NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Privacy Law Reform: Issues and Recent Developments

by

Gareth Griffith

Briefing Paper No 20/98

RELATED PUBLICATIONS

- Listening devices and other forms of surveillance: issues and proposals for reform by Rachel Simpson, Briefing Paper No 20/97
- Privacy and Data Protection Law Reform: Some Relevant Issues by Gareth Griffith, Briefing Paper No 15/96
- The Individual's Right to Privacy: Protection of Personal Information in NSW by Vicki Mullen, Briefing Paper 14/95
- Privacy and Data Protection Bill 1994 by Gareth Griffith, Bills Digest No 13/94

ISSN 1325-5142
ISBN 0 7313 1633 9

December 1998

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Dr David Clune, Manager . . . . . (02) 9230 2484

Dr Gareth Griffith, Senior Research Officer,
Politics and Government / Law . . . . . (02) 9230 2356

Ms Honor Figgis, Research Officer, Law . . . . . (02) 9230 2768

Ms Rachel Simpson, Research Officer, Law . . . . . (02) 9230 3085

Mr Stewart Smith, Research Officer, Environment . . . . . (02) 9230 2798

Ms Marie Swain, Research Officer, Law/Social Issues . . . . (02) 9230 2003

Mr John Wilkinson, Research Officer, Economics . . . . . (02) 9230 2006

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

Information about Research Publications can be found on the Internet at:

http://www.parliament.nsw.gov.au/gi/library/publicn.html

CONTENTS

EXECUTIVE SUMMARY

Building on previous Parliamentary Library publications, this paper takes up the story of privacy law reform from 1996 onwards. The paper begins by distinguishing between different categories of privacy (pages 1-3). It then considers recent developments and proposed developments in various jurisdictions, including Canada, the US and the UK. This discussion takes in issues relating to the protection of privacy in the private sector where the key issue is whether law makers follow the self-regulatory model, as currently preferred in the US and at the federal level in Australia, or whether a co-regulatory/legislative approach is taken, as in New Zealand. Much may depend on what is found to be 'adequate' protection under the EU Data Protection Directive (page 20). The one constant feature of the debate on privacy over recent years, especially as this has related to the protection of privacy in the private sector, has been the concern to establish a nationally consistent regime (page 11).

The immediate response to the long-running privacy debate in NSW is considered in the next section of the paper which takes as its focus the introduction in NSW of the *Privacy and Personal Information Protection Act 1998*. This Act is directed to the State public sector only. It does not cover the private sector; nor does it cover State owned corporations (pages 20-33).

NSW legislation dealing with video surveillance in the workplace is dealt with separately (pages 33-36); while the last section of the paper comments on two further issues, namely, the surveillance of e-mail communications in the workplace and the implications of Internet communication generally for the protection of privacy (pages 36-42).

1. INTRODUCTION

In 1996 the NSW Parliamentary Library published a briefing paper which discussed the key issues in the area of privacy and data protection law reform. It reported that the NSW Government had said that it would introduce new privacy legislation in 1996, with the Attorney General foreshadowing the introduction of 'Australia's most comprehensive privacy and data protection package' containing industry codes of practice for the private sector.[1] The briefing paper reported, too, that on 25 July 1995 the European Union's Council of Ministers adopted the Directive on the Protection of Individuals with regard to the processing of Personal Data and on the Free Movement of Such Data (the EU Data Protection Directive). This Directive, which came into force on 24 October 1998,[2] established a set of legal principles for privacy protection which applies to all EU member-states and, significantly, prohibits the transfer of personal data from EU countries to any countries which do not have 'adequate' data protection laws.[3] More generally, the paper indicated that privacy in its many forms - information privacy, privacy of the person, privacy of communications free from surveillance, as well as privacy of personal space - are all issues of significant current interest and some controversy.

With this in mind, this paper takes up the story of privacy law reform from 1996 onwards, taking as its focus the introduction in NSW of the *Privacy and Personal Information Protection Act 1998*. The paper begins by distinguishing between different categories of privacy. It then considers recent developments and proposed developments in various jurisdictions, including Canada, the US and the UK. This discussion takes in issues relating to the protection of privacy in the private sector. NSW legislation dealing with video surveillance in the workplace is dealt with separately, while the last section of the paper comments on two further issues, namely, the surveillance of e-mail communications in the workplace and the implications of Internet communication generally for the protection of privacy.

2. CATEGORIES OF PRIVACY

A collection of rights: Privacy relates to a bundle or collection of rights which all stem from the idea that, subject to certain legitimate qualifications, in a liberal democracy the individual has a right 'to be let alone'.[4] In more specific terms, the Australian Privacy Charter states:

> People have a right to privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about

---

1 G Griffith, *Privacy and Data Protection Law Reform: Some Relevant Issues*, NSW Parliamentary Library, Briefing Paper No 15/1996, pp 4-7.

2 M Scollay, 'Privacy protection in Australia: how far have we come?' (1998) 48 *Telecommunications Journal of Australia* 7 at 9.

3 G Griffith, *Privacy and Data Protection Law Reform: Some Relevant Issues*, p 7.

4 LD Brandeis and SD Warren, 'The right to privacy' (1890) 4 *Harvard Law Review* 193 at 195.

a person), and freedom from surveillance.[5]

Freedom from surveillance: The word 'surveillance' is defined in the Charter to mean 'the systematic observation or recording of one or more people's behaviour, communication, or personal information'.[6] Surveillance can itself take many forms and may be relevant to a number of the categories of privacy which are discussed below.

Privacy of information: 'Information privacy' is a subset of privacy which, in the words of the Canadian Task Force on Electronic Commerce, 'involves the right of individuals to determine when, how and to what extent they will share personal information about themselves with others'.[7] It is said in this regard that 'information privacy' involves the notion that people, at least to some extent, should be able to regulate the way information about themselves is gathered, stored and used.[8] The underlying question in this context therefore is whether business and government operate in a way that protects the privacy of the personal information they collect and use. Medical and police reports, employment and criminal records, information concerning political or religious affiliations and refused licence applications are all instances of the kind of personal information which data protection laws and principles have sought to protect.

It is said, too, that 'Information privacy is not the same as protecting privacy in its broadest sense because it is concerned mainly with information that has been collected fairly and legally'.[9] Typically, information privacy relates to personal information which is held on established data bases in the public and private sector: public registers, on the one hand, and the data held by such organisations as banks and private hospitals, on the other, are obvious examples.

The growth of electronic commerce, which may involve any combination of government, business and individuals, is an important development in this respect, highlighting as it does the challenges involved in protecting information privacy in the global village created by modern technology. Examples of electronic commerce include electronic data interchange between wholesalers and retailers, telephone banking and the purchase of products and

---

5 'The Australian Privacy Charter' (1995) 2 *Privacy Law and Policy Reporter* 44.

6 Ibid. For a discussion of the different types of surveillance see - R Simpson, *Listening Devices and Other Forms of Surveillance: Issues and Proposals for Reform*, NSW Parliamentary Library, Briefing Paper No 20/1997, p 2; NSW Law Reform Commission, *Issues Paper 12 - Surveillance*, May 1997, p 6.

7 Canadian Task Force on Electronic Commerce, *The Protection of Personal Information: Building Canada's Information Economy and Society*, January 1998, p 28 - http://canada.justice.gc.ca

8 Legislative Assembly of Queensland, Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland, Report No 9*, April 1998, p 9.

9 Victorian Department of State Development, *Discussion Paper: Information Privacy in Victoria - Data Protection Bill*, July 1998, p 12 - http://www.mmv.vic.gov.au/.

services on the Internet.[10] It is said, in addition, that 'The electronic delivery of Government services, such as online registrations and tenders, changes of address and electoral enrolments (which may not always be considered commercial in a conventional sense), assumes a commercial character when supplied via the Internet'.[11]

Privacy of communications: An overlapping yet still distinct category of privacy relates to the privacy of personal communications, be they in oral or written form. The Australian Privacy Charter states that 'People who wish to communicate privately, by whatever means, are entitled to respect for privacy, even when communicating in otherwise public places'.[12] The further point is made that 'Respecting privacy of communications means that (subject to the context and medium by which it occurs) people should be able to conduct their affairs without being subject to surveillance'.[13] The monitoring by employers of E-mail communications in the workplace is an example which has been the subject of recent comment.

Privacy of space or territory: This category of privacy is said to 'recognise that people should have the right to conduct their personal affairs in certain private spaces, such as their homes, free from surveillance and that there should be some controls on people entering that private space or territory'.[14] According to the Australian Privacy Charter the right of individuals to conduct their affairs free from surveillance or fear of surveillance should apply, 'to varying degrees, in the workplace, the use of recreational facilities and public places'.[15]

Privacy of the body or person: With respect to the physical privacy of the person it is said that 'an individual should have freedom in relation to their own body and that a high level of justification is required for a person to be subjected to body searches, or for their physical or behavioural characteristics to be monitored'.[16]

3. BACKGROUND ISSUES

---

10 Canadian Task Force on Electronic Commerce, *The Protection of Personal Information: Building Canada's Information Economy and Society*, January 1998, p 1 - http://canada.justice.gc.ca

11 Victorian Department of State Development, *Discussion Paper: Promoting Electronic Business - Electronic Commerce Framework Bill*, July 1998, p 7 - http://www.mmv.vic.gov.au/

12 'The Australian Privacy Charter' (1995) 2 *Privacy Law and Policy Reporter* 44.

13 Legislative Assembly of Queensland, Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland, Report No 9*, April 1998, p 9.

14 Ibid, p 8.

15 'The Australian Privacy Charter' (1995) 2 *Privacy Law and Policy Reporter* 44 at 45.

16 Legislative Assembly of Queensland, Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland, Report No 9*, April 1998, p 8.

Developments at the Federal level in Australia: The present Federal *Privacy Act 1988* covers the collection, storage, use and disclosure of personal information held by the Commonwealth Government. This scheme also extends to tax file numbers and credit card reporting. Moreover, privacy protection provisions are included in the Federal *Telecommunications Act 1997*.[17] Other than these limited situations the Federal *Privacy Act* does not extend to the private sector. The main question therefore over the past few years, for those involved in the ongoing privacy debate, has been whether the Federal scheme should be extended to cover the private sector more generally, forming the basis of a nationally consistent scheme.

According to the Federal Privacy Commissioner, Moira Scollay, from 1994 to 1996 there were numerous reviews and inquiries into issues associated with the growth of the information society, all of which referred to privacy as an important subject and to 'the need for an appropriate regulatory or protective framework for the private sector in Australia'.[18] These Government reviews of privacy regulation and the private sector included:

- In December 1994 the Broadband Services Expert Group, established by the Federal Government to examine the technical, economic and commercial preconditions for the widespread delivery of broadband services in Australia, recommended that the privacy of users should be protected by developing a self-regulatory scheme for network participants within the framework of the Privacy Act.

- In its June 1995 report, ***In Confidence***, on the protection of confidential personal and commercial information held by the Federal Government, the House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that the protections provided in the Privacy Act should be extended to the private and public sectors by way of a national privacy code.

- The Senate Economic References Committee released in November 1995

---

17 That Act sets out the means for regulating the telecommunications industry in Australia, including a scheme for regulating privacy through industry codes and industry standards (sections 112 and 135). The Australian Communications Authority will oversee this regulation, including any privacy scheme the telecommunications industry adopts. The limitations of the scheme were discussed by Senator Stott Despoja on the behalf of the Australian Democrats who noted, among other things, that there are no legislated mechanisms for investigating a privacy breach or for an individual to bring an action for breach of the industry code or industry standard - N Stott Despoja, 'Personal and Private' (August 1997) 22 *Alternative Law Journal* 165 at 167. The Federal Privacy Commissioner has also noted the limitations of the scheme, stating that the Act 'is limited to carriers, carriage service providers and specified others which means that the coverage of any codes is also limited'. The Commissioner's concern was that the nature of the telecommunications environment is such that many non-regulated organisations could come into possession of personal information as a result of telecommunications services - M Scollay, 'Privacy protection in Australia: how far have we come?' (1998) 48 *Telecommunications Journal of Australia* 7 at 12; see also Federal Privacy Commissioner, *Ninth Annual Report on the Operation of the Privacy Act*, 1 July 1996 to 30 June 1997, pp 46-48.

18 M Scollay, 'Privacy protection in Australia: how far have we come?' (1998) 48 *Telecommunications Journal of Australia* 7 at 9.

Connecting You Now, a report on the impact on industry, employment and the community of telecommunications developments to the year 2000 and beyond. The report recommended that the Information Privacy Principles in the Privacy Act be expanded to cover new telecommunications privacy risks in both the public and private sectors.

