence prohibiting the use or disclosure by a public employee, or former public employee, of personal information obtained in the performance of his/her

---

37 This role has now passed to the federal Privacy Commissioner, see *Privacy Act* 1988 s.27(l), (m) and (n).

38 Privacy Committee of NSW, "Privacy and Data Protection in New South Wales: A proposal for Legislation" Report no. 63/1991.

39 Cl.7.

40 Cl.8.

official functions for the purpose of financial gain or other benefit.[41] These offences result from the evidence obtained by the Independent Commission Against Corruption concerning the disturbing amount of personal information made available by some public sector employees or former employees.[42]

The bill takes a softly softly approach to regulation preferring to encourage the culture of data protection by requiring the production of internal guidelines or codes of practice. Government departments have one year from the commencement of the legislation to prepare codes of practice[43] and are required to classify personal information according to its sensitivity and to specify security procedures for dealing with this information. The codes must generally conform to the data protection principles ("DPPs") set out in the bill.[44]

The DPPs set out a minimum standard for data protection and are based on the Information Privacy Principles,[45] which are a derivative of the OECD Guidelines. The bill does not provide any framework to require adherence to the DPPs, rather it seems to hope that government departments will be somehow magically imbued with an appropriate data protection culture. The codes which result from the efforts of each government department will not be enforceable and there is no power for the Privacy Committee to check whether the codes have been implemented. It would be possible for the codes to be merely façades behind which departments may carry on their activities without regard to the DPPs. On the other hand, it is also possible that considerable pressure may be brought to bear on the departments to ensure proper "value-added" codes are prepared. This approach has worked in the finance industry with the voluntary code concerning electronic fund transfers by consumers.

In relation to the private sector, the privacy committee may prepare or review codes of practice as well as the procedures used for dealing with personal information.[46] Once again the codes are encouraged to conform with the DPPs.

Of course, it is recognised that in order for a proposal to succeed, it must be feasible and able to be implemented without unnecessary administrative costs to industry.

---

41 Cl.6.

42 See Second Reading Speech of Mr Tink, Parliamentary Hansard, NSW 27 February 1992, p.6.

43 Cl.11.

44 Cl.12.

45 See *Privacy Act* 1988 (C'lth), s.14.

46 Cl.14.

However, a balance must be struck between the right of the individuals to have their personal information safeguarded and the need for the free flow of information. Without the ability to register or enforce a code, the review process by the committee may be of little impact.

This proposed legislation is pitched at a low level in the sense that it imposes few requirements on government or industry to set up proper data protection practices. The second reading speech implies that the proposal is cast in these terms so that it will have some prospect of being enacted, even in some modified form.[47] The tenor of the proposal suggests that New South Wales is at the very early stages of data protection culture and that an enforceable regulatory structure would be premature. This belies the number of reports and other works in this area and the work of the Privacy Committee itself since the mid-70s.

It may be more appropriate to adopt an approach more like the Netherlands. It would be possible to encourage the development of codes within, say, two years, in consultation with the Privacy Committee. Should an association or department not do this, then the Committee should have the power to provide regulations imposing an appropriate structure and having the ability to review its implementation from time to time. Over and above this, the Committee, if not data subjects, should be able to bring an action for breach of the DPPs once an appropriate phase-in period is over. This type of model permits industry and government the opportunity to control their own affairs or, failing this, to have a regime imposed on it by the Committee. It is submitted that this scheme will be more efficacious than the current proposal.

The importance of this bill should not be understated as it may be used as a model by other states. New South Wales has clearly played the leading role in this area in Australia and it should now advance from the low-key pioneering role set down in the *Privacy Committee Act* 1975, into a more formal position with the power to, ultimately, ensure that data protection is taken seriously. The bill, however, does not significantly increase the powers of the Privacy Committee from those it currently has.[48] It would still lack any of the powers of enforcement of the DPPs.

(iii) Queensland

Queensland adopted the same model as New South Wales, in 1984, when it enacted the Privacy Committee Act. However, the Privacy Committee in that state has been less active than

---

47 See *Hansard*, NSW parliament, 27 February 1992, p.8.

48 Cl.16.

its New South Wales counterpart. The legislation had a sunset clause in it which took effect in June 1991. No current proposal exists for replacing the Privacy Committee Act so that Queensland is currently without generic privacy legislation.

