Privacy Amendment (Private Sector) Bill 2000

Inquiry by the House of Representatives Committee on Legal and Constitutional Affairs

Submission by Australian Privacy Charter Council

May 2000

CONTENTS

The Australian Privacy Charter Council

The Australian Privacy Charter Council was formed in 1992 to promote observance of best practice privacy standards throughout the Australian Community. Under the chairmanship of Justice Michael Kirby, then of the NSW Court of Appeal, the Council brought together privacy, consumer and civil liberties experts with representatives of the business community.

In 1994, the Charter Council launched the Australian Privacy Charter, which is attached to this submission. The Charter sets out 18 principles, reflecting international best practice, which provide a benchmark against which specific proposals for privacy laws and guidelines can be measured. The Charter and its principles are appended to this submission.

The Charter Council continues in existence to promote the Charter and its principles, to comment on privacy initiatives, or the lack of them, in particular sectors and jurisdictions, and to provide a forum for discussion of privacy which brings together representatives from a wide range of interests - non-government organisations, business and government.

Introduction

This submission is largely based on the one made to the Attorney-General's Department in January on its December 1999 'key provisions' paper. Unfortunately, the Bill as introduced has not addressed most of the criticisms that we made in January of the government's proposals.

We have no doubt that statutory privacy protection in the private sector is urgently required. Regrettably the Bill provides only partial and imperfect 'safeguards' as to *how* personal information can be used. The proposed regime has lost most of its other critical function, which is to give individuals more control over *when and if* personal information can be used. In the context of growing business convergence, e-commerce and so-called customer relationship management (often a code term for cross-selling), it is this control function which will increasingly be demanded by consumers.

Our detailed comments and criticisms of the Bill are given below. If enacted unchanged, it would provide an entirely false sense of re-assurance to the Australian public. It would also fail to achieve one of the main objects set out in Clause 3 – "meets international concerns and Australia's international obligations relating to privacy to meet our international obligations". In our view, based on the expert knowledge of several of our members, the Bill will fail to meet the standard of adequacy required by European Union member states for transfer of personal data to other jurisdictions under Articles 25 & 26 of the 1995 Data Protection Directive (95/46/EC).

As a result of the Bill's major weaknesses, it will fail to give consumers and business alike the confidence to use and invest in electronic commerce and service delivery, which we understood to be one of the government's main objectives.

The good work done over the last two years by participants in the Privacy Commissioner's consultation process, and more recently in the Attorney-General's Department's consultations, will have been largely wasted if Bill is enacted in its current form.

The Charter Council urges the Committee recommend the amendments we suggest in this submission. The required changes, most of which would not be opposed by the majority of business interests, could result in legislation which we could all support.

Many of our recommendations and suggestions would have the result of simplifying the legislation. By seeking to accommodate so many special interests, the government's proposed amendments would make the Privacy Act even more complex and hard to understand than it is already. The Bill fails the important test that should apply to all new legislation - that it be simple and easily understood both by those with obligations and those with rights.

We have not dealt with the many areas of the proposed legislation which we support. In focussing on criticisms and weaknesses, we do not wish to overlook the many uncontentious provisions, or the good work done by the Attorney-General's Department and Parliamentary draftsmen in dealing with issues such as the detailed provisions concerning outsourcing; extra-territorial operation, and temporary public interest determinations. Our silence on a particular provision should not however necessarily be taken as support, as we may have missed some adverse implication which others may detect. We will read other submissions with interest and reserve the option of commenting on other aspects of the Bill in due course.

Comments on particular provisions

The practical effect of the legislation will be determined by the combined operation of the principles, the exemptions and the definitions. The Committee needs to ensure that it does not take the apparent superficial meaning of a particular provision at face value, since it may be undermined either by an exemption or by the effect of a definition - some of the terms used in the Bill do not carry their normal meanings.