- The Senate Finance and Public Administration References Committee reported in December 1995 on service delivery by the Australian Public Service. The report recommended that the mandate of the Privacy Commissioner be expanded to permit investigations into breaches of privacy by contractors and other non-government bodies providing services on behalf of the government.

- The Australian Law Reform Commission and the Administrative Review Council concluded a review of the *Freedom of Information Act 1982* with the tabling of the final report in Parliament on 24 January 1996. The report recommended the creation of a separate statutory office of FOI Commissioner to administer the FOI Act and the removal of overlaps between the FOI Act and the Privacy Act for access and correction rights for personal information. The report also recommended that a national legislative scheme be introduced to provide information privacy protection in all sectors.[19]

- In June 1996, the Australian Broadcasting Authority reported on its inquiry into the content of on-line services. It recognised privacy, in addition to billing and credit management, as issues that need to be addressed if on-line services are to be used effectively and productively. It recommended that industry codes of practice be developed by on-line service providers with the Australian Broadcasting Authority having a monitoring role; the Privacy Commissioner would have a role in handling complaints that involved privacy issues.[20]

- In April 1997 the '**Wallis Inquiry**', which was established by the Federal Treasurer, tabled its final report in relation to its Financial Services Inquiry. The report recommended that, if a privacy regime is to extend to the financial services sector, then any extensions to privacy laws should apply only at a national level. In its view, uncoordinated action at the State and Territory level could result in considerable additional costs and inefficiencies.[21]

- In May 1998, in its report on ***Internet Commerce: To Buy or Not to Buy?***, the Joint Committee of Public Accounts and Audit stated that 'Consumer protection and privacy are threshold issues for the successful development of Internet commerce'.

---

19 ALRC and Administrative Review Council, *Report No 77 - Open Government: A Review of the Federal Freedom of Information Act 1982*, 1995, p 206.

20 M Scollay, 'Privacy protection in Australia: how far have we come?' (1998) 48 *Telecommunications Journal of Australia* 7 at 13-14.

21 S Wallis, *Financial System Inquiry: Final Report*, March 1997, pp 517-524.

> The report discussed the arguments for and against a self-regulatory regime only to conclude that a 'legislated privacy regime will be more effective than a self-regulatory approach. Privacy legislation for the private sector will ensure better coverage, receive international recognition, and will discourage state governments from passing their own legislation'. It recommended, therefore that the Federal Government 'introduce privacy legislation, with specific reference to information communications, to govern the use of personal information in the private sector'.[22]

Back in 1996 it looked as though the Federal Government would introduce legislation to extend the Privacy Act to cover the private sector. The Coalition went into the March 1996 election saying it would, 'in consultation with the States and Territories, ensure the implementation of a privacy law regime in Australia comparable with best international practice'.[23] Subsequently, in September 1996, the Attorney-General's Department released a Discussion Paper on ***Privacy Protection in the Private Sector*** which canvassed the possibility of extending the coverage of the Privacy Act to as much of the private sector as the Commonwealth's constitutional reach would allow. A co-regulatory approach to privacy protection in the private sector, which drew heavily on the New Zealand model,[24] was envisaged based on industry codes of practice supervised by the Privacy Commissioner and subject to statutory backing. If implemented, the proposal would have introduced national privacy legislation covering the private sector.

A 1996 survey of Australian businesses conducted by Price Waterhouse suggested that 64 per cent favoured such a course;[25] a follow-up survey in 1997, based on responses from 130 of the largest companies in Australia, suggested that the comprehensive privacy legislation option was supported by over 70 per cent of companies.[26]

---

22 The Parliament of the Commonwealth of Australia, Joint Committee of Public Accounts and Audit, *Report 360 - Internet Commerce: To Buy or Not to Buy?*, May 1998, pp 199-203.

23 G Greenleaf, 'Privacy and Australia's New Federal Government' (March/April 1996) 3 *Privacy Law and Policy Reporter* 1.

24 This was discussed in G Griffith, *Privacy and Data Protection Law Reform: Some Relevant Issues*, NSW Parliamentary Library, Briefing Paper No 15/1996, pp 9 -15. Basically, the New Zealand *Privacy Act 1993*, which applies to both the public and private sectors, involves a set of statutory Information Privacy Principles (IPPs) together with provision for the development of suitable codes of practice modifying the application of the IPPs to suit specified information, activities, organisations, industries or professions - Legislative Assembly of Queensland, Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland, Report No 9*, April 1998, p 150.

25 M Paterson, 'Privacy protection in Australia: the need for an effective private sector regime' (1998) 26 *Federal Law Review* 371 at 372.

26 'Price Waterhouse survey 1997' (May 1997) 4 *Privacy Law and Policy Reporter* 22. The survey also showed that, of the organisations surveyed, 79 per cent felt that 'only minor changes would be required to their business practices in order to comply with legislation, highlighting the fact that Australian business does not believe there will be significant costs associated with applying good privacy practice'. Note, however, that the survey did not canvass the views of small and medium size businesses.

Such findings not withstanding, on 21 March 1997 the Prime Minister announced that the Government had decided against this legislative option of extending the Privacy Act to cover the private sector. He stated:

> The Commonwealth opposes such proposals which will further increase compliance costs for all Australian businesses, large and small. At a time when all heads of Government acknowledge the need to reduce the regulatory burden, proposals for new compulsory regimes would be counterproductive. On these grounds, the Commonwealth will not be implementing privacy legislation for the private sector.[27]

By way of an alternative, the Prime Minister offered the services of the Privacy Commissioner to provide assistance to the private sector in developing voluntary codes. Following up on this, in August 1997 the Privacy Commissioner released a consultation paper entitled, ***Information privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector***. The Federal Privacy Commissioner explains that 'The scheme presented in this paper attempted to provide a viable self-regulatory option but was designed to be compatible with existing Commonwealth privacy laws and any further legislation which might be considered necessary in particular sectors, States or Territories'.[28] The scheme had four components: (a) principles or standards for the handling of personal information; (b) processes for businesses to sign on to the scheme, and for promoting and monitoring compliance with the principles; (c) mechanisms for handling complaints about breaches of the principles, and providing effective remedies for people affected; and (d) an independent scheme administrator.

The Federal Privacy Commissioner reports that: 'In the broad consultations that followed, it quickly became clear that the major issue is the need for national consistency in privacy standards'. She noted, too, that while there was clear consensus on the need for principles, 'the issues surrounding the mechanisms for implementation were more complex and contentious' and that, as a result, she decided to divide the process of developing a national privacy scheme into two stages, developing principles first and then moving on to the implementation issues.[29] The first stage was completed on 20 February 1998 with the release of ***National Principles for the Fair Handling of Personal Information***, described by the Privacy Commissioner 'a workable compromise that would, if properly implemented, protect people's privacy with minimal red tape'.[30] For the most part these 'National Principles' can be described as a plain English version of the conventional information privacy principles which are found in the Federal privacy legislation. In summary, the

---

27 G Greenleaf, 'Commonwealth abandons privacy - for now' (April 1997) 4 *Privacy Law and Policy Reporter* 1 at 3.

28 M Scollay, 'Privacy protection in Australia: how far have we come?' (1998) 48 *Telecommunications Journal of Australia* 7 at 10.

29 Ibid.

30 The Parliament of the Commonwealth of Australia, Joint Committee of Public Accounts and Audit, *Report 360 - Internet Commerce: To Buy or Not to Buy?*, May 1998, p 192.

National Principles cover guidelines and undertakings in the following areas: collection; use and disclosures; quality and security; openness and transparency; access and correction; identifiers; anonymity; and transborder transfers. The last two features are said to account for the most innovative features of the National Principles which are said by Professor Graham Greenleaf to include:

- there is some recognition of the need for an explicit principle allowing anonymous transactions to the maximum extent possible;

- there is a principle preventing transfers of personal data to jurisdictions where it will not receive 'adequate protection'.[31]

However, Professor Greenleaf spends more time discussing the scheme's deficiencies, an indication that privacy advocacy groups have consistently opposed the self-regulatory regime which the Federal Government seeks to promote. Indeed, at the outset consumer and privacy advocate groups intended to boycott the consultation process altogether. These groups were said to include the Australian Consumers Association, Australian Privacy Foundation, Communications Law Centre, Consumers Federation of Australia, Council of Civil Liberties, Electronic Money Information Centre, NSW Privacy Committee, Public Interest Advocacy Centre and the Tenants Union of NSW.[32] Subsequently, after representations from the Privacy Commissioner, consumer advocates agreed to take part in the process although they continued to stress that its outcome did not 'represent a consensus of views of those consulted'; consumer advocates were willing to discuss principles but not self-regulation.[33] When the National Principles were released in February 1998 it was said that the National Australia Bank and American Express favoured a legislative privacy regime. On the other side, reports suggested that the Insurance Council of Australia, the Australian Bankers Association, together with small business generally supported the voluntary privacy standards,[34] as did Telstra, the Australian Direct Marketing Association, AAMI, Asia Pacific Smart Card Forum and the Australian Chamber of Commerce and Industry.[35] In the journal, *Privacy Law and Policy Reporter* it was reported in August 1998 that:

> The current status of the National Principles for the Fair Handling of

---

31 G Greenleaf, Submission to Senate Legal and Constitutional References Committee, *Inquiry Into Privacy and the Private Sector*, Volume 3, p 560.

32 'Self regulation of privacy data hits troubles', The Australian Financial Review, 9 October 1997.

33 G Greenleaf and N Waters, 'Putting the "National Principles" in context' (February/March 1998) 4 *Privacy Law and Policy Reporter* 161. This special issue was devoted to the National Principles. It included articles from representatives of the Australian Bankers' Association (Ian Gilbert) and of the Australian Chamber of Commerce and Industry (John Martin) supporting the Principles released by the privacy Commissioner.

34 'Privacy code gets cold shoulder', *The Australian Financial Review*, 21 February 1998.

35 'Privacy guidelines blasted as "toothless"', *The Newcastle Herald*, 21 February 1998.

> Personal Information is somewhat uncertain. Consumer and privacy groups have not endorsed it. Only a very limited range of business organisations have endorsed it or shown interest in implementation, among them banking, insurance, direct marketing and retail organisations. The Ministerial Online Council only gave a qualified endorsement in May 1998, urging governments to "endeavour to standardise on the National Principles - *once further developed to set a benchmark*".[36]

It can be said, too, that the National Principles have only received qualified endorsement from the European Union which described them as 'a significant step forward towards the introduction of comprehensive framework for privacy protection in the private sector'. The European Union added that the Principles fall short of the OECD 1980 Guidelines, which Australia adhered to in 1984, and that its concerns were focused on:

- the scope of the Principles which at this stage do not apply to employee data - an important area for international data flows;
- the possibility to use the data for a different purpose from that of collection and namely for direct marketing without providing sufficiently strong safeguards;
- the individual's right to access his personal data, which appears to be subject to a great number of exceptions and restrictions;
- the use of implicit consent for the handling of sensitive data, which we believe should be awarded greater protection; and
- the lack of specific provisions dealing with the issue of onwards transfers. To ensure that any given privacy system is effective, we would caution against allowing data to circulate to organisations that do not abide by the Principles.[37]

In relation to the self-regulation versus co-regulation/legislation debate and the question of what would constitute 'adequate' protection for the purposes of the EU Directive, the European Union stated that self-regulation is 'not, by definition, inadequate'. This is because, it was explained, 'in assessing the adequacy of protection in third countries, we are more concerned with the content and effectiveness of the measures in place than with their form...In the same way as for laws, self regulatory systems will be considered adequate if they cover the principles enumerated above, are effectively enforced and offer a means for the individual to exercise his rights and gain redress if necessary'.[38]

On 6 August 1998 the Federal Attorney General announced what he called a 'privacy first' for the insurance industry, with the launch of the General Insurance Information Privacy

---

36 G Greenleaf, 'Privacy and consumer organisations withhold endorsement of National Principles"' (August 1998) 5 *Privacy Law and Policy Reporter* 41.

37 European Union, Submission to Senate Legal and Constitutional References Committee, *Inquiry Into Privacy and the Private Sector*, Volume 8, p 1356.

