UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 1 *Journal of Computer & Information Law - Fall 2000*

Article 3

Fall 2000

Recent Developments in Private Sector Personal Data Protection in Australia: Will There Be an Upside Down Under, 19 J. Marshall J. Computer & Info. L. 71 (2000)

Paul Kelly

RECENT DEVELOPMENTS IN PRIVATE-SECTOR PERSONAL DATA PROTECTION IN AUSTRALIA: WILL THERE BE AN UPSIDE DOWN UNDER?

by PAUL KELLY†

A. INTRODUCTION

Writing almost two decades ago, the pioneering and preeminent German privacy advocate Herbert Burkert observed that:

> [a]lthough the United States was one of the first countries to enact data protection laws, many Americans today view European data protection regulations with concern and even distrust. There is growing concern that European regulations would be impractical, bureaucratic, and detrimental to the free flow of information. . . . [O]ne reason for American concern seems to be that European laws have some features that are unfamiliar to the American data protection approach. These features include [inter alia] the implementation of data protection agencies . . .[1]

Very little seems to have changed over the past 20 years. Notwithstanding that "[n]early [50] countries now have comprehensive data protection or information privacy laws or are in the process of adopting

† L.L.B. (Syd) Professor, School of Law & Justice, Southern Cross University, Lismore, New South Wales, Australia and a Visiting Academic at The Centre for Information Technology and Privacy Law at The John Marshall Law School, January to April 2000. The author wishes to acknowledge the assistance of Dr. Lee Bygrave of the Faculty of Law, University of Oslo; Mr. Peter Coroneos of the Internet Industry Association, Australia; and Prof. Brian Fitzgerald of Southern Cross University, Australia, for their assistance in the preparation of this article.

1. Herbert Burkert, *Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data Protection Laws,* 3 Computer/Law Journal 167, 168-69 (1981) (citing McGuire, *The Information Age: An Introduction to Transborder Data Flow,* 20 Jurimetrics J. 1 (1979-80), and Bigelow, *Transborder Data Flow Barriers, id.* at 8 in support of these views).

them"[2] and that the "overwhelming majority" of countries with data protection laws have established special authorities to specifically oversee their implementation, the U.S. and Japan stand out as "notable exceptions."[3]

B. PERSONAL DATA PROTECTION IN EUROPE

Traditionally speaking, European data protection laws have generally been stricter, more comprehensive[4] and more bureaucratic[5] than their non-European counterparts.[6] However, this will not necessarily continue to be the case in the future.

It is theoretically possible that change could eventually come about through increased public awareness and understanding of technological processes or through information-gathering systems becoming totally transparent. After evaluating the rationale and functions of the more 'typical' European-style data protection agencies, Burkert for example optimistically concluded that:

> [o]ne can envision . . . a time when these specialised institutions of information control may become obsolete, when general awareness of the value problems of information and communication technology will have been achieved, when public and private users alike will have made their systems sufficiently open, and when the individual or any group of individuals will feel sufficiently confident and equipped to participate in communication no matter how complex the technology may be.[7]

---

2. David Banisar and Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. Marshall J. of Computer & Info. L. 1, 4 (1999).

3. Lee J. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, 94 (unpublished thesis submitted for degree of Doctor Juris, Univ. of Oslo, 1999) (copy on file with *John Marshall Center for Information Technology and Privacy Law*).

4. In many European countries the same comprehensive law applies to both the government and private sectors. *See* Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* 7 (Brookings Institution Press, 1998).

5. Most, for example, require that record keepers either: (1) notify data protection authorities before data processing operations are commenced (often through a formal registration procedure under which authorities are supplied with basic details of intended processing operations); or (2) apply for, and obtain, specific authorisation from the data protection authority (usually in the form of a licence issued subject to compliance with various conditions) prior to establishing a personal data register or commencing processing operations. *See* Bygrave, *supra* n. 3, at 100-01.

6. Bygrave, *supra* n. 3, at 112-113, summarizes numerous differences between the data protection laws of different jurisdictions in terms of their ambit and the monitoring and supervisory regimes they establish as to some extent constituting "a cleavage line between European and non-European . . . regimes, with the former offering generally more comprehensive and stringent safeguards than the latter, but the line is far from clean."

7. Burkert, *supra* n. 1, at 188. In Burkert's view, the "European approach" to data protection in general, and the establishment of data protection agencies in particular, can

Of more current relevance, the wider impacts of the European Union Data Protection Directive[8] ("EU Directive") which came into force on October 24, 1998, have yet to be fully felt outside Western Europe. But as part of the early international response newer so-called "light-touch" legislation-based regimes, referred to as "co-regulatory models," have been introduced (or are in the course of being adopted) to regulate private-sector personal-data protection in several non-European jurisdictions including New Zealand, Canada and Australia. These newer approaches are regarded by some countries as providing an acceptable compromise between the full regulatory models traditionally favoured throughout Western Europe, and the "hands-off" self-regulatory approaches which have been preferred by governments in countries such as the U.S.A.,[9] and also until recently in Australia.

C. PERSONAL DATA PROTECTION IN AUSTRALIA

In many respects, Australia and the U.S. have a great deal in common in the area of personal data protection. Perhaps this should not be surprising – the two countries share similar legal systems, similar market-based economies, and similar concerns for upholding the rule of law

---

be seen as a product of governmental attempts to provide regulatory mechanisms which achieve a balance between society's need to adapt to technological change so as to realise its benefits on the one hand, and the need for technology to adapt to the basic values of society so as to ensure social coherence in a changing environment on the other. He suggests that most data protection problems merely reflect classic "old" societal conflicts such as distribution of power between, for example, individual (or groups of individuals) and state, and that public caution and distrust results in part from a general lack of public understanding of new technologies and the "language of power" that accompanies them, which he argues is most likely also connected with past abuses of information and communication power in Europe. He submits that this in turn has made legislators more cautious and more inclined to delegate policy making, decision making and control functions relating to new information technology – all functions traditionally within the province of the legislature, executive and judiciary – to specialised agencies rather than leaving them to these traditional institutions.

8. *Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,* Official Journal No L 281, 23/11/1995, 31 <http://www.privacy.gov.au/publications/pg2pubs.html#28> (accessed Oct. 4, 2000) (hereinafter EU Directive). For a very brief description of the Directive's aims and effects, *see infra* n. 77.

9. Yet another alternative – which proposes the establishment of a specialised authority but seemingly without supervisory powers – has recently been advocated for the U.S. by Swire and Litan. They recommend the formation of an "Office of Electronic Commerce and Privacy Policy" as a "more structured institutional home within the U.S. government to consider issues arising from the private sector use of personal information," but propose that the Office would facilitate a system of self-regulation and "would make and coordinate policy with respect to privacy and electronic commerce but would not be a regulatory or enforcement agency." Swire & Litan, *supra* n. 4, at 178-79.

and for protecting commonly-held "fundamental" moral and political values such as liberty, justice, autonomy and personal privacy.

