8

Miscellaneous issues

Introduction

8.1 This chapter addresses:

- the application of the Bill to existing information;
- the coverage of tenancy databases by the Bill;
- the provisions of the Bill dealing with direct marketing; and
- the European Union Directive on Data Protection.

Application of the Bill to existing information

Background

8.2 Clause 16C of the Bill outlines the application of the Bill to personal information held by organisations at the date of commencement of the legislation (either 12 months after it receives Royal Assent or 1 July 2001 – whichever is the later).

8.3 According to clause 16C the National Privacy Principles (NPPs) apply as follows to existing information:

- National Privacy Principles 1 (Collection), 3 (Data Quality, but only insofar as it relates to the collection of personal information) and 10 (Sensitive information) apply after the commencement of the legislation in relation to the collection of personal information.

- National Privacy Principles 3 (Data Quality, but only insofar as it relates to personal information used or disclosed), 4 (Data Security), 5 (Openness), 7 (Identifiers) and 9 (Transborder Data Flows) apply to personal information held by an organisation regardless of whether the organisation holds the personal information as a result of collection occurring before or after the commencement of the legislation.
- National Privacy Principles 2 (Use and Disclosure) and 6 (Access and Correction) apply only in relation to personal information collected after the legislation commences.
- National Privacy Principle 8 (Anonymity) applies only to transactions entered into after commencement of the legislation.

8.4 A similar approach was taken at the time of commencement of the existing *Privacy Act 1988* which applies to the public sector.[1]

8.5 Clause 16D provides that the National Privacy Principles only apply to small businesses (that falls within the legislation) from a further 12 months beyond the date on which they are applicable to other organisations.

8.6 The Government's view is that to require that all the principles apply to existing information would impose 'unjustifiably high compliance costs on business, and these costs may well be passed on to the consumer.'[2]

8.7 In the Government's view organisations that hold existing databases of personal information need to take reasonable steps to ensure that the data is accurate, complete and held securely. The organisation will also need to be 'open to consumers about what information it already holds and how it collects, holds and proposes to use or disclose such information.' After the legislation takes effect organisations that hold existing databases of personal information will need to comply with all aspects of the Bill when they update that information, including NPPs 1, 2 and 6 relating to collection, access, use and disclosure.[3]

Arguments of those in favour of the application of NPPs to existing information

8.8 The Committee has received a number of submissions that suggest that some of the excluded NPPs should apply to information collected prior to the commencement of the legislation. NPP 2 (Use and Disclosure) and NPP 6 (Access and Correction) were the focus of submissions on this

1 See section 15, *Privacy Act 1988.*

2 Fact sheet, 'Privacy and Existing Databases', Attorney-General's Department, 12 April 2000.

3 Ibid.

issue. These are regarded by many organisations as central privacy principles that should apply regardless of when information is collected.[4]

8.9 The Australian Consumers' Association described this exemption as 'a serious deficiency'.[5] They suggested that the exemption from the application of these two NPPs to information existing at the date of commencement of the Bill would 'confer commercial advantage to incumbent holders of consumer data, especially those in large corporations.'[6] This, they argued, could potentially:

> …constitute a barrier to entry in some markets, and therefore confront consumers with the impost of less diversity and higher prices while having a two-tier system of privacy protection.[7]

8.10 The Victorian Government also criticised the fact that the NPPs did not apply to existing information and submitted that this would create an 'undesirable division between large stores of information that are currently held and new information that will be collected and used for the same purposes.'[8] This, they argued, would defeat '[m]any of the aims of a data protection law'[9] by leaving 'current misuses of personal information … legal and unrestricted.'[10] In evidence they stated that '[f]or previous information … the obligations about use, disclosure and access do not apply. Unless you re-collect it, the obligations will not kick in.'[11] They also suggested that it would create 'enticing incentives for organisations to run collection campaigns prior to the legislation coming into effect'.[12]

8.11 The Victorian Government also thought that this aspect of the Bill could create practical problems for many organisations in that they may need to apply different requirements to information that may otherwise be held on the same database.[13] Along the same lines the Australian Privacy Charter Council suggested that many organisations would find it easier to apply the same regime to all data.[14]

---

4 For example Communications Law Centre, *Submissions*, p.S339. See also Electronic Frontiers Australia, *Submissions*, p.S319.