38 Ibid, p 1355.

Principles, developed by the Insurance Council of Australia. The Attorney General commented that the general insurance industry is the first industry to have devised and implemented its own privacy code based on the Privacy Commissioner's National Principles.[39]

In the meantime, on 5 March 1998 the Federal Government introduced the ***Privacy Amendment Bill 1998***, the purpose of which was to extend the application of the Privacy Act to personal information held by contractors in relation to services provided to the Commonwealth. In effect the Bill sought to close the out sourcing 'gap' in the protection of personal information which has developed as a result of the contracting out of government services. The Bill did not extend the Federal privacy regime to the private sector generally. Instead, it made it clear that that regime would only apply to contractors when, and to the extent that, they are providing services to the Commonwealth.[40] In the event, this limited-purpose Bill became entangled in the wider debate about extending the privacy regime to cover the private sector. Provisions of the Bill were referred on 14 May 1998 to the Senate Legal and Constitutional References Committee which was directed to look generally at 'The need for Commonwealth privacy legislation to be extended to the private sector...'.[41] The Committee was due to report on 12 August 1998, a deadline which was not met before the General Election was called and one which will very probably be extended by the new Federal Parliament.[42]

Developments at the State and Territory level in Australia: At present there is no privacy legislation in Western Australia, South Australia,[43] Queensland, Tasmania, Victoria or the Northern Territory.[44] In NSW the *Privacy Committee Act* was passed in 1975 and there is now the *Privacy and Personal Information Act 1998*, which is dealt with in a separate section of this paper. Overall, the impression is that the protection of privacy in its

---

39 Federal Attorney General, *Media Release*, 'Privacy first for the insurance industry', 6 August 1998.

40 N Waters, 'Privacy and out sourcing - the privacy Amendment Bill 1998' (March 1998) 4 *Privacy Law and Policy Reporter* 181 at 182.

41 *Commonwealth Parliamentary Debates (Senate)*, 14 May 1998, p 2797. Note that the motion to refer provisions of the Bill to the Senate Committee was moved by Senators Bolkus and Stott Despoja. The latter had introduced as a Private Member's Bill the Privacy Amendment Bill 1997 on 25 September 1997. That Bill would have extended the Privacy Act to cover the private sector. For a commentary on the position taken by the Australian Democrats on privacy see - N Stott Despoja, 'The Democrats' parliamentary privacy initiatives' (September 1997) 4 *Privacy Law and Policy Reporter* 65.

42 As at 26 November 1998 a new reporting date had not been set for the inquiry.

43 South Australia has a Privacy Committee which was introduced under Cabinet Administrative Instruction 1/1989 in July 1989. The South Australian information privacy principles are identical to those in the Commonwealth Privacy Act, but are guidelines, not law.

44 Australian Privacy Commissioner's Office, *Federal Privacy Handbook*, CCH Australia Ltd, [1-100]. It is noted that 'Complaints about breaches of privacy by State government agencies are usually handled by the State Ombudsman'.

many forms remains in its infancy in the Australian States and the question which arises is how is it to be brought to a more mature stage of development.

In part response to this, the one constant feature of the debate on privacy over recent years, especially as this has related to the protection of privacy in the private sector, has been the concern to establish a nationally consistent regime. Indeed, at the same time as the Prime Minister announced in March 1997 that the Federal Government did not intend to legislate for privacy in the private sector, in order to avoid a patchwork of regimes he also requested the States and Territories not to pass their own separate privacy laws for the private sector. **Queensland** and the **Northern Territory** agreed to this request.[45]

In Queensland, however, a major report on privacy by the Legal, Constitutional and Administrative Review Committee was released on 21 April 1998 which made wide-ranging recommendations. Among other things, the report concluded that: a full-time Privacy Commissioner be established by legislation, along the lines of its federal counterpart; information privacy principles (IPPs) relating to personal information held by both State government departments and agencies (as well as to local governments) be established in legislation; the privacy regime should include offence provisions modelled on those found in the Commonwealth Privacy Act; and that the proposed Queensland Privacy Commissioner should inquire into surveillance undertaken by the private and public sectors with a view to establishing better legislative protection for individuals. On the vexed issue of the application of any privacy regime to the private sector the Committee adopted something of a 'wait and see' approach, while at the same time supporting the Federal privacy Commissioner's efforts to reach agreement on a national scheme which include both 'best practice privacy standards and effective supervisory, enforcement and complaint resolution mechanisms'.[46]

Responding to these and other of the Committee's recommendations, the Queensland Attorney General has proposed that the all-party Scrutiny of Legislation Committee should examine all new legislation to see if privacy has been safeguarded and the Queensland archives legislation should be reviewed. Otherwise, due to budgetary and other considerations the Attorney said it was not possible at this stage to 'affirm adoption of the committee's other recommendations'. He added:

> However, the Government remains committed to its policy to introduce legislation to protect privacy and regulate data banks on individuals in light of the increasing pressure on individuals' private lives from rapidly developing information technology and huge data banks, and the intrusive tactics of some media organisations.[47]

---

45 Legislative Assembly of Queensland, Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland, Report No 9*, April 1998, p 26.

46 Ibid, p 160.

47 Queensland Attorney General, Letter to the Clerk of the Queensland Parliament, 20 October 1998.

Significant developments in privacy legislation have been proposed in **Victoria**. In July 1998 Victoria's Treasurer and Minister for Information Technology and Multimedia, Mr Alan Stockdale, released two discussion papers, one entitled *Information Privacy in Victoria: Data Protection Bill*, the second *Promoting Electronic Business: Electronic Commerce Framework Bill*. The first paper foreshadowed the enactment of comprehensive data protection legislation which, in the words of Professor Greenleaf, 'may deliver fair information practices enforceable against both the Victorian public sector and (to the extent of the reach of Victoria's laws) the entire private sector'. Greenleaf continues, 'Although the Act will allow for the development of approved sectoral codes and enforcement mechanisms, the bottom line is that this is co-regulation, not self-regulation'.[48] In other words, the approach is based on the New Zealand privacy model, which was discussed in the Commonwealth Attorney General's 1996 Discussion Paper, *Privacy Protection in the Private Sector*.

In effect, the proposed privacy regime outlined in the *Discussion Paper - Information Privacy in Victoria: Data Protection Bill* has two elements: support for voluntary schemes and codes; and a default legislative scheme. The discussion paper included a draft Bill, the key elements of which are a statement of the information privacy principles as formulated by the Federal Privacy Commissioner's *National Principles for the Fair Handling of Personal Information*, followed by arrangements for the making of voluntary codes. It was explained that:

> Businesses, government agencies and other organisations handling personal information will be encouraged to develop voluntary codes. These codes will be a means of implementing the *National Principles for the Fair Handling of Personal Information*. The codes may be national in coverage, but would be enforceable only in Victoria. Organisations that do not wish to develop codes will be covered by a default legislative scheme. Where a voluntary code is submitted to the privacy Commissioner and approved, the default legislative scheme will not apply so long as the parties concerned comply with the code.[49]

It was proposed that the Federal Privacy Commissioner would take on the role of overseeing the data protection regime, as well as handling and mediating complaints. On the other hand, complaints that cannot be resolved by mediation would, it was proposed, be referred to the Victorian Civil and Administrative Tribunal.

The discussion paper made it clear that, although it was proposing its own scheme, at the same time the Victorian Government would prefer a national approach to the development of data protection laws, stating 'It is in no one's long term interest to allow Australia's

---

48 G Greenleaf, 'Will Stockdale break the privacy impasse?' (July 1998) 5 *Privacy Law and Policy Reporter* 21.

49 *Discussion Paper - Information Privacy in Victoria: Data Protection Bill*, July 1998, p 11 at http://www.mmv.vic.gov.au/

mixture of privacy measures to continue to grow in an ad hoc way'. This is what the Victorian Government feared would be the result of the self-regulatory scheme favoured by the Commonwealth: 'Codes would be developed only by those that know about privacy issues, are committed to addressing them, and are prepared to carry the full costs of complying even though their competition may decide to avoid the obligations and costs altogether'. The Victorian Government's position was formulated in this way:

> The absence of national data protection legislation placed an onus on the Victorian Government to either take action or accept that Victoria will make a slower and rockier transition to an information economy. The first option is the only choice, as the second is unacceptable. Should the Commonwealth's position change, and it develops a suitable national data protection regime, Victoria will vacate the field to the extent of the Commonwealth's jurisdiction.[50]

Whether the proposals outlined in *Discussion Paper - Information Privacy in Victoria: Data Protection Bill* proceed, and in the form set out therein, remains to be seen.[51] The suggestion is that an exposure draft of a Data Protection Bill is to be released later in the year.

The second discussion paper released by the Victorian Treasurer in July 1998, *Promoting Electronic Business: Electronic Commerce Framework Bill*, is discussed in the last section of this paper.

It is reported that **Western Australia**[52] and **South Australia** are adopting a 'wait-and-see approach' as the implications of the European Directive become clearer. To complete the picture, it can be added that in December 1997 the **ACT** Legislative Assembly passed the *Health Records (Privacy and Access) Act* which protects the privacy of personal health information held by both the public and private sectors.

As for **NSW**, in relation to the public sector it has now introduced its own *Privacy and Personal Information Act 1998*, the background to which is considered in a later section of this paper.

Developments in New Zealand and Hong Kong: Briefly, several countries in the Asia-Pacific region have already passed comprehensive privacy legislation covering both the

---

50 Ibid, p 9.

51 For a critique of the initial draft Bill see - G Greenleaf, 'Will Stockdale break the privacy impasse?' (July 1998) 5 *Privacy Law and Policy Reporter* 21.

52 Western Australian Commission on Government, *Report No 1*, August 1995, p 61. While stating its preference for a legislative privacy regime, the report noted that 'In general, privacy legislation should be restricted to the public sector, but there may be some merit in making provision for the private sector to adopt the privacy principles set down by such a legislative scheme'.

public and private sector. In **New Zealand**, the *Privacy Act 1993* provides a co-regulatory model of privacy protection in which legislative data protection principles (IPPs) are coupled with legally binding codes of practice. These codes are issued by the Privacy Commissioner and their purpose is to modify the data protection principles in such a way that makes them more suitable to specific areas of operation, such as health. These codes are disallowable instruments and a breach of a code is treated as a breach of an IPP, which means that the complaints and enforcement provisions of the Act still apply.[53]

The **Hong Kong** Personal Data (Privacy) Ordinance 1995 is in similar terms. However, under the Ordinance a breach of a code of practice does not of itself constitute a contravention of the law, but will be admissible in the investigation of an alleged contravention.[54] Under section 33, the Ordinance also establishes restrictions on transborder dataflow, which means that, subject to certain exceptions, it prohibits the export of personal information from Hong Kong unless the information receives similar protection in the importing country. However, section 33 is yet to come into force.[55] That section would close a possible loophole which Professor Greenleaf has identified in the New Zealand privacy regime. This loophole refers to the fact that, from the EU perspective, there is nothing specific in the New Zealand legislation to stop data which is imported from Europe being 're-exported' to some other jurisdiction where no adequate privacy protection applies.[56]

Developments in Canada: Until recently, the situation in Canada was that the Federal government and most provinces had legislation governing data protection in the public sector, with the *Federal Privacy Act (1982)* applying to all federal government departments, most federal agencies and some federal Crown Corporations. On the other hand, only the Province of Quebec had adopted comprehensive privacy legislation that extended to the private sector.[57] In the rest of the country, it has been said, data protection in the private

---

53 G Griffith, *Privacy and Data Protection Law Reform: Some Relevant Issues*, NSW Parliamentary Library, Briefing Paper No 15/1996, pp 9-15.

54 M Berthold, 'Hong Kong's Personal Data (Privacy) Ordinance 1995' (December 1995) 2 *Privacy Law and Policy Reporter* 164.

55 The other provisions of the Ordinance came into force on 20 December 1996. Section 33 covers two types of transfers of personal data: (a) transfers from Hong Kong to a place outside Hong Kong; and (b) transfers between two other jurisdictions where the transfer is controlled by a Hong Kong data user: G Greenleaf, 'Hong Kong's model contract clears the way for personal data export restrictions' (April 1997) 4 *Privacy Law and Policy Reporter* 14. For a commentary on section 33 of the Ordinance see - G Greenleaf, 'Personal data export restrictions - their role in developing Asia-Pacific privacy laws', from *The New Privacy Laws*, Communication Law Centre Conference, 19 February 1997, p 119.