Employee record exemption

We remain totally mystified as to the logic of the proposed exemption for employee records - the government has produced no evidence or details of the protection that it claims is or will be provided under Workplace Relations legislation. As we have repeatedly stated, the handling of employment records is one of the areas where individuals are most in need of the safeguards provided by accepted privacy principles - given the serious consequences that can flow from inappropriate practices.

However effective the legislation is made in relation to other types of personal information, we will only have 'half a law' if employment records remain exempted.

We acknowledge concerns in the business community about a requirement to give employees access to sensitive human resources information, and some categories of commercial in confidence information. We believe that these concerns have been adequately addressed – to the satisfaction of business representatives - by the Privacy Commissioner in drawing up exemptions to NPP 6. If there are outstanding concerns, we would like to see these spelt out with a view to addressing them by partial exemptions from particular principles.

There can be no justification for exempting employers from unarguable principles such as those relating to data quality (NPP 3) and security (NPP 4). The notice requirements of Principle 1 should also apply – it is difficult to see what possible reason there could be for not telling employees about the extent of monitoring – whether by video or of emails or phones.

Media exemption

Again, while we acknowledge the need for exemptions from some of the principles for the news media, the proposed media exemption (proposed s.7B(4)) is far too broad.

Firstly, it is a serious mistake to try to define the exemption via a definition of journalism that rightly includes reporting etc of 'other information' (definition of journalism and media organisation - items18 &19. This correctly characterises the profession of journalism broadly, but results in the exemption applying to virtually anything that any publisher does. The important issues of freedom of speech and the public interest role of the media are confined to news and current affairs - there is no justification for the exemption extending to so-called 'infotainment' or other forms of publication and broadcasting.

Another danger in the current approach is that any organisation could seek to legitimate a breach of the collection or use and disclosure principles simply by publishing the information, thereby compounding the breach. As an example, the recently launched *Crimenet* web site – a private sector venture which publishes apparently unverified information about alleged offenders - would be likely to fall within the media exemption as currently drafted, thereby escaping from any controls or accountability. So too would the publication last year by a gun lobby magazine of the names and home addresses of politicians favouring gun controls.

While a suitable definition of exempt media activity may be difficult to agree, it is vitally necessary if some of the most scurrilous and intrusive privacy invasive practices 'hiding' behind a media exemption are to be avoided.

One possible partial solution would be to introduce a public interest test whereby news and current affairs providers would have to demonstrate a genuine public interest in the practice concerned in order to take advantage of the exemption.

Small business exemption

It is difficult to see the justification for this exemption other than as a blatant political expedient. Many of the most highly privacy intrusive activities are undertaken by businesses which would almost exclusively fall under any size threshold, let alone the arbitrary and generous $3 million turnover figure used in the Bill. Debt collectors, private investigators, and direct marketers are almost all 'small businesses' and while some of these may be picked up by the 'transfer of personal information' condition (see below) others may not, particularly if they structure their services to deliver 'outcomes' rather than information.

The size threshold is also an open invitation for larger organizations to re-structure their organizations into separate business entities all of which fall under the threshold. The effect of this would be not only to exempt the individual businesses but also to remove any controls over the transfer of personal information between them – for example, a retailer could avoid the application of NPP 2 to direct marketing by splitting its operations into separate 'under $3 million turnover" businesses. In this case, even the 'transfer of personal information' condition would not help, as there would be no transfer – the information would still be within the single 'small business operator' as defined in the proposed section 6D.

The proposed operation of this exemption is also somewhat unclear. "Small business" is defined to exclude organisations holding sensitive data, which seems obtuse, as some small businesses (as the term is normally used) will legitimately hold sensitive data. The exemption then also requires that the small business not "transfer personal information … to anyone else for a benefit, service or advantage." This would seem to ensure that only innocuous activities are exempt, although it should be recognised that the effect will be (rightly) to keep many small businesses under the coverage of the law.

The introduction of the term 'transfer' in this provision (with a different meaning from its use in the transborder data flow principle) is potentially confusing. It may be helpful to clarify that the exemption would not be lost simply as a result of a small business 'disclosing' personal information incidentally as a result of a legitimate activity - eg: to contractors or agents.