5 Australian Consumers' Association, *Submissions*, p.S89. See also Electronic Frontiers Australia, *Submissions*, p.S316.

6 Australian Consumers' Association, *Submissions*, p.S89.

7 Ibid.

8 Victorian Government, Department of State and Regional Development, *Submissions*, p.S200.

9 Ibid.

10 Ibid. See also Communications Law Centre, *Submissions*, p.S339.

11 Victorian Government, Department of State and Regional Development, *Transcripts*, p.274.

12 Victorian Government, Department of State and Regional Development, *Submissions*, p.S200.

13 Ibid.

14 Australian Privacy Charter Council, *Submissions*, pS253. See also Privacy NSW, p.S290 and *Transcripts*, p.187.

Arguments against the application of the NPPs to existing information

8.12 The Committee also received evidence that outlined the problems that would be caused if NPP 2 (Use and Disclosure) and NPP 6 (Access and Correction) were to apply to data in existence when the legislation commenced.

8.13 The Australian Direct Marketing Association (ADMA) emphasised that the need for an adjustment or education period to bring existing private sector databases into compliance is real.[15] Mr Edwards of ADMA stated that 'to say that it should apply to all existing data as a blanket on day one, I think defies reality. It just could not happen.'[16]

8.14 ADMA also reject the criticism that the non-application of NPPs 2 and 6 to data collected prior to the commencement of the legislation will lead to organisations amassing personal information databases prior to commencement. They argue that:

> … [I]t makes no sense from a commercial perspective to amass data without a specific purpose in mind. Marketing databases, by their nature, must be kept up to date in order to be commercially viable. It would be illogical for organisations to allocate precious IT resources to the maintenance and upkeep of databases that had no identified purpose other than to be held in reserve for some undetermined future use.[17]

8.15 In oral evidence ADMA stated that some organisations will need to undertake 'major improvements to their information and handling practices.'[18]

8.16 The Australian Bankers Association submitted that the approach taken in the Bill is 'realistic'.[19] They argued that the 'task of combing through existing data bases and trying to ascribe a primary purpose to the data, if possible at all, would be an immense and costly task.'[20]

8.17 Both the Australian Bankers' Association and the Australian Chamber of Commerce and Industry agreed with ADMA that customer data can become outdated very quickly.[21] Personal data, they submit, has a short

15 Australian Direct Marketing Association, *Submissions*, p.S184.

16 Australian Direct Marketing Association, *Transcripts*, p.142.

17 Australian Direct Marketing Association, *Submissions*, p.S193. ADMA's views were supported by Reader's Digest, *Submissions*, p.S261.

18 Australian Direct Marketing Association, *Transcripts*, p.140.

19 Australian Bankers' Association, *Submissions*, p.S558.

20 Ibid.

21 Australian Bankers' Association, *Submissions*, p.S558, Australian Chamber of Commerce and Industry, *Submissions*, p.S567 and Australian Direct Marketing Association, *Submissions*, p.S193.

life span and it is 'in the interest of business to ensure the accuracy of any personal information that they collect.'[22] On this issue ADMA submitted that if personal data is to be of any benefit to an organisation, the organisation would need to contact those people over time in relation to whom they hold information. During the course of contacting them they would have to go through the process of making the opt-out provision available to them.[23] Reader's Digest stated that for information to be accurate and up to date it has to be used.[24]

8.18 The Victorian Government, however, suggested that '[t]here is a lot of information on databases at the moment that does not have any use-by date'.[25] They cited as examples birth dates, ethnicity, gender or former marriages. Such information, they said, is historical. It does not need updating and can still be accumulated and subject to abuse.[26] Some information such as age and gender could be valuable marketing tools if used together with publicly available material.[27]

8.19 The Australian Consumers Association and Electronic Frontiers Australia thought that a phase in or transitional period should apply to the application of the NPPs to existing information.[28] The Australian Privacy Charter Council considered there was 'no reason why organisations should not be required to use [their] best endeavours' to comply with at least with the spirit of Principles 2 and 6'.[29]