At the basic legal level, for example, both countries have federal systems of government under which specific law making powers are vested in the federal or "national" legislatures, with residual law making powers belonging to the legislatures of their constituent states.[10] Neither country's Constitution contains any express provision relating to privacy.[11] Both are liberal democratic societies whose citizens share a healthy distrust – even dislike – of "big government" and excessive government power. Both countries have embraced new information technologies[12] but have also recognised the "rise of the computer state"[13] as posing a threat to individual privacy, giving governments the potential to abuse the increasing amounts of personal information that they collect on their constituents, partly to facilitate delivery of the services and programs which those constituents expect them to provide. And both have, as a consequence of this recognition, passed legislation at a federal level during the past 20 years to protect the privacy of personal information collected and used by their public sector agencies.[14]

---

10. Contrast the position in Canada, for example, which also has a federal system but under which specific legislative powers are vested in the provincial (equivalent to state) parliaments, with the residue of such powers being vested in the dominion or "national" parliament.

11. *See generally* Commonwealth of Austl. Const. Act 1900 (U.K.) <http://scaleplus.law.gov.au/html/pasteact/1/641/top.htm> (accessed Oct. 4, 2000); U.S. Const. amend. V.

12. The National Office for the Information Economy, *The Current State of Play – July 2000,* 13 <http://www.noie.gov.au/projects/information_economy/ecommerce_analysis/ie_stats/StateOfPlay/index.htm> (accessed Oct. 4, 2000) (Australia 2000) reports that Australians rank among the top 5 nations in the world in terms of accessing the Internet, whether measured in terms of percentages of households or of adult population connected. In the year to February 2000, an estimated 43% of adult Australians accessed the Internet, placing it only marginally behind the United States (45%) in the group of leading nations, according to survey data produced by the Australian Bureau of Statistics; *8147.0 - Use of the Internet by Householders,* #8147.0, May 2000 <http://www.abs.gov.au/Ausstats/ABS%40.nsf/b06660592430724fca2568b5007b8619/ae8e67619446db22ca2568a9001393f8!OpenDocument> (accessed Oct. 4, 2000) and *NUA Internet Surveys,* April 2000 http://www.nua.ie/surveys/how_many_online/index.html (accessed Oct. 4, 2000). The same report puts Australia as 12th in the world in terms of mobile phone penetration, with the U.S. at 16th, according to the Organisation for Economic Cooperation and Development ("OECD"), *Cellular Mobile Pricing Structures and Trends,* 14 (May 2000).

13. David Burnham, *The Rise of the Computer State,* (Random House 1983), *cited in* Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* 30 (Cornell Univ. Press 1992).

14. In Australia, Privacy Act 1988 (Cth) <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/> (accessed Sept. 4, 2000); and in the United States, Privacy Act of 1974, 5 U.S.C. § 552a (1974) <http://www.epic.org/laws/privacy_act.html> (accessed Oct. 4, 2000). The need to regulate to protect information privacy – particularly from the activities of government – arose in Australia from a major controversy that was generated by an unsuccessful attempt to introduce a national identity card ('The Australia Card'). It has been

Until very recently, both countries have also adhered to policies favouring self-regulatory regimes as the basis for personal data protection in their private sectors – with the exception, that is, of certain industry-specific legislation covering (again, in many cases common) areas such as financial and consumer credit records,[15] and personal information and related data held by telecommunications companies and carriers.[16]

But whereas Australia has for many years had a special federal agency responsible for administering its information privacy laws,[17] the U.S. has yet to establish such an institution.[18] The limited role which has been played by the U.S. Office of Management and Budget ("OMB") in relation to the U.S. Privacy Act[19] to date is generally regarded by privacy commentators as having "not been particularly active or effective."[20] As Bennett has claimed, the OMB:

> has not interpreted this role in a positive and active manner; it has issued few guidelines to help federal agencies apply the act; it has exhibited a weak and declining interest in submitting the annual report that the President is expected to provide to Congress each year; and it has adopted a very passive and reactive stance with regard to oversight.[21]

---

suggested that "The [U.S.] Privacy Act would not have been passed in 1974 had it not been for Watergate." Bennett, *supra* n. 13, at 72.

15. In Australia: the Privacy Act 1998 (Cth) <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/> (accessed Jan. 14, 2001); in the U.S.: the Right to Financial Privacy Act, 29 U.S.C. § 304 (1986), and the Fair Credit Reporting Act, 15 U.S.C. § 1681 (1996) <http://www.epic.org/privacy/financial/fcra.html> (accessed Jan. 14, 2001).

16. In Australia: Telecommunications Act 1987 (Cth) <http://scaleplus.law.gov.au/html/pasteact/2/3021/top.htm> (accessed Oct. 4, 2000); in the U.S.: Cable TV Privacy Act of 1984, 47 U.S.C. § 551 (Oct. 30, 1984) *available at* <http://www.epic.org/privacy/cable_tv/ctpa.html> (accessed October 4, 2000), and Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394, 2395,2401,2402 (codified as amended in scattered sections of 47 U.S.L.).

17. The Office of the Federal Privacy Commissioner (formerly the Office of the Privacy Commissioner), established under Privacy Act 1988 (Cth), Part IV.

18. David Banisar notes that "An office within the Office of Management and Budget to coordinate federal stances towards privacy was created in early 1999, and a Chief Counselor for Privacy was appointed. The Counselor has only a limited advisory capacity and most privacy advocates believe the position is ineffective in promoting privacy within the government." *Privacy & Human Rights 2000,* Privacy International, London, U.K., 2000 <http://www.privacynternational.org/survey/phr2000/countriesru.html#Heading10> (accessed Sept. 24, 2000).

19. Section 6 of the Act provides that "the Office of Management and Budget shall – (1) develop guidelines and regulations for the use of agencies . . . and (2) provide continuing assistance to and oversight of the implementation of the provisions." Privacy Act of 1974 (1974) <http://www.epic.org/laws/privacy_act.html> (accessed Oct. 4, 2000).

20. Banisar & Davies, *supra* n. 2, at 109.

21. Bennett, *supra* n. 13, at 176, *citing* U.S. House of Representatives, *Who Cares about Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress,* Report by the Committee on Government Operations, House

And whereas the Australian Government has recently reversed its former policy stance and decided to implement one of these newer "co-regulatory" regimes for its business sector,[22] the U.S. Administration has so far continued to maintain its self-regulatory policy in spite of persistent criticisms by privacy groups,[23] evidence of increasing consumer concerns[24] and mounting business[25] and even government support for change.[26]

Against the background of these similarities and differences, this article traces the history of recent policy shifts from self-regulation to co-regulation that have occurred in Australia; outlines the co-regulatory regime that is currently being implemented for the protection of personal data in the Australian private sector; and explains the rather limited role of Australia's data protection agency – the "Office of the Federal Privacy Commissioner" – within the proposed new regime. Before doing so however, the existing role, powers and administrative structure of the Privacy Commissioner's Office are briefly described. The new private sector scheme has been designed to fit around and be supported by the existing legal and administrative framework to a certain degree, so a basic understanding of the existing system is required.