(iv) South Australia

A Privacy Committee also exists in South Australia as a result of a government proclamation in 1989. Once again this Committee has an advisory and an overseeing role similar in nature to those described above. A bill has been prepared, the Privacy Bill 1991, and introduced into parliament.[49] This bill provides a statutory tort of infringement of privacy[50] and permits aggrieved persons to pursue relevant privacy infringements through the courts.[51] No independent privacy body is set up to handle complaints or carry out investigations.

Infringement of privacy is not defined in the abstract, rather an exhaustive list of infringements to the right of privacy is given.[52] This list includes surveillance and harassment as well as personal information infringements. However, it does not amount to an infringement unless it is substantial, unreasonable and not justified in the public interest.[53] Members of the police, or any persons vested with powers of investigation or inquiry, do not infringe privacy where they are carrying out their duties or powers. There are also exemptions for insurance fraud investigations, debt recovery activities lawfully undertaken, approved medical research and investigations carried out under statute.[54] Several major defences are provided:

(i) where the infringement was reasonably necessary or incidental to the protection of the lawful interest of the defendant or his/her principal, or for the conduct of actual or intended litigation.

---

49 The bill was amended by the government after its introduction to parliament in 1991; and it is intended to reintroduce the bill in its revised form in 1992.

50 Note that both the United Kingdom Committee on Privacy, Report Cmnd. 5012 (1972), the Younger Report, para.664 and the Australian Law Reform Commission in "Privacy" Report No.22/1983, para 1081, rejected this approach.

51 This bill appears to be based upon the *Privacy Bill* 1974, No. 150 (South Australia) which did not proceed.

52 Cl.3(2).

53 Cl.3(2)(ii) and (iii).

54 Cl.3(4).

(ii) the media (press, radio or television) have acted in accordance with reasonable privacy standards set down by either the Australian Journalists' Association or the Australian Press Council.

(iii) where the infringement arises from publication of material a defence exists if the defendant would have had a defence to a defamation action on the basis of absolute or qualified privilege.[55]

Corporations will not be protected by the proposed legislation.[56]

Finally, the Governor may make regulations setting out standards to be adhered to by controllers of personal information.[57] Breach of these standards would be evidence, but not conclusive evidence, of an infringement of privacy.[58] This provision implicitly encourages organisations to attempt to regulate their own affairs or risk strict external regulation. It may have been better to encourage the creation of voluntary codes of practice or guidelines in the first instance to make it plain that these instruments may be taken into account before any regulatory standard is set down by the Governor.[59]

The Act is a positive step in privacy protection, however, it is out of step with both Australian and overseas developments. It also relies upon the data subject having the temerity and money to bring an action.

(v) Victoria

As mentioned earlier, the Legal and Constitutional Committee in Victoria has produced a report on breach of confidence in May 1990. The conclusions of the committee were, inter alia, that an extension of breach of confidence to cover privacy infringements was inadequate and it recommended that action be taken to provide an acceptable remedy in this area.[60] A privacy reference has been given to the Victorian Law Reform Commission and its report is expected by July 1992.

In a related matter, the Attorneys General of New South Wales, Queensland and Victoria have recommended that state

---

55 Cl.4(3).

56 Cl.3(5).

57 Cl.6(1).

58 Cl.6(2).

59 There are similarities between this provision and the Dutch data protection regime.

60 See Legal and Constitutional Committee, "Privacy and Breach of Confidence" Report no. 40/1990.

defamation laws be altered to provide for a legislative truth plus privacy defence.[61]

Under provisions contained in the *Defamation Bill* 1991 (Victoria), truth remains a complete defence to defamation. However, where the alleged material relates to the plaintiff's "private affairs" then the defendant must, in addition to truth, establish that either the publication was warranted in the public interest or that qualified privilege exists and the manner of publication is reasonable in the circumstances.[62] Private affairs include "the health, private behaviour, home life, personal relationships or family relationships of the person."[63] the determination of what constitutes "public interest" is left to the court not the jury.[64]

The private affairs defence seems to provide a further ground for pecunious plaintiffs to pursue a remedy for distasteful matters published about them. However, the width of the non-exhaustive definition of "private affairs" contained in the bill and the unknown meaning of "public interest" leave considerable doubt as to the scope of the defence. In any case, there would seem to be little merit in this form of privacy protection as it protects nothing of the sort, it merely seeks to compensate plaintiffs; their privacy remains invaded. It may also be argued that this provision shifts the delicate balance which exists between the right to protection of personal data and the right to freedom of speech for it permits the defendant to be held liable for a true statement.