Conclusion

8.20 The Committee notes the concern expressed by many about the exclusion of existing information from coverage by the Bill. A total exclusion of existing information does appear to the Committee to leave people totally unprotected in relation to information currently held about them especially given that there is a minimum of twelve months before the legislation commences operation. It sees no reason why providers of existing databases should not be able to indicate at some time to people

22 Australian Chamber of Commerce and Industry, *Submissions*, p.S567.

23 Australian Direct Marketing Association, *Transcript*, p.142. The Fundraising Institute of Australia also agreed that this was the case and supported the provisions of the Bill on the treatment of existing information, *Transcript*, p.278.

24 Reader's Digest, *Transcript*, p.181.

25 Victorian Government, Department of State and Regional Development, *Transcript*, p.274.

26 Victorian Government, Department of State and Regional Development, *Transcript*, pp.274-275.

27 Such as telephone directories or electoral roll, Victorian Government, Department of State and Regional Development, *Transcript*, p.275.

28 Australian Consumers' Association, *Submissions*, p.S89, Electronic Frontiers Australia, *Submissions*, p.S319.

29 Australian Privacy Charter Council, *Submissions*, p.S253.

whose personal information may be on an existing database, how they came by the information and how the information may be removed from the database.

8.21 However, the Committee has also taken careful note of the evidence suggesting that applying the NPPs in full to information already on databases at the time of the commencement of the legislation would be onerous.

8.22 The Committee emphasises that the legislation was introduced into Parliament on 12 April 2000 and there is still a considerable period of time until it commences (either 12 months after it receives Royal Assent or 1 July 2001- whichever is the later). Therefore everyone, including organisations currently holding databases containing personal information, is on notice as to the proposed requirements of the legislation and should be familiarising themselves with the NPPs and preparing to be able to meet their obligations under the legislation once it commences. The Committee hopes that organisations would begin to voluntarily apply the NPPs to any personal information they currently hold.

Recommendation 17

The Committee recommends that as from the date of commencement of the legislation a further period of grace of three years be extended to holders or users of existing information in respect of information held at that time.

8.23 What is regarded by some Committee members as a lengthy period is balanced by the Committee's view that, during that period of grace, if an organisation makes use of material on a database to make any contact with consumers they should inform them of the material they currently hold and its source and provide an opportunity to opt out of further contact with the organisation. The Committee has not had the time to consider the precise mechanism but the Government should ensure that it is covered in the Bill.

Recommendation 18

If, at the conclusion of three years, organisations have not used that information, the Committee recommends that they should be required either to delete it or seek explicit consent from the subject of the information to continue to hold it.

8.24 It should be noted that any sale of existing data or its use for a purpose other than that for which it was collected would mean that the NPPs would apply at that point.

8.25 Some Committee members expressed the reservation that this period allows, effectively, a total of four years grace for existing material on databases. Given that a review is envisaged in two years, the effective operation of this 'phase in' should be included in that review.

8.26 The Committee is confident this will impose no additional burden on organisations given the lead in time to the commencement of the legislation, the period of grace and the requirement to update information. Evidence to the Committee indicated that personal information becomes outdated and useless if not used comparatively regularly. Organisations would not be required to undertake any additional contact with the subject of the information to comply with the Committee's recommendation. Rather the usual contact that will be made as a matter of course by organisations during the period of grace would be used, under the Committee's proposal, to provide an opportunity to people to withdraw from contact with the organisation and discover the source of the information held about them. The proposal is designed to provide a transitional arrangement where existing information is used by an organisation for its own business.

8.27 The Committee expresses reservations that existing databases will also be exempt from NPP 6 (Access and Correction) for a lengthy period of time. The Committee would suggest that during the period of grace, NPP 6 should apply provided this does not become oppressive. In the Committee's view access and correction rights to material held in hard copy (rather than in microfiche or digital form) would be likely to make an access request prima facie oppressive.

8.28 If the organisation proposes to disclose or dispose of the information to another entity the NPPs will apply prior to that disposal.