---

of Representatives, 98th Congress, 1st sess. (Washington, D.C.: Government Printing Office, 1983).

22. Privacy Amendment (Private Sector) Bill 2000 <http://www.aph.gov.au/legis.htm> (accessed Oct. 4, 2000) (currently before the Australian Federal Parliament).

23. The Washington, D.C.-based U.S. Electronic Privacy Information Center ("EPIC") has been among the most persistent and the most vocal in this regard, *see, e.g.* Martin Stone, *Online Privacy Advocates Take Case to Capitol Hill,* E-Commerce Times, June 13, 2000 <http://www.ecommercetimes.com/news/articles2000/000613-nb2.shtml> (accessed June 15, 2000), as well as the various reports, government submissions and media releases accessible via the EPIC Web site at <http://www.epic.org> (accessed Oct. 4, 2000) and through the Electronic Frontier Foundation at <http://www.eff.org/pub/Privacy> (accessed Oct. 4, 2000).

24. *See e.g.* Matt Beer, *64% of Web Users Don't Trust Sites,* San Francisco Examiner, Aug. 17, 1999, <http://www.sfgate.com/cgi-bin/article.cgi?f=/Examiner/archive/1999/08/17/BUSINESS9371.dtl&type=PRintable> (accessed Sept. 28, 2000).

25. *See e.g.* Information Technology Association of America, *Survey Indicates Authentication Concerns Growing as Key Barrier to E-Commerce,* Press Release, March 31, 1999 <http://www.itaa.org/news/pr/pr19990331.htm> (accessed Sept. 28, 2000).

26. In a shift from its traditional position, the Federal Trade Commission recommended to the U.S. Congress that legislation is necessary to protect consumer privacy on the Internet, based on the findings of a survey of online privacy policies. *See Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* May 2000 <http://www.ftc.gov/os/2000/05/index.htm#22> (accessed Oct. 4, 2000). *See also* On-line Privacy and Disclosure Bill (HR 4059 IH); 999 Cong US HR 4059, 106th Congress, 2d Session, introduced Mar. 21, 2000; *Some in Congress Say U.S. Government Could Use an Information-Privacy Czar,* The Wall Street Journal Interactive Edition, <http://interactive.wsj.com/archive/retrieve.cgi?id=SB966811382463874405.djm> (Aug. 22, 2000) (regarding a Republican Bill to create a federal "Office of Information Policy" to coordinate information protection among federal agencies).

D. AUSTRALIA – PUBLIC SECTOR (EXISTING)

As already noted above, Australia has a federal system in which law-making power is shared between the Federal (or "Commonwealth") Government and the governments of its 6 states and 3 self-governing territories.[27]

The sole piece of privacy legislation that currently exists at the state level is limited in its application to state and local government instrumentalities,[28] and the major instrument regulating information privacy in Australia is the federal Privacy Act 1988. The Act as presently in force applies mainly to federal government departments and agencies and applies to the private sector (and to state and local governments) only in relation to tax file numbers and consumer credit information. Other Australian federal laws also cover specific categories of personal information such as telecommunications records,[29] information collected from health insurance claims,[30] records of certain old (generally more than 10 years) criminal convictions of a minor nature[31] and the use of personal records for data-matching operations between the Australian Taxation Office and other federal assistance agencies to detect overpayments and ineligibility for government assistance and understatement of income.[32]

The Privacy Act is based around 11 Information Privacy Principles ("IPPs")[33] that must be complied with by federal government agencies.[34]

---

27. A further 7 Commonwealth territories have not yet been given self-governing powers and are still subject to Commonwealth laws. A third tier of government, known as "local government" and comparable to U.S. county government, also exists within most Australian states but is a creation of the various state legislatures and has no recognition in the Australian Constitution (Commonwealth of Australia Constitution Act 1900 (U.K.)).

28. New South Wales, the most populous State, has only recently introduced the Privacy and Personal Information Protection Act 1998 (NSW) which came into effect on July 1, 2000.

29. Telecommunications Act 1987 (Cth) <http://scaleplus.law.gov.au/html/pasteact/2/3021/top.htm> (accessed Oct. 4, 2000).

30. National Health Act 1953 (Cth) <http://scaleplus.law.gov.au/html/pasteact/0/173/top.htm> (accessed Oct. 4, 2000).

31. Crimes Act 1914 (Cth) <http://scaleplus.law.gov.au/html/pasteact/0/28/top.htm> (accessed Oct. 4, 2000).

32. Data-matching Program (Assistance and Tax) Act 1990 (Cth) <http://scaleplus.law.gov.au/html/pasteact/0/445/top.htm> (accessed Oct. 4, 2000).

33. Privacy Act 1988 (Cth) § 14 <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/> (accessed Sept. 4, 2000). The IPPs are based on the Organisation for Economic Cooperation and Development, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980 ("OECD Guidelines") <http://www.privacy.gov.au/publications/pg2pubs.html#27> (accessed Oct. 4, 2000), and cover the collection, storage, use and disclosure of personal information. They also include provisions enabling individuals to access and correct their personal information records. *Id.*

34. Privacy Act 1988 (Cth) c 16 <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/> (accessed Sept. 4, 2000).

It also creates an independent Office of the Privacy Commissioner[35] and gives the Commissioner a wide range of statutory functions in relation to interferences with privacy including, *inter alia*: resolving complaints;[36] investigating breaches of the Act; examining proposed legislation that might interfere with individuals' privacy; researching and monitoring developments in data processing and computer technology; auditing agencies for compliance; providing policy advice; and promoting awareness of the IPPs so as to encourage adoption and acceptance of privacy standards more broadly in the community.[37]

Powers available to the Commissioner in conducting investigations and performing other functions under the Act include powers to obtain information and documents;[38] to examine witnesses on oath;[39] to require parties to attend compulsory conferences;[40] and the power to enter premises.[41]

Although the Act gives the Commissioner power to make formal determinations following the investigation of complaints,[42] including declarations requiring respondents to perform certain acts or to pay compensation to redress any loss or damage[43] suffered by complainants,[44] the approach favoured by the Commissioner is to resolve complaints by conciliation and negotiation between the parties wherever possible.[45] Any formal determinations that are made by the Commissioner are enforceable by either the Commissioner or the complainant through the Federal Court.[46]

---

35. Id. at § 19.

36. Id. at §§ 36, 38A-38C, 52.

37. Id. at § 27.

38. Id. at § 44.

39. Id. at § 45.

40. Privacy Act 1988 (Cth) § 46 <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/> (accessed Sept. 4, 2000).

41. Id. at § 68.

42. Id. at § 52.

43. Defined to include "injury to the complainant's feelings or humiliation suffered by the complainant." *Id.* § 52(1A).