56 Ibid, p 120.

57 This was under the 1994 *Act Respecting the Protection of Personal Information in the Private Sector* which grants individuals a right of access to personal information held by private sector businesses operating in Quebec and regulates the collection, use and disclosure of personal information. The legislation is overseen by the Commission on Access to Information which is responsible for conducting investigations and settling disputes -

sector was sporadic and uneven.[58] Protection was supplemented, however, by a voluntary scheme based on recognised 'standards' developed by the Canadian Standards Association. The product of wide consultation, these were formulated in the Model Code for the Protection of Personal Information which was adopted as a National Standard in 1996 by the Standards Council of Canada. This approach provided for an oversight mechanism in the form of auditing and certification for those businesses which comply with the standards which, it is said, 'can be used to marketing advantage and may also assist in facilitating the importation of personal data from EC countries'.[59] On the other side, commenting on the limitations of such a voluntary scheme, the Canadian Government Task Force on Electronic Commerce reported in January 1998:

> Not all business or industry associations have undertaken voluntary measures, and there may be a short-term incentive for some companies to ignore such measures and to use personal information inappropriately. This can undermine fair competition in the marketplace, creating an unlevel playing field. It can also erode consumer confidence in an entire industry and create further confusion about rights and rules.[60]

Following that report, the decision was made at the Federal level to extend the legislative privacy regime to the private sector. For this purpose, on 1 October 1998 the Personal Information Protection and Electronic Documents Bill was introduced, featuring ten information privacy principles and a complaints and remedies mechanism based on the office of the Canadian Privacy Commissioner. Where a dispute remains unresolved ceratin matters can be taken before the Federal Court for resolution. It is proposed that this regime will initially apply to the federally-regulated private sector, including telecommunications, broadcasting, banking and interprovincial transportation, as well as to federal Crown Corporations operating in such areas as the atomic energy industry and the ports. Then, three years after coming into force, the provisions will apply more broadly to all personal information collected, used or disclosed in the course of commercial activities. It is said, too, that where a province adopts legislation that is substantially similar to the Federal Act, then the organisations covered will be exempted from the application of the federal law. As Quebec already has legislation which is substantially similar to the proposed federal regime,

---

http://strategis.ic.gc.ca/sc_mrksv/privacy/engdor/homepage.html

58 Task Force on Electronic Commerce, Industry Canada, Justice Canada, *The Protection of Personal Information - Building Canada's Information Economy and Society*, January 1998, p 5 - http://strategis.ic.gc.ca/privacy

59 M Paterson, 'Privacy protection in Australia: the need for an effective private sector regime' (1998) 26 *Federal Law Review* 371 at 388.

60 Task Force on Electronic Commerce, Industry Canada, Justice Canada, *The Protection of Personal Information - Building Canada's Information Economy and Society*, January 1998, p 7 - http://strategis.ic.gc.ca/privacy

it will be exempted from its application.[61]

The background to these developments is the challenge created for privacy regulation by advances in information technology, as well as the concern that the former arrangements would not meet the standard of 'adequacy' set by the 1995 EU Directive. Of this the Government Task Force commented: 'This Directive has the potential to make the protection of personal information a major non-tariff trade barrier with Canada'.[62]

Developments in the USA:[63] The Canadian approach can be contrasted with its US counterpart where the Clinton Administration has, for the moment at least, opted for the establishment of a self-regulatory privacy regime and is supporting private sector efforts to achieve this outcome. It is reported, however, that the US is keeping its options open, with the July 1997 document, *A Framework for Electronic Commerce*, commenting that if industry cannot achieve effective privacy outcomes, then 'we will reevaluate this policy'.[64] Proposals to regulate privacy in cyberspace in the US are discussed in the last section of this paper.

Developments in the European Union, notably the UK:[65] In the past few years the EU has enacted two directives which will provide citizens with a wider range of protections against abuses of their personal information. One is the 1995 Data Protection Directive which, as noted, seeks to harmonise data protection law throughout the EU. The second is the 1997 Telecommunications Directive which establishes specific provisions covering telephone, digital television, mobile networks and other telecommunications systems.[66] It covers publicly available telecommunications services, including publicly available voice, data, fax and electronic mail. On the other hand, the processing of data in connection with non-publicly available telecommunications services is subject to the Data Protection Directive. With the exception of Article 5 of the Telecommunications Directive, dealing with

---

61 Office of the Minister of Industry, Office of the Minister of Justice and Attorney General of Canada, *Media Release, Canada Moves to Promote E-Commerce: Personal Privacy Protection and Electronic Signatures Recognised in Law* - http://strategis.ic.gc.ca/sc_mrksv/privacy/engdor/homepage.html

62 Task Force on Electronic Commerce, Industry Canada, Justice Canada, *The Protection of Personal Information - Building Canada's Information Economy and Society*, January 1998, p 8 - http://strategis.ic.gc.ca/privacy

63 For a brief overview of privacy law in the USA see - RN Standler, *Privacy Law in America*, http://www.rbs2com/privacy.htm

64 Clinton Administration, *A Framework for Electronic Commerce*, 1 July 1997, at www.ecommerce.gov.

65 Recent developments in privacy law in the UK are discussed in the special issue of *Tolley's Communications Law*, Volume 3, No. 5, 1998.

66 *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector* - http://www.2.echo.lu/legal/en/dataprot/wpdocs/wp11en.htm

confidentiality of communications,[67] both directives came into force on 24 October 1998.

In relation to the Telecommunications Directive, in the UK the Department of Trade and Industry has conducted a consultation process, calling first for comments and then for submissions on draft Regulations by 30 September 1998.[68] The main provisions of these draft Regulations include:

- limitations on the use of traffic and billing data, including for marketing purposes;
- means to enable subscribers to protect their privacy in respect of Calling Line Identification;
- the ability for individual subscribers to opt out from receiving unsolicited direct marketing phone calls; and
- enforcement by the Data Protection Commissioner.

In relation to the Data Protection Directive, in July 1998, only months before it came into force, it was reported that a mere three of the fifteen member states of the European Union had 'Directive compliant' laws in place (Italy, Greece and Sweden). However, another four were said to be imminent, including the UK. In fact, the new UK Data Protection Act received Royal Assent on 16 July, although neither the Act itself nor the secondary legislation required to support it are expected to be brought into force before January 1999. The following points can be made about the UK legislation:

- ***commencement:*** there is a three year transition period for data collectors to bring 'processing already underway' into compliance with the new Act, and data already held in manual filing systems need not comply with many aspects of the new regime until 2007;
- ***application:***the Act will apply to data controllers established in the UK or who use equipment in the UK for processing of data;
- ***data subjects' rights:*** a data controller will have the right to prevent processing for the purposes of direct marketing and, in certain circumstances, to prevent processing likely to cause the individual damage or distress. An individual will have the right to claim compensation where a data controller contravenes the Act. Further, an individual will be able to apply to the courts for correction, blocking, erasure or

---

67 Article 5 does not require implementation until October 2000.

68 For comments on the Directive see - S Dresner, 'EU adopts privacy directive on telecommunications' (January-February 1998) 4 *Privacy Law and Policy Reporter* 143; N Walters, 'EU telecoms privacy Directive - UK implementation' (August 1998) 5 *Privacy Law and Policy Reporter* 59; UK Department of Trade and Industry, *Telecoms Data Protection Directive Implementation in the UK - Draft Regulations*, http://www.dti.gov.uk/CII/tdpd/condoc2.htm

destruction of inaccurate data;

- ***notification:*** data controllers are required to notify the Data Protection Commissioner before processing commences. The broad categories of information to be notified are listed in the Act which does not apply, in this respect, to manual records;

- ***enforcement:*** the Data Protection Commissioner may issue an enforcement notice where a data controller has contravened the data protection principles. An 'information notice' may also be issued requiring the controller to provide information where the Commissioner suspects a principle has been breached;

- ***exemptions:***where the processing is 'in the public interest', personal data processed for journalistic, artistic or literary purposes will be exempt from certain provisions of the Act; and

- ***transfer of data overseas:*** personal data may only be transferred to third countries outside the European Economic Area[69] if those countries ensure an 'adequate level of protection for the rights and freedoms of data subjects'. Commenting on this, the Office of the UK Data Protection Registrar has said that 'It is unlikely that adequate protection to EU standards will be found widely outside the EU and alternative safeguards are being evaluated. The development of model contract clauses to guarantee the protection of personal data is one possibility but the problem of enforcing such a contract to protect the data subject is still being considered'.[70]

The International Chamber of Commerce and model contractual clauses: In fact, by way of response to the need to comply with the EU Data Protection Directive, on 24 September 1998 the International Chamber of Commerce (the ICC) released a report entitled, *Model Clauses for Use in Contracts Involving Transborder Data Flows*.[71] The ICC states that these clauses 'are an appropriate and cost-effective means to fulfil' the need for an 'adequate' level of protection, as required by the EU Directive. In particular, the use of these model clauses is to be discussed with the Member States of the EU for endorsement under Article 26(2) of the Directive which provides:

> ...a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection...where the controller adduces sufficient guarantees with respect to protection of privacy...; such guarantees may in particular result from appropriate contractual clauses.

---

69 This includes Norway, Iceland and Liechtenstein, as well as the 15 EU member states.

70 This commentary is based on the documents, *New Data Protection Act: Preparing for the New Law* and *New Data Protection Law: Implementing the EU Data Protection Directive*, which are found at the Registrar's home page at - http://www.open.gov.uk/dpr/dprhome.htm

71 The full text is at - http://www.iccwbo.org/Commissions/Telecom_IT/Model_clauses.htm

Jay Forder, consultant editor of the journal *Law and Technology*, explains that the 'controller' for the purposes of the model clauses is the 'data exporter' from a European country, while the person in the non-EU country to whom the data is transferred is called the 'data importer'. Forder continues: 'The model clauses are designed to be generic. Their main import is that they require the data importer to observe the laws applicable in the data exporter's jurisdiction...Initially, responsibility for responding to citizens' concerns will rest with the data exporter under the laws of the EU member state'.[72] Thus, as the report states, as in most export control legislation, the person exporting the data is the appropriate party to subject to legal responsibility for export and for preventing violations of data protection by the other (importing) party, an arrangement which is intended to avoid the legal and practical difficulties of data protection authorities trying to regulate parties outside their jurisdiction. Moreover, under this regime a citizen would be able to express his or her concerns to the data exporter in a familiar language and legal system. Further, the model clauses would provide the data exporter with powers and rights to ensure compliance by the data importer, while the data exporter has the right to seek contractual remedies from the data importer in the event of a breach of the data protection laws in the country of export. As Forder warns, 'It goes without saying that an Australian (or other) importer who uses these clauses ought to make quite sure they are familiar with the laws applicable in the country of the exporter!'.[73] The powers and rights granted to the data exporter include:

- requiring the data importer to submit to verification or audit procedures of its processing facilities and information handling;
- requiring submission by the data importer to the jurisdiction of a country's courts for certain relief;
- requiring the data importer to permit the data subject the same rights it would have had against the data exporter in respect of the data prior to its export;
- an indemnity for violations of contractual provisions;
- rights of termination of the clauses if the data importer is in breach of contract; and/or
- return of, or deletion of, the personal data on termination of the relationship for any reason.

Comments: What emerges from this overview of developments in the privacy field in selected jurisdictions is the sheer fluidity of the situation at present. Together, the EU Directives and technological advances have combined to make privacy protection, especially as this relates to the private sector, a hot topic of debate and regulatory concern throughout

---

72 J Forder, 'Avoiding the clash of the titans' (October 1998) *Law and Technology*, Issue 9, pp 6-7.

73 Ibid, p 7.

the world. With respect to personal information in the private sector, the key issue is whether law makers follow the self-regulatory model, as currently preferred in the US and at the federal level in Australia, or whether a co-regulatory/legislative approach is taken, as in New Zealand. Much may depend on what is found to be 'adequate' protection under the EU Data Protection Directive. The immediate response to the long-running privacy debate in NSW is considered in the next section of the paper.

4. THE NEW SOUTH WALES PRIVACY AND PERSONAL INFORMATION ACT 1998

Background: The general background to the present privacy debate in NSW has been discussed in other Parliamentary Library Briefing Papers. It is enough here to say that this State was the first to enact privacy legislation in Australia, with the passing of the *Privacy Committee Act 1975* (NSW). That legislation established the Privacy Committee which has had 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. Since 1982 the Committee had been recommending the introduction of data protection legislation. In the meantime, the problems of the lack of effective legislation to deal with privacy breaches in relation to personal information were sharply illustrated with the exposure (as reported in 1992) by the ICAC of the widespread and corrupt use of personal information held by certain government departments.[74] The ICAC report disclosed a large-scale trade in official information based on an extensive network dubbed the 'Information Exchange Club' and recommended the introduction of uniform, or at least consistent, privacy and data protection laws throughout Australia.[75]

In the light of these and other concerns,[76] the Privacy and Data Protection Bill 1994 was introduced by the then Attorney General, Hon JP Hannaford MLC. The Bill lapsed. However, as noted the cause of privacy protection was taken up by the incoming Attorney General, Hon JW Shaw QC, MLC who foreshadowed the introduction in 1996 of comprehensive privacy and data protection laws for the public and private sectors based, it seemed, on the co-regulatory model favoured in New Zealand in which industry codes of practice are backed up by legislative enforcement. In the event, this foreshadowed legislation was not introduced.