8.29 Mr Cadman wished to record the following as his observations on this issue. Evidence given to the Committee by commercial users of databases clearly indicated that data, unless amended, is of little worth after three years. To impose further privacy obligations as proposed in recommendations 17 and 18 on holders of data would be an unnecessary and onerous obligation. The National Privacy Principles (NPPs), with the exception of NPP 2 and NPP 6, will cover all organisations which hold databases. At the date of commencement of the Act, all data collected will have to comply with the Act.

Application of the Bill to tenancy databases

8.30 The Committee received a number of submissions raising specific privacy problems resulting from the accumulation of personal information on tenancy databases. These databases have developed since the late 1980s. Submissions have highlighted the scope such databases create for breaches of privacy. The Committee was disturbed by some of the evidence presented.

8.31 The Residential Tenancies Authority (Queensland), the statutory authority responsible for the administration of the residential tenancy law in Queensland,[30] stated that '[r]esidential tenancy databases are a commercially operated information service used within the residential rental industry to screen tenants.'[31] The Authority submits that tenancy databases operate across state borders.[32] Generally, they stated, real estate agents use the databases to list tenants for a breach of their tenancy agreement or to obtain information about those listed on the database.[33] It would appear from the submissions that large amounts of personal information have been, and are being, collected.

8.32 The Residential Tenancies Authority (Queensland) submitted that privacy issues arising as a consequence of the databases include, for example, the existence of incorrect information on the databases that the tenant cannot access or easily correct, mistaken identity, people not being informed of their listing and continued listing despite the outcome of a judicial process in the tenant's favour.[34] Several submissions outlined examples of the adverse effect of listing on tenants and the difficulties encountered in accessing and correcting incorrect or outdated information.[35] For example, the Hawkesbury Women's Housing Information Service highlighted the problems faced by people fleeing violent relationships who faced difficulties obtaining accommodation due to databases listing defaults in the name of the former partner. They also cited difficulties faced by people with identical surnames in obtaining accommodation because of defaults listed against a person with an identical name.

---

30 Residential Tenancies Authority of Queensland, *Submissions*, p.S434.

31 Ibid.

32 Ibid.

33 Ibid. The Tenants Union of New South Wales stated in their submission that the Tenancy Information Centre Australiasia Holdings Pty Ltd could have over 200,000 tenants on its database and another (Rentcheck) 250,000-350,000.

34 Residential Tenancies Authority of Queensland, *Submissions*, pp.S434-435.

35 The Hawkesbury Women's Housing Information Service, *Submissions*, pp.S451-452. The Uniting Care NSW/ACT, *Submissions*, pp.S458-459 provided several examples in their submission. See also Northern Area Tenants Service Inc, *Submissions*, pp.S453-454 and submission from Ms Kathryn Lucas, *Submissions*, p.S463.

8.33 Several submissions canvassed other concerns about the Bill but a common concern was the lack of application of many of the NPPs to information that is on the databases at the time of commencement of the legislation.

8.34 In the light of these concerns many organisations submit that the NPPs should apply to personal data held on tenancy databases whether it was collected before or after the commencement of the legislation. The Tenants' Union of NSW submitted that clause 16C has the effect of legitimising the holding, use and disclosure of data that has been amassed[36] and the exclusion of NPP 6 (Access and Correction) will deny tenants access to information held currently as well as the opportunity to correct information.[37] The Residential Tenancies Authority (Queensland) also had concerns about the non-application of NPP 6 to information gathered prior to the commencement of the legislation. They argued that individuals should have the right to correct personal information already held when the law commences where the information is not complete or accurate.[38] The Tenants' Union of Queensland indicated it would support a phasing in period to allow relevant companies to systematically check compliance.[39]

Conclusion

8.35 The Committee was disturbed by some of the evidence presented about the consequences for some tenants of their listing on tenancy databases. The evidence suggests that the difficulties some tenants continue to experience is the result of being listed on tenancy databases, notwithstanding the fact that the reasons for their listing have been satisfactorily remedied. As a consequence in some cases finance and employment relationships are unfairly affected.