44. *Id.* at § 52(1)(b)(ii) – (iii).

45. Office of the Federal Privacy Commissioner, *Eleventh Annual Report on the Operation of the Privacy Act for the Period 1 July 1998 – 30 June 1999,* 53, available at <http://www.privacy.gov.au/pdf/99annrep.pdf> (accessed Oct. 4, 2000) (hereinafter *Annual Report*).

46. Privacy Act 1988 (Cth) §§ 55, 62 <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/> (accessed Sept. 4, 2000).

E. OFFICE OF THE PRIVACY COMMISSIONER – ADMINISTRATIVE STRUCTURE

The Privacy Commissioner's Office is divided into 4 main sections,[47] each of which deals with different functions of the Commissioner. They are:

- A Policy Section which provides policy advice on privacy issues in response to requests from Government Ministers, Federal Government agencies and the private sector. This section also examines proposed legislation for privacy implications and conducts research into technological and social developments that affect individual privacy;[48]
- A Promotion and Education Section, which provides training and publishes information about privacy issues, including a Web site that provides comprehensive information about the Commissioner's Office and about Australian and international privacy laws.[49] Another important role of this Section is the operation of a telephone Privacy Hotline Service[50] that provides general advice to individuals concerning their rights under the Act and related legislation, assists them in making complaints if required and also handles media requests for information on privacy-related matters;[51]
- A Complaints and Compliance Section, which investigates complaints from individuals about interferences with privacy; conducts audits of the personal information-handling practices of government agencies and other organisations (such as telecommunications companies) covered by the Act; and monitors the conduct of government data-matching programs;[52] and
- An IT Standards Section, which handles data-matching issues and privacy advice in relation to information technology and electronic commerce.[53] An important recent initiative of this Section has been the preparation and publication in 1999 of Guidelines for Federal and ACT Government World Wide Web sites,[54] the purpose of which are "to assist agencies to adopt the best privacy practice and comply with the Privacy Act in respect to their [W]eb sites."[55]

---

47. *Annual Report*, *supra* n. 45, at 112.

48. Office of the Federal Privacy Commissioner, *About the Privacy Commissioner* <http://www.privacy.gov.au/about/index.html> (accessed Sept. 4, 2000).

49. *See generally* Privacy Commissioner's web site <http://www.privacy.gov.au> (accessed Sept. 4, 2000).

50. The Privacy Hotline is also accessible by post, fax or e-mail (privacy@hreoc.gov.au).

51. *Annual Report*, *supra* n. 45, at 43-4 & 49

52. Office of the Federal Privacy Commissioner, *About the Privacy Commissioner*, <http://www.privacy.gov.au/about/index.html> (accessed Sept. 4, 2000).

53. *Annual Report*, *supra* n. 45, at 75. *Id.* at 111 (Appendix 6: Finance and Administration; and Office of the Federal Privacy Commissioner).

54. *1999 Guidelines for Federal and ACT Government World Wide Websites* <http://www.privacy.gov.au/publications/pg2pubs.html#16.1> (accessed Oct. 4, 2000).

55. *Annual Report*, *supra* n. 45, at 103.

F. AUSTRALIA – PRIVATE SECTOR (PROPOSED)

The approach to privacy protection in the Australian private sector has been particularly volatile over recent years, with at least two policy turnarounds by the current (conservative) Liberal/National Coalition Government and at least one by the former Labor Government (the current Opposition).

It was a Labor government that was responsible for the passing of the Privacy Act 1988. At the time that legislation was before the Parliament, the minority Australian Democrats Party had sought to introduce its own bill to extend the Act to the private sector but did not have the numbers and was unable to win the necessary support from the major parties (Labor and the Liberal/National Coalition), all of which were at that time opposed to such a measure.

During the first half of the 1990s, support for comprehensive private sector protection grew gradually across the political spectrum, as reflected in the recommendations and reports of a number of public bodies.[56] A survey of Australian businesses released in 1996 revealed that by that time some 64% of Australian businesses favoured such a course.[57]

In September 1996, the Australian Attorney General's Department released a discussion paper[58] which outlined "a possible co-regulatory approach to extending the Privacy Act to the private sector"[59] and honoured the Coalition Government's 1996 election policy that it would "as a priority, and in consultation and development with the states and territories, ensure the implementation of a privacy law regime in Australia comparable with best international practice."[60]

In March 1997 however, the Prime Minister suddenly announced that his Government "will not be implementing privacy legislation for

---

56. Moira Paterson, *Privacy Protection in Australia: The Need for an Effective Private Sector Regime,* 26 Fed. L. Rev. 1 <http://law.anu.edu.au/publications/flr/vol26no2/Patters.htm#P-1_0 (accessed Sept. 29, 2000).

57. Price Waterhouse, *Privacy Survey 1996,* (Sydney 1996). The survey disclosed that 32% of businesses surveyed believed that the best way to address the issue of information privacy was a Privacy Act that regulated both the public and private sectors, while another 32% favoured the option of a national Privacy Act with industry-specific codes similar to the recently introduced New Zealand Act. Paterson, *supra* n. 56.

58. Hon. Daryl Williams AM QC MP, Attorney General and Minister for Justice, *Privacy Protection in the Private Sector,* News Release, Canberra, 1996.

59. Hon. Daryl Williams AM QC MP, Attorney General and Minister for Justice, *New Privacy Commissioner,* News Release, Canberra, 1996 <http://www.law.gov.au/aghome/agnews/1996news/19123.htm> (accessed Nov. 17, 2000).

60. *Liberal and National Parties' Law and Justice Policy,* February 1996, reproduced in 3 Privacy Law and Policy Reporter 4 (1996) <http://www.austlii.edu.au/au/other/plpr/vol3/vol3No01/v03n01b.html#3_PLPR_4> (accessed Feb. 7, 2001).

the private sector"[61] and that he had also asked the State and Territory governments not to enact such legislation, referring to "the need to reduce the regulatory burden" and concerns about the compliance costs which a legislation-based scheme would impose on business.[62]

Several months after the Prime Minister's announcement, in August 1997, the then-Privacy Commissioner Moira Scollay released a "consultation paper" which proposed the formulation of a single national *voluntary* code as "a viable self-regulatory option . . . designed to be compatible with existing Commonwealth privacy laws and any further legislation which might be considered necessary in particular sectors, States or Territories."[63] From the discussions that followed the release of that paper, the Commissioner realised that national consistency in privacy standards was a key issue for business and consumers alike.[64] It also became clear to her that while the content of the principles that would form the basis of any national scheme would be contentious enough, other issues such as implementation and compliance mechanisms would be even harder to resolve.[65] She accordingly "decided to start with the development of principles and then move on to the implementation issues."[66]

The first draft of the Commissioner's *National Principles for the Fair Handling of Personal Information* ("NPPs"),[67] was released in February

61. John Howard MP, Prime Minister, Press Release, *Privacy Legislation,* Canberra (Mar. 21 1997).

62. *Id.*

63. Moira Scollay, Australian Privacy Commissioner, *Information Privacy in Australia - A National Scheme for Fair Information Practices in the Private Sector,* 4 PLPR 42 (1997) 44, <http://www.austlii.edu.au/au/other/plpr/vol4/#3> (accessed Sept. 25, 2000).