However, a detailed information privacy code of practice was developed at a departmental level by the NSW Health Department, which itself probably foreshadows the kind of code that would operate in the area of public health under a legislative privacy regime. This May 1996 code of practice, which replaced an earlier code issued in 1993, is comprehensive in

---

74 V Mullen, *The Individual's Right to Privacy: Protection of Personal Information in NSW*, NSW Parliamentary Library Briefing Paper No 14/1995, pp 8-10.

75 ICAC, *Report on Unauthorised Release of Government Information*, 1992.

76 Note the concerns about the Computerised Operational Policing System (COPS) expressed in the NSW Ombudsman's Special Report to Parliament, *Improper Access to and use of Confidential Information by the Police*, 14 April 1994.

scope, dealing with such issues as privacy concerns in relation to medical research, health records, access to personal health information by government authorities and data collection. The approach taken in formulating the code was said to be consistent with that taken by the Commonwealth Privacy Act which encourages the development of specific guidelines to govern particular areas of practice.

Privacy and Personal Information Protection Act 1998 - scope: This legislation was introduced into Parliament on 17 September 1998. It does not cover the private sector. Instead, it is directed to the ***State public sector only***. On this key issue the Attorney General stated in the Second Reading Speech:

> This Bill applies information privacy principles only to the public sector at this stage. Whilst the Government remains committed to its pre-election undertaking to develop effective data protection laws which apply to both the private and the public sectors, it has been decided that this should be done in a uniform manner on a national basis.[77]

The Attorney General went on to note developments at the federal level, including the possibility that a national privacy model might be developed to apply to the private sector, presumably self-regulatory in nature. When these matters have been resolved, the Attorney General concluded, 'the present legislation can be amended to apply to the private sector, if that is deemed appropriate at that time'.[78]

For the Opposition, the Shadow Attorney General, Hon JP Hannaford MLC, said if it won office it would follow the model proposed by the Victorian Government, in that it would encourage Federal legislation to cover the private sector, but that, in its absence, a Coalition Government would introduce NSW legislation to ensure privacy protection in the private sector. This legislation would be developed in conjunction with Victoria so as to enure consistency.[79]

Among other things, the Act covers ***local government*** and the ***Police Service*** in NSW, as well as ***government departments***, the ***Education Teaching Service*** and any person or body providing data services for or on behalf of a '***public sector agency***' as defined in section 3 of the Act. A '***public sector official***' is defined to include statutory office holders, judicial officers, public servants, teachers, the police, local government councillors and employees, as well as officers and employees of the Legislative Council and Legislative Assembly. The term does not appear to extend to those engaged as consultants to a public sector agency.

After considerable debate, ***the Act does not cover State owned corporations***. A successful amendment was in fact moved by the Opposition in the Legislative Council which had the effect of including such corporations under the new privacy regime. On that occasion the

---

77 *NSWPD* (Hansard Proof, LC), 17 September 1998, p 41.

78 Ibid.

79 *NSWPD* (Hansard Proof, LC), 14 October 1998, pp 28-29.

Shadow Attorney General stated: 'The principle that the Opposition advocates is that privacy should apply to a government agency unless it is exempted...A State-owned corporation is a government agency that has been corporatised to drive efficiencies within that agency. Adherence to privacy principles should not affect efficiency.'[80] However, this amendment was itself successfully challenged and overturned in the Legislative Assembly, with the Hon PFP Whelan MP arguing that the inclusion of State owned corporations under the privacy regime would place them 'at a competitive disadvantage with the private sector'; to this he added, 'The Government has taken the view that State owned corporations should only be covered by privacy legislation when the private sector is similarly covered'.[81] The Legislative Assembly amendment was agreed to by the Legislative Council on 25 November 1998.[82] For its part, however, the Opposition remained convinced of the need to include State owned corporations under the privacy legislation, with the Shadow Attorney General commenting: 'It is interesting to reflect that when the Independent Commission Against Corruption investigated breaches of privacy by government agencies selling private information, what have become State owned corporations were amongst the worst offenders. The water board and electricity agencies were amongst the worst offenders'.[83] The point is made that 'Some of the State's largest public sector authorities, including State Rail, Sydney Water and the electricity distributors, will be exempt from having to comply with new laws supposedly designed to protect the privacy of people dealing with Government bodies'.[84] The Hon AA Tink MP concluded that, as a result of this and other exemptions, 'the bill will become a Clayton's privacy legislation'.[85]

Privacy and Personal Information Protection Act 1998 - structure and content: The structure of the NSW Act is familiar enough. Part 2 is headed 'Information protection principles'(IPPs) and it sets out 12 principles of the kind found in most privacy legislation, including the Federal and New Zealand Privacy Acts, all of which are based on the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The Act refers to specific exemptions from these IPPS, for law enforcement and other agencies. Part 3 then provides for the making of privacy codes and management plans, which would permit certain other sectors, such as health, to modify the IPPs or to apply for total exemption from their operation. Part 4 establishes the office of the NSW Privacy Commissioner and sets out the relevant complaints mechanism. Next, Part 5 which is headed 'Review of certain conduct' establishes the enforcement provisions. Public registers are dealt

---

80 *NSWPD* (Hansard Proof, LC), 28 October 1998, p 62. The Bill, as amended, did not make explicit mention of State owned corporations, but these would have been defined as public sector agencies as they are required under the *State Owned Corporations Act 1989* to be audited by the Auditor-General.

81 *NSWPD* (Hansard Proof, LA), 18 November 1998, p 110.

82 *NSWPD* (Hansard Proof, LC), 25 November 1998, p 81.

83 Ibid, p 48.

84 LM Garcia, 'State bodies to escape privacy laws', *The Sydney Morning Herald*, 21 November 1998.

85 Ibid.

with separately in Part 6 of the Act, while Parts 7 and 8 cover the Privacy Advisory Committee and miscellaneous matters respectively.

One comment, made by Professor Graham Greenleaf, on the legislation in the form that it was first introduced into Parliament was that it was 'structurally sound...It only requires excision of its too-smart-by-half bureaucratic protection "features" to provide reasonable privacy protection in the public sector'[86] - this being a reference to the legislation's exemption provisions.

Information protection principles: The Act is based on the application of information protection principles to public sector agencies. The Act also allows for modifications to and exemptions from these IPPs. These principles, which are set out in sections 8 to 19 of the Act, deal with the following:

- *1.Collection of personal information for lawful purposes.*
- *2.Collection of personal information directly from the individual.*
- *3.Requirements when collecting personal information*, which relate to such things as the need to give notice to the individual that information is being collected, the purpose of the collection, the intended recipients and the details of any rights of access or correction that may apply.
- *4.Other requirements relating to collection of personal information*, which stipulates that the information must be relevant to the purpose for which it is collected, and that the collection itself does not intrude unreasonably on the individual's personal affairs.
- *5. Retention and security of personal information*, which includes the requirement that the information is kept for no longer than is necessary for the purposes for which it may be lawfully used, and that the information must be disposed of securely.
- *6. Information about personal information held by agencies*, which requires a public sector agency to take reasonable steps to ensure that individuals can find out if the agency holds information about them and, if so, what is its nature, why was it collected and how may it be accessed.
- *7. Access to personal information held by agencies*, which ensures a right of access to the individual.
- *8. Alteration of personal information*, which requires a public sector agency to permit an individual to check the accuracy and relevance of information and, if the information is amended, the individual must be notified if reasonably practicable.

---

86 G Greenleaf, 'NSW not up with the times on privacy', *The Australian Financial Review*, 2 October 1998.

- *9. Agency must check accuracy of personal information before use.*

- *10. Limits on use of personal information*, which restricts the use of information to the purpose for which it was collected. Certain exceptions apply, for example, where an individual consents to use of the information for some other purpose, or where such use would prevent or lessen serious or imminent harm to the individual concerned.

- *11. Limits on disclosure of personal information*, which basically restricts disclosure to certain circumstances, for example, where the public sector agency believes disclosure would prevent or lessen serious or imminent harm to the individual concerned. Further, if the information is disclosed to a public sector agency, that agency must not use or disclose the information for a purpose other than that for which the information was given to it.

- *12 . Special restrictions on disclosure of personal information*, the first subsection to which refers to the prohibition against disclosure of information relating to such things as an individual's ethnic origin or political opinions unless disclosure is necessary to prevent serious or imminent harm to the person. The second subsection relates to restrictions on ***transborder data flows***. It was inserted as a result of an amendment moved by the Hon I Cohen MLC for the Greens who explained its rationale in these terms: 'In order to ensure that the transfer of personal data to New South Wales is not prevented by the European Directive, the Hong Kong legislation or possibly the new Victorian Act, new subclauses are needed to prevent disclosure of personal information to organisations that are not subject to similar privacy protections as those found in the New South Wales Act or do not otherwise provide sufficient guarantees of privacy protection'.[87] Actual privacy legislation is not required in another jurisdiction to permit flow of data from NSW. Instead, the new Privacy Commissioner is to specify in a code of practice what types of contracts, industry codes of conduct and other protections will qualify as a 'relevant privacy law' for the purpose of the subsection.

Principles 1-4 above only apply to personal information collected after the privacy legislation is in force. On the other hand, the remaining principles are to apply to information already held by public sector agencies.

Personal information: These IPPs apply to what the Act calls personal information, a term which is defined to mean 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.[88] Such information is said to include 'such things as an individual's fingerprints,

---

87 *NSWPD* (Hansard Proof, LC), 28 October 1998, pp 66-67.

88 Section 4 (1).

retina prints, body samples or genetic characteristics'.[89] The Act then lists what is not personal information and therefore is not protected by the IPPs. In addition to excluding information about someone who has been dead more than 30 years and information in a publicly available publication, the list of exclusions also includes:

- information about individuals under the witness protection scheme, presumably on the basis that restrictions of data gathering may endanger the witness in question; and information about an individual arising out of a warrant issued under the Federal *Telecommunications (Interception) Act 1979*, presumably because, in such circumstances, by definition information is gathered covertly;

- information about an individual arising out of a Royal Commission or Special Commission of Inquiry, presumably in response to such considerations as the urgency and public importance attached to the work of such bodies, as well as their extensive powers and their temporary nature. In fact, a later section provides that ***courts, tribunals and Royal Commissions*** are not affected by the new privacy legislation, thereby quarantining the powers and functions of such bodies from the reach of the IPPs;[90]

- information about an individual arising out of a complaint about the conduct of a police officer under Part 8A of the *Police Service Act 1990*, the rationale for which was not explained in the Second Reading Speech but presumably it relates to the requirements of efficient investigation;

- information or an opinion about an individual's suitability for appointment or employment as a public servant. In other words, government departments would be able to share information about the employment suitability of an individual;

- and information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations.

Privacy and the Freedom of Information Act: Section 5 of the Privacy and Personal Information Protection Act defines the relationship between itself and the *Freedom of Information Act 1989* by stating the latter is not affected by the former. Thus, the requirements of open government established under the FOI regime are not affected by the introduction of privacy legislation. Section 20 (5) of the privacy legislation also makes reference to the FOI Act, stating that certain information protection principles *(Information about personal information held by agencies*; *Access to personal information held by agencies*; and *Alteration of personal information*) do not affect any relevant conditions or limitations found under the FOI Act.[91] This has been interpreted to mean that the privacy

89 Section 4 (2).

90 Section 6.

91 Note, too, that the Office of the Privacy Commissioner is made an exempt body under the FOI Act.

and FOI regimes will remain consistent, 'but the extra protections provided by the IPPs will apply'.[92]

A general point to make is that there is considerable overlap between privacy and FOI legislation, particularly where access and correction rights are concerned. It is also the case that conflict can also arise between the two regimes, notably where an FOI request includes a document that contains the personal information of someone other than the applicant. It can be noted that this potential for conflict is modified by the inclusion in the FOI regime of an exemption for 'Documents affecting personal affairs' which provides: 'A document is an exempt document if it contains matter the disclosure of which would involve the unreasonable disclosure of information concerning the personal affairs of any person (whether living or deceased).'[93] However, the term 'personal affairs' is not defined, which raises the question as to whether it is to be interpreted in a way that is consistent with the term 'personal information' under the privacy legislation. Also, the prohibition is only against 'unreasonable' disclosure, which leaves unresolved the question of when information concerning personal affairs would be released to a third party.