The question remains, should the law err in favour of the one or the other? Civil rights supporters will argue that it represents an important deterrent to protect reputation whilst the media, for example, will claim that it unduly fetters freedom of speech. One thing is certain, in these days of attempting to make law clearer and more accessible to the general public, this proposal fails. It appears better not to cross-thread the law of defamation with the concepts of reputation and privacy (or private affairs) rather the protection of privacy should be provided as part of a comprehensive framework independent of the complex, expensive defamation litigation proceedings.[65]

---

61 See Discussion Paper on Reform of Defamation Law, Attorneys General of New South Wales, Queensland and Victoria, 1990.

62 See *Defamation Bill* 1991 (Vic) Cl.20.

63 Cl.4.

64 Cl.9.

65 See generally, Palmer, A. "Defamation Law Reform" (1991) 65 LIJ 505; Castles, A "Now And Then" (1992) 66 ALJ 167; and O'Connor, K "The Truth: the Whole Truth and Nothing But the Truth? Australian Newspapers

(vi) Western Australia

Western Australia is currently preparing reform proposals but to date, nothing has been released. An opposition member's bill, the *Data Protection Bill* 1988, was introduced in the Western Australian parliament in that year.[66] This bill was based on the *Data Protection Act* (UK) which sets up a registration system across the public and private sectors. It did not proceed.

(b) The Federal Privacy Act

The *Privacy Act* 1988 covers federal agencies and departments, users and recipients of the tax file number and the credit reporting industry. Accordingly, the thrust of the Act is to regulate the federal public sector with some sectoral extensions into the private industry. The Act is inappropriately named as it does not deal with privacy protection generally, rather only the protection of personal information.

The regime does not require registration of personal information or files held, rather it sets up a model, in the form of information privacy principles, which the agencies and departments must adhere to. These principles must be read in conjunction with the *Freedom of Information Act* 1982 (C'lth). The Commissioner may exempt a federal government agency from adherence to one or more of these principles where "the public interest in the agency doing the act, or engaging in the practice, outweighs, to a substantial degree the public interest in adhering to that Information Privacy Principle."[67]

In relation to the tax file number a set of guidelines has been provided by the Commissioner which must be adhered to by recipients and users of the restricted identifier. Data-matching using the tax file number has also been specifically controlled.[68]

The consumer credit reporting industry is subject to detailed and complex provisions set out in the *Privacy Amendment Act* 1990 (as amended) and the Code of Conduct 1991. This legislation concerns the contents collection, use, and disclosure of consumer credit information. It limits, inter alia, the parties who have access to consumer credit files held by credit reporting bureaux. The legislation is not directed towards the protection of credit information where it is not relevant to consumers. Stringent requirements are placed on credit providers, which include financial institutions, as to the access and use they make of information gained from

---

Towards the Year 2000". Paper presented at Library Society Seminar, Sydney, 20 October 1990.

66 See second reading speech of Mr Hassell, Parliamentary Hansard, 12 October 1988, p.31.

67 *Privacy Act* 1988 (C'lth) s.72.

68 See *Data-Matching Program (Assistance and Tax) Act* 1990 (C'lth).

the credit reporting bureaux. Substantial penalties may apply for breach of these provisions. For example, where disclosures are made knowingly or recklessly by credit providers, other than in accordance with the Act, then fines of up to $150,000 apply[69]. Several crimes are created including: false or misleading credit reports;[70] unauthorised access to credit information files or credit reports;[71] and obtaining access to credit information files or credit reports by false preferences.[72]