64. "Everyone wants to avoid a patchwork of different standards applying across different industries, technologies and State and Territory boundaries." Moira Scollay, Australian Privacy Commissioner, Foreword to *National Principles for the Fair Handling of Information,* Revised edition, January 1999 (available at <http://www.privacy.gov.au/publications/pg2pubs.html#59>) (accessed Oct. 4, 2000).

65. *Id.*

66. *Id.*

67. The 10 NPPs outline when and how a business can collect personal information and apply to Australian businesses and to foreign businesses that trade in Australia. They are, generally speaking, typical of the fair information principles which "form the core of the Data Protection laws of dozens of countries," Banisar & Davies, *supra* n. 2, at 11, and are derived from the OECD Guidelines, <http://www.privacy.gov.au/publications/pg2pubs.html#27> (accessed Oct. 4, 2000), and the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,* ETS No. 108, 1981 <http://www.coe.fr/eng/legaltxt/108e.htm> (accessed Oct. 4, 2000). In a nutshell, they require collectors of information to: (1) only collect personal information that is necessary for the business' functions or activities; (2) inform people in advance why their personal information is being collected and what it is to be used for; (3) allow people reasonable access to their information and to correct it if it is incomplete or wrong; (4) ensure that personal information is securely held and cannot be interfered with, stolen or improperly used; (5) use personal information only for its originally intended use, except with the consent of the

1998. Reiterating the government's policy that "the imposition of a heavy-handed regulatory approach to addressing privacy is not necessary," the NPPs were promoted as providing "a basis for business to develop practices to ensure that the privacy of individuals is protected."[68] Although the NPPs were based on the IPPs which already applied to the public sector under the Privacy Act, they had been modified to take account of private sector business practices as a result of consultations with a working group of representatives of commerce and industry[69] and thus set slightly lower standards than the IPPs.[70]

While several industry codes based upon the NPPs were subsequently developed with the Commissioner's assistance,[71] the overall response from business was later described as lacking in both consistency and comprehensiveness with respect to businesses which those voluntary codes covered.[72]

Like their U.S. counterparts, Australian privacy advocates and academics[73] – and even some government bodies[74] – had long been critical of the self-regulatory regime that relied solely on market forces and "moral suasion" for its efficacy. But apparently the greatest pressure for

---

individual concerned or in certain other exceptional circumstances. One NPP which is not so typical, Principle 8, introduces a principle of anonymity, providing that "Wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering into transactions." The most recent version of the NPPs (as contained in the Privacy Amendment (Private Sector) Bill 2000) (*available at* <http://www.law.gov.au/privacy/NPP.html>) (accessed Oct. 4, 2000).

68. Hon. Daryl Williams AM QC MP, Attorney General & Minister for Justice, *Privacy Principles Released,* News Release (Feb. 20, 1998) <http://www.law.gov.au/aghome/agnews/1998newsag/387_98.htm (accessed Oct. 4, 2000).

69. According to the News Release the representatives included "banks, insurers, other financial services, retailers, telecommunications, direct marketers and privacy consumer groups." *Id.*

70. Parliament of the Commonwealth of Australia, House of Representatives, *Privacy Amendment (Private Sector) Bill 2000 Explanatory Memorandum,* 14 <http://scaletext.law.gov.au/html/ems/0/2000/rtf/0642435022.rtf> (accessed Oct. 4, 2000) (hereinafter *Explanatory Memorandum*). They were also modified to enable their application to health information and transborder data flows, as required by the EU Directive. *See* EU Directive, Official Journal No L 281, 23/11/1995, 31 <http://www.privacy.gov.au/publications/pg2pubs.html#28> (accessed Oct. 4, 2000).

71. The first was the Insurance Council of Australia's *General Insurance Information Privacy Principles,* launched on August 6 1998: Hon. Daryl Williams AM QC MP, Attorney General & Minister for Justice, *Privacy First for the Insurance Industry,* News Release, August 6, 1998. <http://www.law.gov.au/aghome/agnews/1998newsag/453_98.htm> (accessed Oct. 4, 2000).

72. *Explanatory Memorandum, supra* n. 70, at 10-11.

73. *See e.g.* Paterson, *supra* n. 56; Roger Clarke, *Internet Privacy Concerns Confirm the Case for Intervention,* 42 Communications of the Association for Computing Machinery Inc. 60 (1999) <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html> (accessed Feb. 7, 2001).

74. *See* Paterson, *supra* n. 56.

the Australian Government to revert to its former policy eventually came from Australian business itself. An informal coalition of "old economy" and "new economy" industry bodies, including the powerful Australian Bankers' Association, the Insurance Council of Australia, the Australian Chamber of Commerce and Industry and the Internet Industry Association ("IIA") eventually joined forces in attempting to persuade the Government to re-review its policy and resurrect its previously proposed co-regulatory legislative approach.[75] In a letter to the Australian Prime Minister on October 30, 1998, the IIA urged the Government to review and reconsider its position on the private sector in the light of three main trends or factors. These were: firstly; concerns about the effects of potentially inconsistent State legislation on businesses operating within a cross-jurisdictional national market;[76] secondly, the need to promote consumer confidence in the integrity of Internet transactions so as to facilitate the growth of electronic commerce; and thirdly, the potentially adverse effect on Australian/European trade in the absence of a legislative framework, as a consequence of the implementation of the EU Directive.[77]

The next significant development occurred just one month after the Government's receipt of the IIA's letter. In December 1998, "in order to accelerate the development of e-commerce in both countries,"[78] the U.S. and Australian leaders issued a Joint Statement in which they formally agreed on the "underpinning principles behind a range of specific policy

75. *See* E-mail from Peter Coroneos, Executive Director, Internet Industry Association, to author, Sept. 27, 2000. In the opinion of Mr Coroneos, "Realistically it was only when the banks said they would not stand in the way of the new policy that [Prime Minister] Howard really warmed to the idea. I infer from that that it was their earlier opposition that was the main obstacle." *Id.*

76. *See infra* n. 126.

77. EU Directive, Official Journal No L 281, 23/11/1995, 31 <http://www.privacy.gov.au/publications/pg2pubs.html#28> (accessed Oct. 4, 2000). The Directive is primarily intended to further the development of the European Common Market by increasing the free flow of information within the European Union. *Id.* at Recitals (1)-(9). It addresses perceived shortcomings and inconsistencies in levels of protection previously afforded to personal data within member states by requiring them to protect the privacy of individuals' personal information, *id.* at Art. 1.1, setting minimum standards for such protection, *id.* at Arts. 5-24, and requiring each member state to pass its own national laws that meet those minimum standards, *id.* at Art. 4. Once such laws are in place, it generally prevents member states from restricting or prohibiting the free flow of personal data between them, *id.* at Art. 1.2, and prohibits its transfer to other countries that lack "an adequate level of protection," *id.* at Art. 25, subject to certain limited exceptions or "derogations," *id.* at Arts. 13, 26, such as national defence/security and crime control, *id.* at 13.1, where the individual concerned has given unambiguous consent, *id.* at 26.1(a), or where the transfer is necessary for the performance of a contract involving the individual. *Id.* at 26.1(b), 26.1(c).