The 'personal affairs' exemption in the New South Wales FOI legislation is similar to that found in section 41 of the Federal *Freedom if Information Act 1982*. One difference is that the Federal Act refers instead to 'personal information' and this is defined in a way that is consistent with the Federal Privacy Act.

Note that, in a major review of the Federal FOI Act, the Australian Law Reform Commission and the Administrative Review Council recommended that section 41 of the Federal FOI Act be redrafted to provide that a document is exempt if: (a) it contains personal information; (b) its disclosure would constitute a breach of IPP 11 of the Federal Privacy Act - *Limits on disclosure of personal information;* and (c) its disclosure would not, on balance, be in the public interest.[94] In fact, in the discussion paper for the report it was suggested that the relationship between the FOI Act and the Privacy Act has always tended to be 'glossed over' and the recommendation was made that in the medium to long term there was a need to rationalise current legislation dealing with government information practices by the creation of a single information Act covering FOI, archive and privacy matters.[95] The report itself rejected the single information Act proposal on the basis that

---

92 G Greenleaf, 'NSW privacy bill passes Legislative Council' (September /October 1998) 5 *Privacy Law and Policy Reporter* 69 at 70.

93 Schedule 1, clause 6 (1), *FOI Act 1989* (NSW). It provides, too, that 'A document is not an exempt document by virtue of this clause merely because it contains information concerning the person by or on whose behalf an application for access to the document is being made'.

94 ALRC and Administrative Review Council, *Report No 77 - Open Government: A Review of the Federal Freedom of Information Act 1982*, 1995, p 128. Public sector agencies would determine whether information falls within section 41, with the assistance of guidelines issued by the FOI Commissioner after consultation with the Privacy Commissioner.

95 ALRC and Administrative Review Council, *Discussion Paper 59 - Freedom of Information*, May 1995, p 130.

each separate piece of legislation in force at present has a distinct purpose that is 'understood by the bureaucracy and, to some degree, by the community'. The problem of applying a single information Act across the board to the public and private sectors was also discussed. 'Nevertheless', the report concluded, the ALRC and the Administrative Review Council remained 'strongly of the view that the connections between these Acts must be clearly understood and appreciated by those subject to them and by those who oversee their administration'.[96] It can be argued that the conclusion is relevant to any jurisdiction which has separate privacy and FOI legislation.[97]

Exemptions: In the form that it was first introduced into the NSW Parliament, the privacy legislation was heavily criticised in some quarters, particularly for the scope of the exemptions it allowed under sections 22-28. Professor Greenleaf commented that the relevant Bill was a 'travesty even in relation to the public sector: it contains pages of exemptions which have been found unnecessary in the Federal Privacy Act for the past 10 years; it allows exemption by ministerial regulation at so many key points it looks like Swiss cheese...'.[98] Further, Mr Chris Puplick, the head of the privacy Committee and the man reportedly nominated to become the first NSW Privacy Commissioner, is said to have commented that the Bill as first introduced 'had too many exemptions and is out of step with international standards'; he was said to be particularly concerned that the Bill had 'generous exemptions' for the NSW police and other investigative agencies, as well as about provisions that 'largely exempt' information gathered about people seeking employment in the public service.[99] In the event, the amendments moved by the Greens to this part of the legislation were defeated,[100] with the result that the exemptions regime remains substantially in tact.[101] The exemptions include:

- Law enforcement and other public sector agencies are exempted from compliance with specific IPPs where the information concerned was collected for law enforcement purposes. For example, a public sector agency is not required to comply with the principle embodied in section 9 *(Collection of personal information*

---

96 ALRC and Administrative Review Council, *Report No 77 - Open Government: A Review of the Federal Freedom of Information Act 1982*, 1995, p 49.

97 Note, too, that the FOI Act is amended to include the Office of the Privacy Commissioner in the list of exempt bodies and offices in Schedule 2.

98 G Greenleaf, 'NSW not up with the times on privacy', *The Australian Financial Review*, 2 October 1998; G Greenleaf, 'NSW privacy bill passes Legislative Council' (September /October 1998) 5 *Privacy Law and Policy Reporter* 69 at 71.

99 C Meritt, 'Privacy head attacks proposed laws', *The Australian Financial Review*, 25 September 1998.

100 *NSWPD* (Hansard Proof, LC), 28 October 1998, p 68. The proposed amendment would have allowed for a one-year exemption for ICAC, the Police Service, the Police Integrity Commission and the NSW Crimes Commission which would have allowed time for a code of practice to be drawn up for them.

101 The Government moved a successful amendment to section 25, inserting a reference to the *State Records Act 1998* in the exemption regime.

directly from individual) if the information concerned is collected in connection with proceedings before any court or tribunal.[102]

- Similarly, specific exemptions are made for investigative agencies. For example, such agencies need not comply with the principle (embodied in section 12 (a)) that personal information must be kept for no longer than is necessary for the purposes for which the information may be lawfully used.[103]

- Except for the exercise of their administrative and educative functions, the ICAC, the Police Service, the Police Integrity Commission and the NSW Crime Commission are all specifically exempted from the privacy regime.[104]

- The Ombudsman's Office, the Health Care Complaints Commission, the Anti-Discrimination Board, the Guardianship Board and the Community Service Commission are not required to comply with the IPP embodied in section 19 (*Special restrictions on disclosure of personal information*). The disclosure of health related information is also exempted in certain circumstances.[105]

Note, too, that information, or a class of documents, may be exempted by regulation from the definition of 'personal information;[106] similarly, a person or body can be declared to be an 'investigative agency' and therefore exempted from the privacy regime.[107] Professor Greenleaf has commented in this regard that the legislation 'contains provisions which allow the Minister to repeal it in instalments, by regulations or by codes'.[108]

Privacy codes of practice and management plans: A code of practice can modify the application of the IPPs to a public sector agency or, indeed, further to an amendment moved by the Government, a code may exempt altogether a public sector agency (or class of agency) from the requirement to comply with any IPP.[109] A public sector agency must consult with the Privacy Commissioner about a draft code before it is submitted to the Minister (the Attorney General). The Commissioner may, in turn, make submissions concerning the draft code to the Minister who, on his or her discretion, may then decide to establish the code. Once in place, a public sector agency must comply with a relevant

---

102 Section 23.

103 Section 24.

104 Section 27.

105 Section 28.

106 Section 4 (3) (k).

107 Section 3.

108 G Greenleaf, 'NSW privacy bill passes Legislative Council' (September /October 1998) 5 *Privacy Law and Policy Reporter* 69 at 70.

109 Sections 20 (2) and 30.

privacy code. Breach of a code may result in the application of the enforcement provisions under Part 5 of the Act.

With the approval of the Minster, the Privacy Commissioner may make a written direction that a public sector agency is not required to comply with either an IPP or a code of practice.[110] In fact, under an amendment which was moved successfully by the Opposition in the Legislative Council, the Privacy Commissioner was granted greater power over codes of practice, notably a power to ensure that a code can only exempt a public sector agency from compliance with an IPP if '***the Privacy Commissioner is satisfied that the public interest in allowing the exemption outweighs the public interest in the agency complying with the principle***' (emphasis added). The effect of this would have been to place the Privacy Commissioner, not the Attorney General, in a position where he or she could veto any proposed code. Introducing this amendment, the Shadow Attorney General argued that this provision (along with the remainder of section 29 (7)) would provide that the IPPs would operate as the 'benchmark' against which any privacy code of practice might be developed, an approach which was said to be consistent with privacy legislation in New Zealand, Hong Kong and the United Kingdom.[111] In New Zealand it is the Privacy Commissioner who has the power to issue a code of practice free, it seems, from Ministerial intervention in the process;[112] it is the IPPs which form the benchmark against which the code is made; and, while there is no general public interest test as such, the 'public interest' is one criteria by which specific exemptions permitting a breach of certain IPPs are to be decided.[113] Note, too, that the Commonwealth *Privacy Act 1988* permits the Privacy Commissioner to make 'public interest determinations' where he or she is satisfied that: (a) an act or practice of an agency breaches, or may breach, an Information Privacy Principle; and (b) 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.

In the event, this 'public interest' aspect of the Opposition amendment which had been agreed to by the Legislative Council was subsequently overturned by the Legislative Assembly. Moving the amendment for the Government, the Hon PFP Whelan MP argued that the Privacy Commissioner's 'power of veto' over a code of practice on public interest grounds 'is not appropriate'. The Minister continued:

> Whilst the Privacy Commissioner has a role in initiating the preparation of privacy codes and in advising the Minister when the Minister is considering making a privacy code, it is not for the Privacy Commissioner to veto a code. In the end it is for the Minister, properly advised, to determine

110 Section 41.

111 *NSWPD* (Hansard Proof, LC), 28 October 1998, p 70.

112 Section 46, *Privacy Act 1993* (NZ).

113 Section 54, *Privacy Act 1993* (NZ).

whether a code should be made.[114]

The Government prevailed, with the effect that the NSW Privacy Commissioner is to have less control over the making and issuing of codes of practice than is the case in certain other privacy regimes. In NSW a code of practice is to be made by an order of the Attorney General in the Government Gazette.[115]

Under section 29 (6) a code must provide standards of privacy protection which protect NSW public agencies against import restrictions, a provision which, according to Graham Greenleaf, 'should mean that any codes must be "adequate" in terms of the EU Directive'.[116]

Each public sector agency is directed to prepare and implement a privacy management plan within 12 months of the commencement of section 33 of the Act.

Public registers: Disclosure of personal information held on a public register is restricted to a purpose consistent with the purpose of the register itself. To achieve this, a statutory declaration may be required from a person wishing to inspect personal information contained on a register. A person may also request that the information be removed from, or not placed on, the register as publicly available, or that it not be disclosed to the public.[117]

Privacy and the State Records Act 1998: When it was first introduced into Parliament concerns were raised by the NSW History Council, the Professional Historians' Association and others that the privacy legislation would in effect be a 'straightjacket' for historians by cutting off their access to many valuable documents.[118] An editorial in *The Sydney Morning Herald* stated that the legislation should 'allow for the important rights of professional historians and other academics to have access to publicly held information about private individuals for the purpose of legitimate research'.[119] Dr Shirley Fitzgerald offered the example that historians would no longer be able to 'search health records to build a picture of the state of health in NSW at a particular time because the information had not been gathered with that in mind'.[120]

Responding to these concerns, the Government introduced amendments designed to 'clarify'

---

114 *NSWPD* (Hansard Proof, LA),18 November 1998, p 112.

115 Section 31 (5).

116 G Greenleaf, 'NSW privacy bill passes Legislative Council' (September /October 1998) 5 *Privacy Law and Policy Reporter* 69 at 70.

117 Section 57 and 58.

118 D Jopson, 'Historians refuse to wear "straightjacket" privacy law', *The Sydney Morning Herald*, 23 September 1998.

119 Editorial, 'Private and public rights', *The Sydney Morning Herald*, 28 September 1998.

120 D Jopson, 'Historians refuse to wear "straightjacket" privacy law', *The Sydney Morning Herald*, 23 September 1998.

the relationship between the privacy regime and the *State Records Act 1998*. 'The amendments', the Attorney General said, 'have been included to address concerns raised by the State Archives Authority and the History Council, both of which support these amendments'.[121] These included an insertion into section 25 of the privacy legislation of an explicit reference to the fact that compliance with the IPPs is not required if non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under the *State Records Act 1998* (or indeed any other Act). Section 29 was amended to provide that the protection of information that is more than 30 years old under a code of practice must be consistent with any guidelines under section 52 of the *State Records Act 1998*.

The Privacy Commissioner and the complaints process: One function of the Privacy Commissioner is to receive and, where appropriate after a preliminary assessment, resolve privacy complaints by conciliation. The procedures for conciliation are to be determined by the Commissioner who may then report his or her finding or recommendations concerning the complaint to the complainant, as well as to other persons or bodies 'materially involved in matters concerning the complaint'.[122] The Privacy Commissioner has no enforcement powers.