An anomalous position exists in the area of telecommunications. Until February 1992, the Australian telecommunications network provider, Telecom, was subject to the provisions of the *Privacy Act* 1988 (C'lth). The de-regulation of the industry has seen Telecom, now OATC, move outside the jurisdiction of the federal Act. Austel, the telecommunications regulator, is considering submissions on how privacy protections will be best maintained in the new environment. What should be the appropriate framework, and how should particular services and technologies be regulated are central questions.[73] There is a great deal of work on this sector being done overseas, particularly by the European Commission and the Council of Europe.[74]

(c) The Common Law

No right to privacy is recognised under the common law in Australia. Several recent new decisions have provided obiter dicta giving strong endorsement to the need for privacy protection laws either by statutory means or, failing that, by under the common law: see *Tucker v News Media Ownership*[75] and *T v AG*[76]. A mishmash of laws exist which directly, and indirectly, have some impact on data protection. These include actions for breach of confidence, privileged communications, trespass, and the implied contractual duty of secrecy.[77] However, these laws, at best, only provide incidental protection.

---

69 *Privacy Act* 1988 (C'lth) s.18N(2) (as amended).

70 s.18R

71 s.18S

72 s.18T

73 Services, like calling line identification, call forwarding and telemarketing have specific privacy and data protection concerns.

74 See European Commission, proposed directive on the protection of personal data and privacy in the context of public digital telecommunications networks (COM (90)) 314, SYN 288, 1990) and Council of Europe draft Recommendation on data protection and the telecommunications section (Strasbourg, 1992).

75 [1986] 2 NZLR 716.

76 Unreported decision of Ellis J., High Court, 1 December 1988.

77 For a more detailed discussion of these areas, see Tucker, G *Information Privacy Law in Australia* 1992, Longman Cheshire, Ch 3 and Hughes, *Data Protection in Australia*, The Law Book Co, 1991, Chs. 6 & 7.

(d) The Criminal Law

The criminal law has also provided limited protection of data generally. In particular, personal data is protected specifically in computer crime legislation.[78] These provisions exist in most Australian states, territories and at federal level. Although the legislation is not uniform, generally offences exist prohibiting unauthorised access to computers and/or data contained in them. In some cases, these offences are only misdemeanours. The *Crimes Act* (C'lth) provides:

"(2) A person who:

(b) intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows, or ought reasonably to know, relates to:

(v) the personal affairs of any person;

is guilty of an offence. Penalty: Imprisonment for 2 years"[79]

Similar provisions exist in the NSW counterpart.[80] Whilst it may be useful to have penal sanctions underpinning this area, these only give incidental support to any civil remedies and may provide some deterrent effect.

Conclusions

It cannot be said that Australian governments have ignored privacy concerns. The legion of reports, legislative proposals and Acts demonstrate considerable effort. However, much of this has led to nothing with the *Privacy Act* 1988, with its enlarged jurisdiction, being the only substantial development. There are several projects still on-going in some states and territories; unfortunately these lack cohesion.[81]

Constitutional questions aside, other federations have had success in developing and unifying data protection laws. For example, Germany and, to a limited extent, Switzerland, have workable national regulations.[82] Without uniform regulation in Australia there will be a lack of procedural

---

78 See generally, *Informational Privacy Law in Australia* Ch.5.

79 Part VIA s.76B and see also s.76D(2)(b)(v).

80 See the *Crimes (Computers and Forgery) Amendment Act* 1989 (NSW), No.71.

81 National uniformity was advocated by the Australian Law Reform Commission in 1983, ALRC Report on Privacy No.22/1983, paras.1088 - 1092.

82 Germany has already extended its data protection law to the five new Lander which have resulted from the unification of East and West Germany in October 1990.

simplicity for business operating across state boundaries which will add unnecessary costs to it.

In addition to a united approach, Australia should take account of the EC draft directive, once it is in final form, so that neither governments nor industry will suffer adversely from having "inadequate" data protection regulations. The model contained in the *Privacy Act* 1988 (C'lth) is a good starting point. This could be adopted by state and territory governments for application to the public sectors. It could also be applied to the private sector, but would require substantial redrafting.

It is not only government that can have input into this area. The development of internal guidelines or codes of practice by industry associations are important and mark a movement towards the appropriate culture. This process has only just begun in Australia. It is hoped that Australia moves out of its "privacy creep" phase and embraces the regulation of the area with broader, less parochial, vision.