The complexity of the formula for the small business threshold (s.6D) with its many conditions, is a recipe for confusion - both for businesses themselves, and also amongst consumers - who cannot realistically be expected to know if a business they are dealing with is covered by the Act or not. Nothing will bring the law into disrepute faster than the many cases in which individuals will make a complaint about an interference with their privacy only to be told that there is nothing that can be done simply because the business concerned arbitrarily qualifies for the small business exemption. For small businesses, the cost of working out whether they are exempt, and of constant monitoring to ensure they stay within the conditions, will surely outweigh the marginal costs of full compliance.

We are sympathetic to the concerns of small businesses about compliance costs, and it is unfortunate that the government's delay in bringing forward legislation means that implementation will overlap the GST introduction. However, overseas experience

shows that the compliance 'burden' associated with the introduction of privacy laws is much less than feared and anticipated.

If the privacy interests of Australians deserve legislative protection, then that protection must apply irrespective of the size of the organisation handling personal information.

Exemption for political activity

This exemption has been introduced at the last minute and has not been subject to any discussion or consultation in the development of the legislation. We challenge the government to disclose the detailed advice it claims to be relying for its claim that subjecting political activity to the privacy principles would infringe an implied constitutional right to freedom of political communication.

Even if there is an overriding public interest in exempting political parties and representatives from some of the principles - such as the collection, use and disclosure principles (which we refute), there can be no good reason for exempting them from the need to comply with the other principles, such as those requiring data quality, openness, security etc. There can also be no objection to the right of access, which becomes all the more important as a safeguard if the effect of some of the principles is limited.

We invite the Committee to consider most seriously the message that the legislation will send to the community if it says, in effect, that most organisations cannot use unfair or deceptive collection practices, or use or disclose personal information in unexpected ways, or keep their opinions about individuals secret; but that it is perfectly in order for political parties and politicians to do all of these things!

Use by related bodies corporate

The National Privacy Principles (NPPs) already had a serious weakness in the wide definition of 'organisation'. This has now been compounded and magnified by the inclusion of a provision (proposed s.13(B)) that expressly allows collection and disclosure between organisations that are 'related bodies corporate' as defined under the Corporations Law.

It is not entirely clear what the effect of this exemption will be - the Explanatory Memorandum and the Attorney-General's Department Fact Sheet suggests that uses and disclosures will still be subject to all the provisions of NPP 2. But if so, it is difficult to see why the related bodies corporate exemption is required and what it achieves (what value is there in sharing without an end-use in mind?). Proposed new NPP 2.3 suggests that the effect of the provision will be to ease the limits that NPP2 might otherwise place on secondary uses such as marketing. We suggest that the Committee might like to explore the intention behind this provision, and its practical effect, in detail.

There is in our view no justification for a broad exemption from the application of any aspect of the collection and use & disclosure principles to transfers of information between organisations simply on the basis of an arbitrary company law association.

The structure of corporate groups is usually quite opaque to consumers and often bears no relation to functions, activities or lines of business.

The basis of the use and disclosure principle is to ensure that only those uses and disclosures that are within the reasonable expectation of individuals are permitted without consent (unless they meet one of the other defined exceptions). To override this presumption in favour of corporate groups being able to internally exchange data at will would fatally undermine the principle.

The use and disclosure principle (NPP 2) should apply unaltered to transfers between different legal entities. If owners choose to take advantage of complex corporate structures for other reasons, they should not gain the incidental benefit of being able to ignore individuals' legitimate and reasonable expectations about privacy.

To give a practical example, many people are concerned about the use of personal information for the purposes of marketing of goods or services that are unrelated to an earlier transaction during which their details were originally captured. The effect of this provision (proposed s.13(B) together with NPP 2.3) may be that many such marketing uses will not even have to pass the (already inadequate) tests included in NPP 2.