78. *Australia-United States Joint Statement on Electronic Commerce,* December 1998, [hereinafter *Joint Statement*], text available as attachment to Howard Press Release, *infra* n. 79.

issues"[79] in what were perceived as key areas of electronic commerce and the information economy. The areas included taxes and tariffs, enforcement and authentication measures, online content, intellectual property rights, privacy and consumer protection. In the Statement, it was agreed as a Policy Principle that:

> Where the market alone will not solve problems, self-regulation gives maximum control and responsibility to the individual and should be the preferred approach. In some cases this may need to be facilitated by legislation to ensure effective arrangements[80]

and as a Policy Issue that:

> Ensuring the effective protection of privacy with regard to the processing of personal data on global information networks is necessary as is the need to continue the free flow of information. With regard to frameworks for personal data protection, governments and business should consider consumers' concern about their personal information. Governments should support industry in implementing effective privacy protection. Personal information should be collected and handled in a fair and reasonable manner consistent with generally accepted privacy principles. The OECD Privacy Guidelines provide an appropriate basis for policy development.[81]

Exactly 14 days after the issue of the Joint Statement by the Australian Prime Minister, the Federal Government announced its intention "to legislate to support and strengthen self-regulatory privacy protection in the private sector"[82] According to its news release, the Government had come to the view that:

> those businesses that are self-regulating should be supported by an environment of consistency and certainty in relation to data protection standards across the private sector . . . [and] [t]he best way of achieving that consistency and certainty is to establish a light touch legislative regime based on the Privacy Commissioner's *National Principles for the Fair Handling of Personal Information.*[83]

---

79. John Howard, MP, Prime Minister, *Australia-United States Co-operation on Electronic Commerce,* Press Release (Dec. 1, 1998) <http://search.aph.gov.au/search/> (accessed Sept. 28 2000).

80. *Joint Statement, supra* n. 78 at ¶ II(2).

81. *Id.* at ¶ III(3)(B).

82. Hon. Daryl Williams AM QC MP, Attorney General & Minister for Justice & Senator the Hon Richard Alston, Minister for Communications, Informational Technology and the Arts – Joint News Release, *Government to Strengthen Privacy Protection,* December 15, 1998 <http://www.law.gov.au/aghome/agnews/1998newsag/Joint_13_98.htm> (accessed Sept. 20, 2000).

83. *Id.*

G. THE PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000

The scheme announced by the Government was described as a "light-touch legislative regime" based primarily on industry codes, with a default legislative code based on the National Privacy Principles applying only where industry codes were not adopted. The news release promised that the scheme would be designed to "avoid imposing undue burdens or constraints on business," and emphasised the Government's belief that its decision "will provide a boost to electronic commerce by increasing the confidence of users that their personal data will be adequately protected."[84]

The Privacy Amendment (Private Sector) Bill 2000 was eventually introduced into the Australian Parliament on 12 April 2000, heralded by the Attorney General in his Second Reading speech as "the most significant development in the area of privacy law in Australia since the passage of the Privacy Act in 1988."[85] Mindful of the problems it now acknowledged as being associated with the self-regulatory approach (which are summarised in the Attorney General's speech referred to above and covered in greater detail in the Explanatory Memorandum referred to below) but rejecting the "full regulation" option of "a regulatory strategy based on prescriptive Commonwealth legislation,"[86] the Government had chosen to pursue a "co-regulatory" approach, which it described as "a legislative framework within which self-regulatory codes of practice can be given official recognition."[87]

The main objective of the Bill is to establish a comprehensive national privacy scheme for private sector organisations and to do so in a way that:

- meets international concerns and Australia's international obligations relating to privacy;
- recognises individuals' interests in protecting their privacy; and
- recognises important human rights and social interests that compete with privacy, such as the desirability of a free flow of information and the right of business to operate efficiently.[88]

The scheme it establishes has been promoted by the Government as

---

84. *Id.*

85. Hon. Daryl Williams AM QC MP, Attorney General & Minister for Justice, House of Representatives, *Parliamentary Debates* (Hansard) (Apr. 12, 2000) 15749 <http://www.aph.gov.au/hansard/reps/dailys/dr120400.pdf> (accessed May 4, 2000).

86. The example given being "the extension to the private sector of the framework that presently applies to the public sector under the Privacy Act," *Explanatory Memorandum, supra* n. 70, at 14.

87. *Id.* at 17.

88. The Parliament of the Commonwealth of Australia, House of Representatives, Privacy Amendment (Private Sector) Bill 2000, cl. 3 [hereinafter Privacy Amendment (Private Sector) Bill 2000].

being responsive to both business and consumer needs.[89] Business interests have been accommodated in that the NPPs which form the foundations of the new law, while based on the IPPs which apply to the public sector, have been modified as a result of the consultation process to take account of private sector business practices, and so set slightly lower standards than the IPPs.[90] The scheme is also responsive to business in that the NPPs function as a default set of "minimum standards" to which private sector organisations[91] will be bound unless they have adopted their own written privacy code. This allows and encourages individual industry sectors to formulate codes tailored to their own needs and markets, and for those that do not do so, it also possibly avoids the costs of developing and implementing their own self-regulatory regimes, or alternatively of having to comply with varying State and Territory laws.

Consumer interests are protected in that privacy codes must be approved by the Privacy Commissioner,[92] and can only receive approval if the Commissioner is satisfied that they provide at least an equivalent standard of privacy protection as the NPPs – including, among other things, satisfactory procedures for making and dealing with consumer complaints and provision for the appointment of an independent adjudicator to whom complaints may be made.[93] Consumer interests are therefore also served by all organisations being subject to relatively consistent and standardised fair information practices, including identifiable complaints mechanisms and available remedies.

In addition to evaluating applications for privacy code approvals and maintaining a register of approvals,[94] the only other roles imposed on the Privacy Commissioner under the Bill are:

- the resolution of complaints against (and a corresponding purely "complaints-driven" general oversight of compliance with the NPPs by) those organisations or industries which do not implement their own privacy codes;[95] and
- if considered appropriate, the formulation and publication of guidelines covering the making of and dealing with complaints under ap-

89. Hon. Daryl Williams AM QC MP, *Privacy in the Global Environment,* Speech at Australia-Israel Chamber of Commerce CEO Reception, Selby Anderson Solicitors, Sydney (May 18, 2000) 3 <http://search.aph.gov.au/search/> (accessed Oct. 4, 2000).