8.36 It is the Committee's view that the Bill should apply to tenancy databases from the date of commencement. This provides the owners of the databases with at least 12 months to prepare and to revisit their policies and procedures.

8.37 As was noted in Chapter 2 a number of submissions also noted that tenancy databases may fall within the small business exemption. The Committee is confident that the recommendations contained in that Chapter will ensure that tenancy databases will be covered by the Bill. In

36 Tenants' Union of NSW, *Submissions*, p.S474.

37 Ibid. See also Tenants Union of Queensland, *Submissions*, p.S528.

38 Residential Tenancies Authority of Queensland, *Submissions*, p.S436.

39 Tenants' Union of Queensland, *Submissions*, p.S528.

the light of the evidence it has received the Committee is strongly of the view that tenancy databases must be covered.

Recommendation 19

The Committee recommends that the National Privacy Principles apply to tenancy databases from the date of commencement of the Bill and the Government ensure that tenancy databases do not gain the benefit of the small business exemption.

Direct marketing

8.38 National Privacy 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:

> (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.[40]

Criticisms of NPP 2.1(c)

8.39 The approach set out in NPP 2.1(c) is described as the 'opt-out' approach. That is, in order for consumers to avoid receiving direct marketing

40 See NPP 2.1, Schedule 3 of the Bill.

material, they must take a positive step to 'opt-out' of receiving further communications from the direct marketer. The alternative to the 'opt-out' approach is the 'opt-in' approach which requires the express prior consent of the individual to whom the information relates before a direct marketing approach can be made. The Committee notes that a large number of submissions argued that the 'opt-out' approach was inadequate and that the Bill should provide for a mandatory 'opt-in' mechanism.[41] This issue is clearly one that generates a good deal of concern in the community. Mr Tony Troughton-Smith, for example, submitted that he was:

> …firmly of the opinion that an "opt-in" model would better protect the rights of each of us as individual citizens instead of the "opt-out" approach currently proposed. Any organisation requesting information from any individual should be compelled to state the purpose for which the information is required, and [be] prevented from using the information in any other way without explicit advance permission of the person concerned.[42]

8.40 In advocating the 'opt-in' position, Mr Tristan Owen observed that under the Bill:

> …I can only "opt out" which means I would have to contact hundreds of organisations and go through a lot of hassle to try and get off their databases.
>
> It should be illegal for information given for one purpose (filling out forms, using credit cards, etc) to be use for another purpose without my informed written consent.[43]

8.41 In an exhibit attached to its submission, Xamax Consultancy Pty Ltd argued that NPP 2.1(c) '…would effectively legitimate (sic) existing privacy abuses inherent both in direct mail and in outbound tele-marketing.'[44] It was also argued that, if the Bill was passed in its present form it would:

> …considerably worsen relationships between marketers and consumers. The opt-out regime legitimised by this Principle is completely against the public's interest.[45]

---

41 See for example submissions number 2, 3, 5, 6, 7, 13, 14, 16, 17, and 19.

42 Mr Tony-Troughton-Smith, *Submissions*, p.S3.

43 Mr Tristan Owen, *Submissions*, p.S14.

44 Xamax Consultancy Pty Ltd, *Exhibit 4*.

45 Ibid.

8.42 The Australian Consumers' Association criticised NPP 2.1(c) for being 'convoluted and complex.'[46] It argued that determination of 'practicality' when seeking consent to direct market will be made by direct marketers.[47]

8.43 In oral evidence the Association acknowledged that an opt-in regime would 'present a lot of challenges.'[48] However, it was pointed out that an opt-in standard was being proposed as best practice in terms of electronic mail.[49]

8.44 In addition, the Association noted that the terms of NPP 2.1(c)(iv) mean that a consumer would only ever be given one chance to opt out of receiving further communications.[50] The Association recommended that the consumer be given an opportunity to opt-out on each approach made by a direct marketer.[51]

8.45 The Australian Privacy Charter Council made a similar point when it noted that:

> It is already clear that some direct marketers are seeking an interpretation of the Principle which would allow a continuation of unsolicited approaches without even an opt-out opportunity being offered. This is in our view wholly contrary to the "spirit" of the Principle which is intended to give individuals a choice in most circumstances as to whether they continue to receive unsolicited communications from organisation about goods and services…[52]