Ownership changes

The provisions relating to transitions in partnerships (proposed s.13(C)) seem adequate to deal with changes in ownership, but similar provisions should also apply to changes in ownership of corporations. We had assumed that the normal application of business law would apply to such transitions and that special provisions would not be necessary in the Privacy Act. But if such provisions are included, it should be made clear that successor 'owners' inherit the obligations about use and disclosure that applied to their predecessors, and that they would not be free to redefine the boundaries of use and disclosure without reference to the individuals concerned.

State owned businesses

The Bill proposes to leave coverage of State owned corporations to the discretion of State governments, who can choose to have the federal Act apply to their businesses. (proposed s.6F). (The combined effect of proposed sections 6C(4) and 6F is confusing)

Currently, only NSW has privacy legislation and that law exempts state owned corporations - presumably on the basis of putting them on a equal footing with privately owned competitors. Now that those competitors are to be covered by the federal law, we hope that the NSW government will close the gap, either by extending their own law (the Privacy and Personal Information Protection Act 1998) or by taking up the option of having their own businesses subjected to the federal Act.

Given the slow progress in other States, we would like to see the federal law apply to State owned corporations as the default position, with an option for States and Territories to subject them instead to their own law.

Health information

We do not disagree with the need for special attention to personal health information, but the provisions in the Bill are too generous in relation to management and research uses without consent. We share the serious concerns of the Health Issues Centre and the Consumers Health Forum who have analysed the health provisions in more detail, with expert knowledge, and support their submissions. We have not been able to give these provisions as much attention, but do have the following specific concerns.

The interaction of the various provisions concerning sensitive and health information is quite complex and not easy to fully understand.

In the definitions, it should be expressly stated that health information includes information about an individual's genetic make-up - this is potentially one of the most sensitive pieces of information about someone, and the public will rightly demand that the most stringent privacy principles apply to genetic information.

The definition of health service includes activities "claimed" by the provider to be in the defined categories. If the only use of the definition was to apply more stringent standards the breadth of the this definition would not matter too much, but as the effect is in some cases to give access to more generous use and disclosure rules, extreme care needs to be taken to ensure that only recognised health professionals can take advantage of them.

Principle 2.4 seems extraordinarily complicated to deal with the admittedly important issue of disclosure of health information to carers and relatives. Including such elaborate and prescriptive text in the principles defeats the objective of keeping them concise and easily understood. It should not be difficult to devise a simple 'humanitarian' exemption and leave the detailed interpretation to Commissioner's Guidelines and practical common sense.

We remain concerned that the sensitive information principle (NPP10) applies only to collection. The more restrictive conditions of this principle should apply not only to collection but also to ‘secondary’ use and disclosure of sensitive information collected initially for a bona fide purpose.

Note about ‘related purpose’

The government has accepted the Privacy Commissioner’s advice to vary the wording of Principle 2.1(a) for sensitive (including health) information, which will be required to be ‘directly related’ to the purpose of collection to take advantage of this exception. While we support the intention of this amendment, we are concerned that it might have the unintended effect of lessening the protection offered to all other personal information, which can be used under exception (a) if the purpose is merely ‘related’. Our concerns in this respect are heightened by the suggestion in the Privacy Commissioner’s advice on health information that such uses as management and planning of health care may be regarded as ‘directly related’.

While this is intended to be the subject of further guidelines, we are disturbed by this interpretation. We would argue that many of the ‘administrative’ uses of health

information being discussed are not only **not** 'directly related', they are **not even** 'related'- at least closely enough to gain the benefit of exception (a). It is essential that the statutory regime retains the integrity of the fundamental 'purpose limitation' principle and does not allow too many self-serving uses to be 'authorised' by the necessary related purpose exception.

Fortunately, the other part of the test in exception (a) – that the use be within the reasonable expectation of the individual – should ensure that there is not too much 'creep' towards excessively broad interpretations. But constant vigilance will be required to ensure that the natural tendency of data users to regard most intended uses as 'related' is held in check.