As originally introduced into Parliament, the legislation would have precluded a complainant from first having a complaint dealt with by the Commissioner by means of conciliation and, afterwards, seeking a remedy through the Administrative Decisions Tribunal. In other words, once the matter had been reported upon by the Commissioner that would have been an end to it. In this way, the original Bill provided two separate procedures for complaint handling: the conciliation approach; and the request that a public sector agency conduct an internal review, followed by an appeal to the Administrative Decisions Tribunal where the complainant remained unsatisfied. In its amended form, however, these two procedures are combined so that, even after conciliation by the Privacy Commissioner, a complainant may still seek an internal review and have a right of appeal to the Administrative Decisions Tribunal. Without this amendment, Graham Greenleaf has said that the legislation would have been 'worthless'.[123]

The Administrative Decisions Tribunal and the complaints process: Thus, where a public sector agency has contravened an IPP, a code of practice or has disclosed personal information kept in a public register, a complainant may seek an internal review of the relevant conduct. At the request of the agency, such a review may be undertaken by the Privacy Commissioner who must, in any event, be notified when an application for review is received by an agency. If the applicant is not satisfied with the review, either because of its findings or the action taken as a result of these, then an appeal can be made to the Administrative Decisions Tribunal. A number of courses are open to the Tribunal which may make one or more orders, including: the payment of damages by the agency not exceeding

---

121 *NSWPD* (Hansard Proof, LC), 28 October 1998, pp 64-65.

122 Section 50.

123 G Greenleaf, 'NSW privacy bill passes Legislative Council' (September /October 1998) 5 *Privacy Law and Policy Reporter* 69 at 70.

$40,000; the correction of personal information which has been disclosed; and the performance of an IPP or privacy code of practice.[124] An order may only be made if the conduct of the agency has caused financial loss, or psychological or physical harm.[125] Any order or decision of the Tribunal may be appealed to an Appeal Panel of the Tribunal.[126]

Note that the power to make orders under section 55 (2) only relates to conduct occurring 12 months after the commencement of Division 1 of Part 2, which sets out the IPPs.[127]

Commencement: It would seem from the above that those procedures relating to the Administrative Decisions Tribunal only come into force one year after the IPPs have been in operation. However, it appears that conduct which is complained about and is only subject to conciliation by the Privacy Commissioner need not satisfy this 12 month rule; that part of the Act would come into force concurrently with the IPPs. So, it seems, would the provisions relating to criminal offences under the Act.

Corrupt disclosure by public sector officials: The Act also imposes criminal sanctions against public servants who intentionally disclose or use personal information about other persons 'to which the official has or had access in the exercise of his or her official functions'. A person who induces a public servant to act this corrupt way would also commit a criminal offence.[128] These and other criminal offences under the Act are to be dealt with summarily before a single Magistrate of the Local Court.[129]

Privacy and whistleblowers: Another area of concern when the privacy legislation was first introduced related to its impact on protected disclosures by public servants, with an editorial comment in *The Sydney Morning Herald* stating that the Government should concede that privacy law 'is unbalanced if it does not also protect disclosure by whistleblowers of information which is in the public interest'.[130] In response, the Government moved an amendment to clarify the point that the prohibition against corrupt disclosure in section 62 'does not prohibit a public sector official from disclosing any personal information about another person if the disclosure is made in accordance with the *Protected Disclosure s Act 1994*'.

5. THE WORKPLACE VIDEO SURVEILLANCE ACT 1998

---

124 Section 55 (2).

125 Section 55 (4) (b).

126 Section 56.

127 Section 55 (4) (a).

128 Section 62. There is a maximum penalty of two years imprisonment.

129 Section 70. Other offences include the wilful obstruction of the Privacy Commissioner (section 68).

130 Editorial, 'Private and public rights', *The Sydney Morning Herald*, 28 September 1998.

Background: The issues in the debate concerning workplace video surveillance have been discussed in previous briefing papers.[131] It is enough to note here that, prior to the *Workplace Video Surveillance Act 1998* there was no legislation directly governing either covert or overt electronic visual surveillance in NSW.[132] This contrasts with the laws in Austria, Germany, Norway and Sweden, to cite one international survey, under which employers are obliged to seek agreement with workers on such matters.[133] The form of surveillance at issue here typically involves observation of a target, primarily through the use of cameras, closed circuit television or video cameras.

In an attempt to fill the regulatory vacuum in NSW, if only in part, in September 1995 the Privacy Committee published *Guidelines on Overt Video Surveillance in the Workplace*. Then in July 1997 the NSW Department of Industrial Relations published a *Voluntary Code of Practice for the use of Overt Video Surveillance in the Workplace*. That there was a need for legislation, however, in this increasingly controversial area was confirmed in the report of the Working Party on video surveillance which was delivered to the Attorney General in December 1996.[134] That report, in turn, formed the basis of the 1998 Act.[135]

The Workplace Video Surveillance Act 1998: The Act's purpose is to regulate the covert video surveillance of employees in the workplace by their employers. When introducing the legislation into Parliament the Attorney General said this was an 'industrial issue of great importance', noting that 'A number of major industrial disputes have arisen over video surveillance by employers'. To this the Attorney General added that the legislation:

> strikes a balance between the competing interests of different parties. The privacy of employees is important in the workplace. Workers should be able to undertake their duties with as little interference as possible to their privacy...On the other hand, employers should have the opportunity to

---

131 G Griffith, *Privacy and Data Protection Law Reform: Some Relevant Issues*, NSW Parliamentary Library, Briefing Paper No 15/1996, pp 26-28; R Simpson, *Listening Devices and Other Forms of Surveillance: Issues and Proposals for Reform*, NSW Parliamentary Library Briefing Paper No 20/1997, p 4, 10 and 15.

132 But where the equipment used could also be characterised as a listening device (that is, as a form of aural surveillance), in which case it would be governed by the *Listening Devices Act 1984.* Note that section 6 of the *Industrial Relations Act 1996* (NSW) includes the 'surveillance of employees in the workplace' in the definition of an 'industrial matter', but that this does not make it illegal to use surveillance devices in the workplace. Note, too, that section 65 of the *Casino Control Act 1995* (NSW) makes it a condition of a casino license being granted that the NSW Casino Control Authority approve plans including those for the monitoring of casino operations, which may include the operation of closed circuit television cameras.

133 Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, http://www.gilc.org/privacy/survey/intro.htm

134 NSW Department of Industrial Relations, *The Working Party on Video Surveillance in the Workplace*, December 1996.

135 *NSWPD*, 26 May 1998, p 5087.

investigate serious problems in the workplace.[136]

The key features of the Act are as follows:

- It ***regulates only covert surveillance*** and, for this purpose, it distinguishes between covert and overt video surveillance. It creates a presumption that all video surveillance is covert unless three stipulated conditions are fulfilled. These are : first, that employees have been notified in writing of the intended use of surveillance at least 14 days before it occurs (or less than 14 days if the employee agrees); the cameras or any equipment used for surveillance are clearly visible in the relevant part of the workplace; and there must be clearly visible signs to notify people that they may be under video surveillance. Video surveillance for a purpose other than the surveillance of the activities of employees in the workplace is not covert surveillance if it is in accordance with an agreement with an employee. Such an agreement must be made by a body representing a substantial number of the employees.[137]

- It prohibits all covert video surveillance of employees in the workplace unless it is done ***for the sole purpose of finding out if an employee is participating in any unlawful activity in the workplace***.

- Covert surveillance must also be authorised by what is called a '***covert surveillance authority***' which is to be issued by a Magistrate.[138] Such an authorisation will not remain in force more than 30 days.[139] It cannot be used to check work performance or for monitoring toilet areas, showers, change rooms or bathing facilities.[140] An application for an authorisation must include certain information, including the grounds for suspecting that an employee(s) is involved in unlawful activity in the workplace.

- A Magistrate must not issue a covert surveillance authority without considering whether it might 'unduly intrude' on the ***privacy*** of the employee(s) concerned or any other person.

The legislation has been the subject of some comment and criticism, especially from the security industry. For example, John Woolfe, partner at Alexander Woolfe Solicitors, specialists in security industry law, has said that 'The definitions can easily become foggy'. He explains that the Act is only supposed to restrict *workplace* surveillance, but he offers

---

136 *NSWPD*, 26 May 1998, pp 5087-5088.

137 Section 4.

138 This imposition of a function on a magistrate is not a conferral of jurisdiction on the Local Court; Magistrates will hear applications under the Act as persona designata - section 24; *NSWPD*, 26 May 1998, p 5091.

139 Section 16.

140 Section 9 (3).

the example that State Rail is in the process of planning a multi-million dollar security re-vamp of Sydney train lines to protect the travelling public. But what about SRA staff? Isn't a railway station their place of work?'.[141] Woolfe is also reported to have said that the Act would limit use of video surveillance to such an extent that in some cases it could not be employed as evidence in a court. The example he offers is as follows: 'Suppose you gain an "authorisation" to monitor an employee who you thought was stealing from the workplace. But whilst monitoring him, the cameras pick up another employee who is dealing drugs. Under the new Act, this evidence may be inadmissible in court because there was no authority for you to monitor the second employee's conduct'.[142] Further, it is argued by Woolfe that authorisation cannot be given retrospectively, which means that if cameras pick up a worker acting illegally, the footage may not be admissible because no authority for the employer to monitor that particular employee had been obtained before the offence was committed.[143]

On the other side, it was reported in September 1998 that civil liberties and privacy groups 'condemned Australian companies' unbridled video surveillance of employees and the public, after a business survey showing 56 per cent of companies used video monitoring'.[144] The Price-Waterhouse Coopers business survey of 65 of Australia's top 100 companies showed that covert electronic monitoring was conducted by a significant minority, with around '12 per cent failing to notify employees that their activities were being monitored'. Although video surveillance was used mainly for external security, 22 per cent of companies used it to monitor the internal movements of employees and 1 per cent for time and motion studies.[145]

In any event, as at 26 November 1998 the *Workplace Video Surveillance Act 1998* had not been proclaimed to commence.

6. TECHNOLOGY AND THE INVASION OF PRIVACY - FURTHER ISSUES IN THE DEBATE

The invasion of privacy by various technological devices is by no means restricted to covert video surveillance in the workplace. Without attempting to offer an exhaustive account of what is an increasingly diverse field of debate, two further issues can be noted, namely, the surveillance of e-mail communications in the workplace and the implications of Internet communication generally for the protection of privacy.

---

141 B Love, 'Watch who you watch: new legislation could leave NSW CCTVs blind!', *Security Australia*, November 1998, p 4.

142 Ibid.

143 Ibid.

144 L Lamont, 'Privacy worry over bosses' video eye on workers', *The Sydney Morning Herald*, 10 September 1998.

145 S Long and S Beer, 'Big brother is watching at a workplace near you', *The Australian Financial Review*, 10 September 1998.

E-mail communications in the workplace: This issue has been the cause of some debate in NSW in recent months with the NSW Labor Council calling in October 1998 for the Government to regulate the interception of E-mail communications in the workplace. At present there is no such regulation. Mr Michael Costa, President of the NSW Labor Council is reported to have said that, while there should not be an 'unfettered use' of E-mail by employees, some regulation is needed to protect workers; also, companies should be required to explain their standards and practices to their employees.[146] It is said in this context that:

> E-mail surveillance is now common in Australian companies, with computer programs available that can search internal electronic mail for four-letter words or the names and nicknames of senior personnel...One software package - Remotely Possible, made by US company Avlan - lets managers secretly watch every keystroke and read every message that you send - as you send it. And it's not just internal E-mails that can be monitored. E-mails sent through a third party provider, like Hotmail, can also be easily tapped into. It's a fine line between Big Brother watching you, and an employer's right to check up on their workers.[147]

The Daily Telegraph report goes on to explain that both the ANZ and Westpac banks monitor their workers E-mail, although Westpac only does it when it is investigating a specific complaint. Mr Paul Edwards, ANZ's head of group media relations, stated that the bank kept E-mail records for security reasons, as well as 'for internal correspondence related to customers and other employees'. Mr Edwards continued, 'The bank would not use it for, say, monitoring union activities...It's much more related to looking at harassment or use of the system for inappropriate material, sexual or any other sort'.[148] Responding directly to the views of the NSW Labor Council, the Executive Director of the NSW Employers Federation, Mr Garry Brack, reportedly stated that employers have every right to control what their employees are doing: 'Costa uses the term eavesdrop which suggests some heinous crime by the employer...This is not a question of eavesdropping, it's a question of trying to make sure the business functions...Let him identify the specifics and paint for us a picture of what he believes is acceptable and unacceptable rather than dreaming up colourful language that tries to portray employers as some kind of pariahs'.[149]

It is reported that a spokesman for the Hon JW Shaw MLC, Attorney General and Minister for Industrial Relations, said the Minister supported the call for monitoring regulations, stating: 'In principle we agree with the call that there be a clear understanding and a policy should be in place so that employees and employers have agreed guidelines on privacy

---

146 A Harvey, 'When e-mail is an open letter', *The Daily Telegraph*, 9 October 1998.

147 Ibid.

148 Ibid.

149 'Employers "pariahs" on staff privacy', *The Illawarra Mercury*, 10 October 1998.

issues'.[150] The spokesman also noted that the issue would be dealt with by the NSW Law Reform Commission in its forthcoming report on surveillance.