90. They have also been modified to enable their application to health information and transborder data flows, as required by the EU Directive.

91. "Organisation" is defined to mean an individual, a body corporate, a partnership, a trust or any other unincorporated association that is not a State instrumentality or agency. Privacy Amendment (Private Sector) Bill 2000, cl. 6C <http://www.law.gov.au/privacy/NPP.html> (accessed Oct. 4, 2000).

92. *Id.* at cl. 5.

93. *Id.* at cl. 18BB(2)-(3).

94. *Id.* at cl. 18BG.

95. *Id.* at cl. 27(1)(aa)-(ac).

proved codes.[96]

Once a code has received the Commissioner's approval, he or she has no further role in relation to that code or the industry it covers (assuming it has appointed an independent complaints adjudicator) unless application is made for the code to be varied, or it is revoked at the instance of the Commissioner or an organisation bound by it.[97]

H. MAIN CRITICISMS AND RESPONSES

Even before being tabled in Parliament, the Bill received considerable criticism based on the "large numbers of exemptions and exceptions"[98] it contained and on numerous other grounds. After its Seconding Reading, the Bill was referred to the House of Representatives Standing Committee on Legal and Constitutional Affairs (comprising a 6:4 majority of government members) for inquiry and report. In its report on the Bill released in June 2000,[99] the Committee – having received some 130 written submissions and a considerable volume of oral evidence from witnesses during public hearings – acknowledged most of the criticisms and made 23 recommendations for amendments.

A further report on the Bill by a similarly Coalition-weighted Senate Legal and Constitutional Legislation Committee was due to be released in October 2000 and a more comprehensive and wide-ranging Inquiry into e-privacy by a Senate Select Committee on Information Technologies (set up before the introduction of the Bill into Parliament) was due to report in November 2000.

Particularly controversial are the Bill's "small business" exemptions, which not only drew expected initial criticism from the European Union[100] but also received adverse comment from the Privacy Commissioner who saw them as preventing the scheme from achieving its goal of giving people the assurance to participate in e-commerce, confident that

96. *Id.* at cl. 18BF(1).

97. Privacy Amendment (Private Sector) Bill 2000, cl. 18BE.

98. Roger Clarke, *Privacy Bill Needs Much More Work,* The Australian (Feb. 15, 2000) 3 <http://www.anu.edu.au/people/Roger.Clarke/DV/ACS000215.html> (accessed Oct. 4, 2000).

99. Parliament of the Commonwealth of Australia, *House Of Representatives Standing Committee on Legal and Constitutional Affairs, Advisory Report on the Privacy Amendment (Private Sector) Bill 2000,* June 2000, [hereinafter *H.R. Advisory Report*] <http://www.aph.gov.au/house/committee/laca/Privacybill/contents.htm> (accessed Oct. 4, 2000).

100. European Commission, *Submission to House of Representatives Standing Committee on Legal and Constitutional Affairs, Inquiry into Privacy Amendment (Private Sector) Bill 2000,* <http://www.aph.gov.au/house/committee/laca/Privacybill/submiss.htm> (accessed Oct. 4, 2000); *see also* Simon Hayes, *Privacy Bill Under Fire from the EU,* The Australian (June 13, 2000) <http://www.australianit.com.au/> (accessed June 21, 2000).

their information will not be misused.[101] All private sector organisations are to be exempt from the legislation for an initial period of 12 months after its commencement.[102] In accordance with the Government's policy to minimise compliance costs for small business, it will only apply after the initial period to those small businesses[103] that are considered by the Government to constitute a risk to personal privacy – namely those which provide a health service; hold health information (other than merely as part of their employee records); are contracted to provide government services; or are involved in collecting personal information or disclosing it to third parties "for a benefit, service or advantage."[104] Estimates by both government and privacy group sources agree that upwards of 90% of all Australian businesses will fall outside the new regime under these exemptions.[105]

Direct marketing also constitutes an exemption of a kind because of the way it is addressed in the NPPs. Principle 2.1 provides that an organisation must not use or disclose personal information about an individual for a purpose (called a secondary purpose in the Bill) other than the primary purpose of collection unless, inter alia:

> (c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
>
> (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
>
> (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
>
> (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
>
> (iv) the organisation gives the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications.

---

101. Australian Privacy Commissioner, *Submission to House of Representatives Standing Committee on Legal and Constitutional Affairs, Inquiry into Privacy Amendment (Private Sector) Bill 2000* (cited by Karen Dearne, *Privacy Free Zone,* Australian IT (June 27, 2000) 16 <http://www.australianit.com.au/common/story> (accessed July 5, 2000)). The full text of many of the submissions made to the *Inquiry* are available in PDF format at <http://www.aph.gov.au/house/committee/laca/Privacybill/submiss.htm> (accessed Oct. 4, 2000).

102. *Privacy Amendment* (Private Sector) Bill 2000, cl. 16 D. This provision is designed to allow small business extra time to ensure its compliance. *Explanatory Memorandum, supra* n. 70, at 5.

103. Defined as businesses with annual turnovers of $AU 3 million or less *Privacy Amendment* (Private Sector) Bill 2000, cl. 6D(1).

104. *Id.* at cl. 6D(4), which effectively makes these businesses "organisations" rather than "small businesses" for the purposes of the Bill, and thus outside of its "small business" exemptions.

105. Dearne, *supra* n. 101.

Generally referred to as an "opt-out" approach, this requires consumers to take a positive step to avoid receiving further communications from a direct marketer, as compared with an "opt-in" approach which requires express prior consent by a consumer before a direct marketing approach can be made. Notwithstanding a large number of submissions which argued that the Bill should provide for a mandatory opt-in mechanism and acknowledgment in the Report that the issue "is clearly a matter of concern to many members of the community . . . [and] illustrates the tensions inherent in the balance between the privacy of the individual and the need to avoid placing undue restrictions on business"[106] and even that "[a] opt-in standard is desirable,"[107] the Committee concluded that it was not convinced that an opt-in approach would be practicable. It therefore recommended only minor amendments intended to give NPP 2.1(c) more clarity, including that the opt-out opportunity must be given to consumers *every time* personal information is used for the secondary purpose of direct marketing and that notice of this opportunity be placed prominently on the material and accompanied by certain prescribed contact details.[108]

Other exemptions that have been criticised are those proposed for employment-related use of employee records,[109] for media organisations,[110] and for politicians and political parties.[111]

The Bill has also been attacked for weaknesses in its provisions relating to health information[112] and the effectiveness of its overall enforcement regime,[113] especially with regard to the lack of monitoring by the Commissioner of complaints handled by independent adjudicators under industry codes and the lack of appeal rights – particularly for complainants – against decisions by industry adjudicators or the Privacy Commissioner.[114]

In response to the House of Representatives Advisory Report, the Government has released details of the amendments it proposes to make

106. *H.R. Advisory Report, supra* n. 99, at 103.