8.46 Electronic Frontiers Australia (EFA) submitted that NPP 2.1(c) was:

> …contrary to international developments and effectively legitimizes the practice of "spamming" (the sending of unsolicited E-mail advertising) on the Internet.[53]

8.47 EFA recommended that:

> …the direct marketing exception should be replaced with an "opt-in" provision that permits the use of personal information for direct marketing purposes only by specific prior consent.[54]

---

46 Australian Consumers' Association, *Submissions*, p.S90.

47 Ibid.

48 Australian Consumers' Association, *Transcript*, p.S121.

49 Ibid.

50 Australian Consumers' Association, *Submissions*, p.S91.

51 Ibid.

52 Australian Privacy Charter Council, *Submissions*, p.S254.

53 Electronic Frontiers Australia, *Submissions*, pp.S317-318.

54 Ibid.

8.48 This recommendation was not restricted to the electronic world. In oral evidence it was argued that direct mail in all of its forms should be subject to an-opt in requirement.[55] However, in a supplementary submission, EFA conceded that a provision which specifically excluded email from the direct marketing exemption could be an acceptable position.[56]

8.49 In addition, EFA gave evidence that if the opt-out system were to be retained in the Bill, it would favour a system which, as part of the details provided to enable the consumer to opt-out, an Australian street address and telephone number were required to be set out.[57]

8.50 The National Party Communications and Information Technology Committee's submission also focussed on the impact of NPP 2.1(c) in the electronic environment. The submission argued that the practice of 'spamming' is not adequately addressed in the Bill:

> The major problem with the proposed legislation is that National Privacy Principle 2.1(c) is "opt-out" for electronic forms of communication. This means that people must pay to receive direct marketing e-mails without knowing what is in them first.[58]
>
> … The Committee believes that no person should be compelled to pay to receive something before knowing what it is. Unfortunately, this is precisely what an "opt out" principle results in when it is applied to electronic forms of communication…[59]

8.51 The National Party Committee's proposed solution to the problems of spamming was to insert a new sub-principle into NPP 2.1(c) which would prevent the use of personal information for direct marketing purposes if there would be a direct or indirect cost to the recipient of receiving the initial communication from the organisation.[60]

8.52 The Coalition Against Unsolicited Bulk Email, Australia's submission also noted that:

> Because the cost of sending millions of copies of spam is near zero…[it] is plain to anybody that even with spammers being required to provide an opt-out facillity, the one shot that they get

55 Electronic Frontiers Australia, *Transcript*, p.297.

56 Electronic Frontiers Australia, *Submissions*, p.S637.

57 Electronic Frontiers Australia, *Transcript*, p.300.

58 National Party Communications and Information Technology Policy Committee, *Submissions*, p.S125.

59 National Party Communications and Information Technology Policy Committee, *Submissions*, p.S127.

60 National Party Communications and Information Technology Policy Committee, *Submissions*, p.S125.

> would result in electronic mail boxes ceasing to be viable very quickly if this behaviour were taken as acceptable.[61]

8.53 The Coalition recommend that NPP 2.1(c) be amended to prevent direct marketing unless the organisation determines on each occasion that it proposes to use the information that:

- it is impracticable for the organisation to seek the consent of the individual; and
- the individual would not incur any direct or indirect costs in receiving the communication.[62]

Support for NPP 2.1(c)

8.54 The Committee notes, however, that a number of witnesses expressed their support for the Bill. ADMA, for example, expressed its support for a light touch legislative regime dealing with privacy.[63] ADMA advised the Committee that it was the first industry association to incorporate the Privacy Commissioner's National Principles for the Fair Handling of Personal Information (on which the NPPs in the Bill are based), in their entirety, into its Code of Practice.[64]

8.55 ADMA pointed out that the code it now has in place will exceed the minimum requirements of the Bill.[65] In addition, ADMA members are obliged to remove the names of individuals who register with ADMA's Do Not Mail/Do Not Call and E-mail Preference Services from their mailing lists.[66]