As with all privacy issues, the interception of E-mail communications in the workplace is a more or less universal phenomenon. Certainly, the question has been addressed in the US, with the production in 1996 by the American Employment Law Council of a major report on *Electronic Interaction in the Workplace*. That report discussed the relevant US case law as it stood at that time, including the finding that there is no reasonable expectation of privacy in E-mail communications voluntarily made to a supervisor over a company-wide E-mail system, and this was in spite of the fact that the employer assured the employee that E-mail messages would not be intercepted by management.[151] The main concerns of the report, which was written by an employer body, were with such things as: potential liability for monitoring employees' E-mail use; potential liability for employee conduct on an E-mail system; and the right of unions to access company employees via E-mail. The report concluded that 'One way to manage the many risks and hazards presented by e-mail and the Internet is to maintain a formal policy that addresses these problems and establishes clear ground rules for the use of e-mail and the Internet'.[152]

A Canadian report which covers similar ground, albeit from a rather different standpoint, is the Ontario Information and Privacy Commissioner's *Privacy Protection Principles for Electronic Mail Systems*. The Commissioner has in fact developed the following seven principles to heighten awareness of the privacy issues associated with the use of E-mail: (a) the privacy of E-mail users should be respected and protected; (b) organisations should create an explicit policy to address the privacy of E-mail users; (c) organisations should make their E-mail policy known to users and inform users of their rights and obligations regarding the confidentiality of messages on the system; (d) users should receive proper training about security/privacy issues related to the use of e-mail; (e) e-mail systems should not be used for the purposes of collecting, using and disclosing personal information, without adequate safeguards to protect privacy; (f) providers of e-mail systems should explore technical means to protect privacy; and (g) organisations should develop appropriate security procedures to protect e-mail messages.[153]

Privacy in cyberspace: A window onto the many challenges posed by the Internet for the protection of privacy is gained from a recent article by the Hon Justice Michael Kirby. He writes:

---

150 Ibid.

151 *Smyth v The Pillsbury Co*, 914 F Supp 97 (ED Pa 1996).

152 The American Employment Law Council, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, http://www.mlb.com/speech1.htm

153 The Information and Privacy Protection Commissioner /Ontario, *Privacy Protection Principles for Electronic Mail*, http://www.ipc.on.ca/web_site.eng/matters/practice/email.htm

> Some of the chief protections for privacy in the past arose from the sheer costs of retrieving personal information; the impermanency of the forms in which that information was stored; and the inconvenience experienced in procuring access...Other protections for privacy arose from the incompatibility of collections with available indexes and the effective undiscoverability of most personal data. These practical safeguards for privacy largely disappear in the digital age. A vast amount of data, identified to a particular individual, can now be collated by the determined investigator. The individual then assumes a virtual existence which lives in cyberspace instead of in what in what is sometimes described as 'meat space'. The individual takes on a digital persona made up of a collection of otherwise unconnected and previously unconnectable data.[154]

Some might consider this a pessimistic view of cyberspace and its opportunities, as something of a technological dystopia. Nonetheless, there seems to be general agreement that the Internet has the potential to raise almost as many problems for privacy as opportunities for communication. Justice Kirby went on to say that, in the light of

technological change and the enhanced capacity of the Internet, informed writers are suggesting that new privacy principles are needed, including:

- ***a right not to be indexed*** - that is, a right not to have an Internet page 'indexed' by such search engines as Yahoo!, Alta Vista and WebCrawler. This means that the page will not be disclosed to an inquirer when a search is conducted. At present a 'rogue' robot indexer may override a clear instruction not to index an Internet page, as a result of which personal information may be revealed against a person's express wishes.[155]

- ***a right to encrypt personal communications effectively*** - this means that a message is scrambled so that only the intended recipient will be able to unscramble and subsequently read its content. For example, Pretty Good Privacy (PGP) is said to be the best known encryption program; it has over 100,000 users including human rights groups such as Amnesty International.[156] An issue discussed in the report, *Internet Commerce: To Buy or Not to Buy?*, is that the ability of individuals to use powerful encryption systems to protect personal privacy 'may be in conflict with

---

154 M Kirby, 'Privacy in cyberspace' (1998) 21 *University of NSW Law Journal* 323 at 325.

155 As Graham Greenleaf explains, Internet-wide search engines such as Alta Vista use robots to trawl the Internet, creating complete word occurrence indexes of every page and every item posted to every news group that the robot is allowed to access. This means it is possible to search for occurrences of a name or phrase occurring anywhere in the text of any web page, or in any News posting - G Greenleaf, 'An endnote on regulating cyberspace: architecture vs law? (1998) 21 *University of NSW Law Journal* 593 at 615.

156 Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, http://www.gilc.org/privacy/survey/intro.htm

> community needs'. It is said that 'the community expects adequate and effective law enforcement, national security and the requirement that individuals and organisations pay the appropriate amount of taxation'.[157]

On the same theme, it can be added that in Australia the 'anonymity' principle has been making progress towards becoming a legal requirement of cyberspace regulation.[158] It has its origin, locally, in Principle 10 of the Australian Privacy Charter - 'People should have the

option of not identifying themselves when entering transactions'. Tim Dixon explains that the principle holds that people 'should only be required to identify themselves in transactions when there is a substantial public interest reasons why an individual should be identified'. As ever complexities and tensions emerge in the operation of such a principle, with Dixon stating that 'The right to anonymity strengthens the protection of free speech, although it may of course also widen the scope for defamatory comments and hate speech'. Exceptions to the principle would also be required, including in relation to an 'ongoing relationship between an individual and an organisation and which involve a significant level of risk, such as the provision of credit, or air travel'.[159]

The whole debate about privacy in cyberspace is connected to developments in the field of electronic commerce, about which there is an ever-growing body of analysis and comment; added to which governments and governmental organisations are eager to develop appropriate regulatory principles and practices.

For example, in the US the Clinton administration, in its the July 1997 document, *A Framework for Electronic Commerce*, stated:

> If privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more

---

157 The Parliament of the Commonwealth of Australia, Joint Committee of Public Accounts and Audit, *Report 360 - Internet Commerce: To Buy or Not to Buy?*, May 1998, pp 187-191. The 1998 Report of the Electronic Commerce Expert Group to the Federal Attorney General was also discussed, the conclusion of which was that a 'detailed legislative regime for electronic signatures needs to be considered with caution'. The Expert Group pointed out that there is no international uniform approach, and legislative approaches may not have due regard for market-oriented solutions. The Expert Group recommended that legislation 'Should deal simply with the legal effect of electronic signatures' - Report of the Electronic Commerce Expert Group to the Attorney General, *Electronic Commerce: Building the Legal Framework*, March 1998, p ii.

158 G Greenleaf, 'An endnote on regulating cyberspace: architecture vs law? (1998) 21 *University of NSW Law Journal* 593 at 609.

159 T Dixon, 'Telecommunications privacy' (January/February 1997) 4 *Telecommunications Law and Policy Review* 121 at 135.

> direct role in safeguarding consumer choice regarding privacy online.[160]

In an interesting development, in its report of June 1998, *Privacy Online: A Report to Congress*, the US Federal Trade Commission found that industry association guidelines, while encouraging members to provide notice of their information practices, 'fail to provide for access and security or for enforcement mechanisms'. The report continued:

> The Commission also examined the practices of commercial sites on the World Wide Web. The Commission's survey of over 1,400 Web sites reveals that industry's efforts to encourage voluntary adoption of the most basic fair information practice principle - notice - have fallen far short of what is needed to protect consumers. The Commission's survey shows that the vast majority of Web sites - upward of 85% - collect personal information from consumers. Few of these sites - only 14% in the Commission's random sample of commercial Web sites - provide any notice with respect to their information practices, and fewer still - approximately 2% - provide notice by means of a comprehensive privacy policy.[161]

A particular area of concern for the Commission was the collection of information from children, with very few sites taking any steps 'to provide for meaningful parental involvement in the process'. To counter this, the Commission recommended that Congress develop legislation placing parents in control of the online collection and use of personal information from their children'.[162] More generally, the Commission referred to the need for 'substantially greater incentives' to spur self-regulation and to ensure the widespread implementation of basic privacy principles in the online industry. It concluded:

> The development of the online marketplace is at a critical juncture. If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential. To date, industry has had only limited success in implementing fair information practices and adopting self-regulatory regimes with respect to the online collection, use, and dissemination of personal information. Accordingly, the Commission now recommends legislation to protect children online and this summer will

---

160 Clinton Administration, *A Framework for Electronic Commerce*, 1 July 1997, at www.ecommerce.gov. This is discussed in The Parliament of the Commonwealth of Australia, Joint Committee of Public Accounts and Audit, *Report 360 - Internet Commerce: To Buy or Not to Buy?*, May 1998, p 196.

161 The report is reproduced in Senate Legal and Constitutional References Committee, *Inquiry Into Privacy and the Private Sector*, Volume 7, pp 1177-1247. The references used here are from the executive summary at pages 1181-1184. The report can also be found at - http://www.ftc.gov

162 In September 1998 the Federal Trade Commission Chairman, Robert Pitofsky, testified before the US Senate Subcommittee on Communications supporting the Children's Online Privacy Protection Act of 1998 - Federal Trade Commission, *Media Release*, 'FCT testifies in support of federal legislation protecting children's online privacy', 23 September 1998.

> recommend an appropriate response to protect the privacy of all online consumers.[163]

The Federal Trade Commission's report was one of the studies submitted to the US Department of Commerce's inquiry into privacy, following its January 1998 paper, *Elements of Effective Self-regulation for Protection of Privacy*, which appears to be the focal point of the Clinton Administration's response to the EU Directive. The Department of Commerce's report is itself part of a larger report on electronic commerce.

On 7-9 October 1998 Ministers from OECD countries, including Australia, met in Ottawa to discuss regulation of the Internet and electronic commerce at a conference entitled, 'A Borderless World: Realising the Potential of Global Electronic Commerce'. This resulted in a series of declarations relating to specific regulatory issues, including the protection of privacy on global networks. Among other things, the Ministers said they would: ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress; encourage the use of privacy enhancing technologies; and encourage the use of contractual solutions and the development of model contractual solutions for online transborder data flows.[164]

Nearer home, confidentiality and privacy issues are also addressed in the second discussion paper released by the Victorian Treasurer in July 1998, *Promoting Electronic Business: Electronic Commerce Framework Bill*. Electronic commerce refers, typically, to communications between computers by the electronic processing and transmission of data. Many issues arise in this context, including the requirement of holding parties to contracts submitted electronically, for example, where a person subscribes to a journal or purchases a book using electronic means. There is, in addition, an obvious need to ensure that such data is only accessed by those authorised to do so. However, the discussion paper noted that, as these privacy concerns do 'not fit comfortably within the electronic commerce framework', they are best left to separate legislation dealing specifically with privacy and data protection.[165]

Again, it remains to be seen whether Victoria does in fact introduce its own electronic commerce regime. The situation is complicated by the fact that on 30 July 1998 the Federal Attorney General announced that legislation for electronic commerce would be introduced by the Commonwealth. This would be in the form of a uniform Commonwealth model law to be enacted by all Australian jurisdictions with the cooperation of the States and Territories. It is to be based on the model Law on Electronic Commerce developed by the

---

163 Ibid, p 1184.

164 C Connolly, 'OECD conference on electronic commerce' (1998) 1 *Internet Law Bulletin* 101-104.

165 *Discussion Paper: promoting Electronic Business: Electronic Commerce Framework Bill*, July 1998, p 14 at http://www.mmv.vic.gov.au/

UN Commission on International Trade Law.[166]

7. CONCLUSIONS

Privacy regulation world-wide is in a state of transition. In NSW there has been some movement, in the form of legislation to protect personal information that is stored and collected by the public sector, as well as in relation to the *Workplace Video Surveillance Act 1998*. It has been noted that the latter has yet to be proclaimed to commence, while the former has been the subject of considerable critical debate.

The next big issue that awaits this and many other jurisdictions is the regulation of privacy in the private sector and the question as to whether a self-regulatory or co-regulatory/legislative model is to be preferred. The one area of general agreement in the privacy debate in Australia relates to the need to avoid a patchwork of privacy regimes for the private sector in the States and Territories.

There are also the many and varied privacy issues associated with developments in electronic communications, all of which raise complex problems of a technical and legal nature, many of which are international in scope and nature.

166 Federal Attorney General, *Media Release*, 'Legal framework for electronic commerce', 30 July 1998.