107. *Id.* at 104.

108. *Id.* at Recommendation 20.

109. *Privacy Amendment* (Private Sector) Bill 2000, cl. 7B(3). The Government considers this area better dealt with under workplace relations legislation. *Explanatory Memorandum, supra* n. 70, at 5.

110. Originally, broadly defined as including many other organisations that provide information to the public. *Privacy Amendment* (Private Sector) Bill 2000, cll.18, 19, and 42.

111. *Id.* at cl. 7C.

112. *See id.* at items 16, 17, 27 (amending definitions in § 6 of Act) and 131 generally, and NPP 10 in particular.

113. The scheme established by the Bill is "complaints-driven": *see generally id.* at items 98-130.

114. Dearne, *supra* n. 101, provides a good overview of several of the enforcement criticisms.

to the Bill when it next comes before the House for debate.[115] In relation to the small business exemptions for example, small businesses previously exempted from the new law will now be able to voluntarily opt-in so as to subject themselves to the default privacy standards in the absence of applicable approved industry codes.[116] The media exemption will now only be available to organisations that commit publicly to published media industry codes[117] and businesses that handle health information will be required to comply with the law earlier than was previously the case.[118]

Overall reaction to the original Bill and the Government's proposed amendments to it have generally not been positive to date. Prominent Australian privacy commentator and editor of the Privacy Law and Policy Reporter, Professor Graham Greenleaf, has expressed the opinion that "[t]here are so many exceptions in the Bill that it will make it easier [than it has previously been] for businesses to claim they're adequately protecting people's privacy when they aren't" and that it will therefore protect businesses from allegations of privacy invasion,[119] while an Australian Computer Society privacy spokesman has claimed that "it's not a privacy bill, it's a legitimisation of privacy-invasive practices bill."[120] Flack on various aspects has also come from the Australian Consumers Association and the Health Issues Centre,[121] with the former organisation's submission to the ongoing Senate e-Privacy Inquiry referring to "Weblining – an information-age version of that nasty old practice of redlining - . . .[as being] like call number display on steroids."[122]

I. CONCLUSION

In Australia and the U.S., there have been increasing calls for government action to strengthen personal data protection in the private sector, particularly as a result of public concerns about new threats to

115. Hon Daryl Williams AM QC MP, Attorney General and Minister for Justice, *Privacy Protection in the Private Sector Moves Closer,* News Release (Sept. 8 2000) <http://law.gov.au/aghome/agnews> (accessed Sept. 14, 2000).

116. Attorney General's Department, *Privacy Amendment (Private Sector) Bill 2000: Outline of Proposed Government Amendments – September 2000,* 11 <http://www.law.gov.au/privacy/summamend.htm> (accessed October 4, 2000).

117. *Id.* at 20-21.

118. *Id.* at 26.

119. Dearne, *supra* n. 101.

120. Karen Dearne, *Halt 'Privacy Invasion' Bill, Inquiry Told,* Australian IT (Oct. 3, 2000) 7 <http://www.australianit.com.au/common/storyPage/0,3811,1266280%5E442,00.html> (accessed Oct. 3, 2000).

121. *Id.*

122. Karen Dearne, *Privacy on the Line,* Australian IT (Oct. 3, 2000) <http://www.australianit.com.au/common/storyPage/0,3811,1266431%5E501,00.html> (accessed Oct. 3, 2000).

individual privacy posed by the Internet and other information technologies. Recent media reports and surveys in both countries suggest that such concerns are generally justified. In Australia for example, a survey carried out early in 2000 indicated that up to 92% of Australian companies were collecting personal information through Web sites,[123] and a 1999 national poll revealed that 56% of Australians were particularly worried about the invasion of privacy created by new information technologies.[124]

The Australian Government, driven primarily by a desire to promote the growth of e-commerce in response to doubts regarding Australia's ability to meet the "adequate protection" requirements of the EU Directive,[125] calls for a "light-touch" legislative regime for both new-economy and old-economy business associations and the possibility that some Australian States and Territories would impose their own controls[126] and potentially create inconsistencies between different Australian jurisdictions, has finally been persuaded to change its former self-regulatory policy. Having rejected the option of full regulation based on prescriptive legislation, it is in the course of implementing a co-regulatory scheme that it hopes will address public concerns and still achieve its other policy objectives.

In a recent presentation to an E-Commerce and Privacy Conference, a Director of the Office of the Privacy Commissioner in Canada offered the following reflections on his experience in the position:

> Having spent the last several years at the Office of the Privacy Commissioner, I have come to recognize that while there may be changing responsibilities and expanding jurisdictions, and that while there may be different audiences and shifting priorities, there is an underlying agenda to our work or mission and it is fairly straightforward, if somewhat delicate. It is to promote the perspective that all of our practices in this increasingly digital and commercialized world must be informed by a sense of human values and that they must take place in an environment of ethical principles. And that respect for the individual and for the privacy rights of the individual must be fundamental to all our in-

123. Freehill Hollingdale & Page, *Internet Privacy Survey Report 2000*, 8-10 <http://www.freehills.com.au/4A25682300141146/All/C79C9F807E7A22944A25689400093AAA?OpenDocument&1=10-Articles+and+Publications~&2=50-Internet+Privacy+Survey~&3 (accessed Oct. 4, 2000).

124. Roy Morgan Research Centre, *"Big Brother" Bothers Most Australians,* The Bulletin (Aug. 30, 1999) (Finding No. 3221) <http://www.roymorgan.com.au/polls/1999/3221/index.html> (accessed Oct. 4, 2000).

125. *See* sources cited *supra* n. 77, and accompanying text.

126. The State of Victoria had threatened to do this and introduced a bill to cover both public and private sectors in its parliament but later agreed to defer its bill and contribute to the federal process. *See* Hon. Daryl Williams AM QC MP, Attorney General, *Victorian Agreement on Privacy Welcomed,* News Release (Dec. 16, 1998) <http://www.law.gov.au/aghome/agnews/1998newsag/504_98.htm> (accessed Oct. 4, 2000).

formation practices.[127]

The proposed new co-regulatory regime for the Australian private sector is certainly not without its critics. Most would agree that the exemptions and exceptions it currently proposes for small business are its major downside. Whether there will be a corresponding upside will eventually be judged by its performance in two major tests: firstly, whether it satisfies the EU Directive's "adequate level of protection" requirements; and secondly, the extent to which it succeeds in boosting consumer confidence in transacting with Australian businesses via the Internet by encouraging and supporting business to adhere to basic ethical principles in its information technology practices.

127. Brian Foran, Office of the Privacy Commissioner of Canada, *The Role of the Federal Privacy Commissioner, Panel Presentation to E-Commerce and Privacy Conference,* Ottowa, Ontario, (Feb. 21, 2000) <http://www.privcom.gc.ca/english/02_05_a_000221_2_e.htm> (accessed Oct. 4, 2000).