8.56 In oral evidence, ADMA advised the Committee that the opt out standard is the standard that has generally been adopted internationally.[67] It rejected, however, the idea that an opportunity to opt-out should be given with every consumer contact, suggesting that having to repeatedly ask whether the customer would like to opt out would not accord with commercial reality.[68]

61 Coalition Against Unauthorised Bulk Email, Australia, *Submissions*, p.S162.
62 Coalition Against Unauthorised Bulk Email, Australia, *Submissions*, pp.S165-166.
63 Australian Direct Marketing Association, *Submissions*, p.S189.
64 Australian Direct Marketing Association, *Submissions*, p.S188.
65 Australian Direct Marketing Association, *Submissions*, p.S193.
66 Ibid. ADMA represents approximately 450 corporations with an interest in direct marketing communications, *Transcript*, p.139.
67 Australian Direct Marketing Association, *Transcript*, p.143.
68 Ibid.

8.57 Reader's Digest Australia, one of the world's largest direct mail marketers, supported the concept of 'light touch' legislation.[69] American Express also supported the legislation and noted that it has had an "opt-out" program for its card members around the world for a number of years.[70] American Express further commented on:

> …the importance of opt-out programs in a balanced approach to privacy protection. It places the privacy choice on those who should decide ie the consumers. If he/she chooses to receive mail because he/she likes the product or services then there should be no impediment to doing so. Conversely, if it is felt that privacy is being infringed upon or there is a desire not to receive mail then the decision should be easily made. It is a situation where both consumers and business achieve their objectives.[71]

8.58 Coles Myer supported the inclusion of NPP 2.1(c) and argued that the principle was important to allowing businesses to grow a customer base by informing potential customers of their products or services.[72] Coles Myer went on to argue that in its view the requirement of giving consumers opportunity to opt-out was a significant protection.[73] It was also pointed out that companies may see a competitive advantage in obtaining consent for direct marketing activity but that, in an internationally competitive environment, this should be a market generated response rather than a regulatory requirement.[74]

Conclusion

8.59 The Committee accepts that the issue of direct marketing is clearly a matter of concern to many members of the community. It is also clear that this issue illustrates the tensions inherent in the balance between the privacy of the individual and the need to avoid placing undue restrictions on business.

8.60 The Committee, despite the sincere beliefs held by many to the contrary, is not convinced that an opt-in approach to direct marketing would be practicable. The Committee accepts that it would be difficult for the majority of businesses to establish systems to enable them to coordinate the sort of information that would be required to determine whether an individual has consented to receiving advertising material.

---

69 Reader's Digest, *Submissions*, p.S262.
70 American Express, *Submissions*, p.S440.
71 Ibid.
72 Coles Myer, *Submissions*, p.S42.
73 Ibid.
74 Ibid.

8.61 In addition, the Committee notes that it appears that the opt-out standard is the generally accepted international privacy benchmark for direct marketing although there are suggestions that electronic direct marketing internationally is moving towards opt-in. An opt-in standard is desirable. However, the Committee was advised that business generally has not reached the stage in its information handling techniques to adequately administer an opt-in regime. While the Committee encourages businesses to voluntarily adopt an opt-in approach, for the purposes of creating a legislative standard to apply across the private sector generally, opt-out is a more appropriate benchmark.

8.62 The Committee is not, however, totally satisfied with the opt-out process set out in the Bill. In the Committee's view the Bill should be clarified to ensure that the opportunity to opt-out of receiving direct marketing material is given on every occasion that material is sent to the consumer, by the same means as the information was sent. The evidence of direct marketers that this would not be appropriate was unconvincing. The Committee can see no reason why the opportunity to opt-out cannot be given repeatedly. The fact that a consumer does not receive or read the first piece of direct mail that they are sent should not deprive them of the choice to prevent further material from being sent.

8.63 Equally, the Committee is not satisfied that the means by which the offer to opt-out is made is adequately addressed by the Bill. The Committee recommends that the Bill contain a set of minimum requirements for the content of the opt-out offer. These minimum requirements are that:

- the offer be prominently placed on the direct marketing material
- be accompanied by a street address and telephone number in Australia;
- be accompanied by an email address if the original communication was made via email; and
- if the organisation sending the material has them, its ACN and ABN numbers.

Recommendation 20

The Committee recommends that the Bill be amended to make clear that every time personal information is used for the secondary purpose of direct marketing the organisation must provide an opportunity for the individual to opt-out of further communications. The offer to opt-out must:

(a) be prominently placed on the direct marketing material

(b) be accompanied by a street address and telephone number in Australia;

(c) be accompanied by an email address if the original communication was made via email; and

(d) if the organisation sending the material has them, be accompanied by its ACN and ABN numbers.

European Union Directive

8.64 In the *Information Paper on the Introduction of the Privacy Amendment (Private Sector) Bill 2000* issued to coincide with the introduction of the Bill in the Parliament, the Government stated that, in developing a system for the fair handling of personal information in the private sector, the Government's intention is to ensure that the scheme is, among other things,

> …compatible with the *European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* to remove any potential barriers to international trade.[75]

8.65 The Information Paper goes on to state that the Bill 'will …provide Australian businesses with certainty when trading with European Union Member States.'[76]

8.66 In his Second Reading Speech the Attorney-General stated that:

> The Bill is intended to facilitate trade in information between Australia and foreign countries. Without such legislative measures, this trade may be adversely affected. The 1995 European Union directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data restricts the transfer of personal information from member countries to other countries unless adequate privacy safeguards are in place. I am confident that this

75 Attorney-General's Department *Information Paper on the Introduction of the Privacy Amendment (Private Sector) Bill 2000*, p.1, *Exhibit 31.*

76 Ibid.

> bill will provide adequate privacy safeguards to facilitate future trade with EU members.[77]

8.67 In its submission to the Committee, however, the European Commission expressed doubt about whether the Bill, as currently drafted, would provide an adequate level of protection for European citizens. The Commission notes in particular that the proposed exclusion of employee data and small business will mean that these sectors cannot be included in any consideration of 'adequacy' for the purposes of the EU Directive.[78] It states that in the event of the Bill being recognised as providing adequate protection by the EU, employee data and small business would be excluded from the decision.[79] The Commission submits that

> In particular, we envisage the exclusion of small business would be problematical, since it would be very difficult in practice to identify small business operators before exporting the data to Australia.[80]

8.68 They go on to state that it is not clear whether small business wishing to import data from the EU can voluntarily adhere to the provisions of the Bill or what other means are at their disposal to provide an adequate level of protection.[81]

8.69 The submission notes many other concerns with the Bill.[82] A major concern is that the Bill, as currently drafted excludes non-Australians.[83] The Commission states that their most important concern in that regard is the protection awarded to EU citizens when their data is exported from Australia.[84] This leads the Commission to cite particular concern in relation to NPPs 6 (Access and Correction), 7 (Identifiers) and 9 (Transborder Data Flows).[85] The submission also states that the exclusion of non-Australians from the protection provided by the Bill means that an Australian company could import data from European citizens and subsequently export it to a country with no privacy laws without the Bill applying. Such a measure would make it possible to circumvent the EU directive.[86]

---

77 Second Reading Speech, House of Representatives, *Hansard*, 12 April 2000, p.15075. See also Explanatory Memorandum.

78 Delegation of the European Commission, *Submissions*, p.S611.

79 Ibid.

80 Delegation of the European Commission, *Submissions*, p.S607.

81 Delegation of the European Commission, *Submissions*, p.S611.

82 Delegation of the European Commission, *Submissions*, pp.S611–613.

83 Delegation of the European Commission, *Submissions*, p.S607. See clause 5 of the Bill.

84 Delegation of the European Commission, *Submissions*, p.S612.

85 Ibid.

86 Ibid.

Conclusion

8.70 Given that one of the aims of the legislation is to enhance the capacity of Australian entities to trade with the European Union, the Committee notes the concerns expressed by the Commission in its submission and suggests that the Government should satisfy itself about the matters raised in the submission.