Relationship of Codes to the default statutory regime

While we do not object to the principle of providing an option for Codes of Practice to 'customise' the regime for particular sectors, we have strong reservations about the way in which the Bill provides for Codes as an alternative to the default statutory scheme.

It remains to be seen what demand there is for Codes - it may well be that, as in New Zealand, very few sectors see the value in developing a Code, and are happy to live with the default regime. The Explanatory Memorandum itself points out one of the weaknesses of the approach "For example, different codes nominate various dispute resolution bodies, creating jurisdictional problems and administrative burdens for business." And yet the Bill expressly provides for such different bodies (Code adjudicators).

Codes and Complaint-handling

The Bill appears generally to envisage that a Code will **either** include self contained complaint handling machinery, **or** leave complaint handling entirely to the Commissioner, either under the default statutory scheme, or by appointing the Commissioner as the Code adjudicator, presumably to handle all stages of complaints. However, proposed s.40(1B) (Item 80) appears to envisage a hybrid system, which would allow sectors to initially deal with complaints through an industry body (Code adjudicator), but to refer complex or difficult complaints to the Privacy Commissioner. Such a hybrid arrangement may be very attractive to some sectors and we seek confirmation that this is the effect of Item 80.

Enforcement of Codes

The Bill fails to provide adequate arrangements for the enforcement of codes, and for ensuring consistency of interpretation. As we have argued in earlier submissions, it is essential that there be some formal link between an approved Code and the statutory enforcement mechanisms. Proposed s.18BB(3)(d) (item 58) suggests that a Code adjudicator's decisions will have the same status as those of the Privacy Commissioner in the default scheme. This is given effect by proposed s.55A (item 99) which provides that adjudicators' determinations will be enforceable in the federal court (or magistracy), and we welcome this as a significant improvement over earlier

proposals. However, private sector Code adjudicators are (rightly) not given the same *powers* as the Privacy Commissioner (such as requiring witnesses and information, entering premises and inspecting records), and their effectiveness in investigating complaints may therefore be hindered. (We are alarmed to see that the Commissioner's powers under the default scheme are also to be limited by Item 92 – see below under Commissioner's functions and powers).

The proposed regime appears to assume that most complaints will be resolved through 'friendly' and co-operative discussion. While it is true that the Privacy Commissioner has rarely had to exercise his or her formal powers, the importance of having such powers 'in reserve' should not be underestimated. It should also be borne in mind that to date, the Commissioner has been dealing primarily with Commonwealth agencies and larger credit providers - sectors where a high level of 'voluntary' compliance and co-operation can be expected. Under the wider jurisdiction, the Commissioner, and Code adjudicators to a lesser extent, will face many organisations which are much less inclined to co-operate.

Lack of Appeal rights

The Bill also fails to provide a right of appeal against decisions of Code adjudicators. The ability to enforce a favourable determination in the federal court (or magistracy) is of no value to a complainant whose complaint has not been upheld by a Code adjudicator. Given the unavoidable tendency for industry appointed adjudicators to be influenced by sectoral interests (this after all being the rationale for their existence), it is essential that complainants are able to appeal to a genuinely disinterested person or body if they are dissatisfied with the decision of an adjudicator.

Our other related concern is about consistency of interpretation. Very few privacy complaints can be expected to reach the federal court (magistracy) and this will not therefore be an effective way of ensuring consistency. This is another reason why it is essential in our view that the Privacy Commissioner be given some role in reviewing decisions of Code adjudicators - not necessarily an automatic right of appeal, but at least the ability (discretion) to intervene in significant cases, either as a result of a complainant's request or on his or her own initiative.

Even with the requirement in proposed s.18BB(3)(a)(i) that a Code complaint handling scheme must meet prescribed standards (envisaged as the 1997 Consumer Affairs Benchmarks[1]), we have no confidence, on the basis of self-regulation to date in various sectors, that Code adjudicators left entirely to their own devices will provide individuals with an impartial, fair and consistent judgements on privacy issues, particularly given the necessarily broad nature of the principles.

Ultimate authority to set the privacy standards expected of the private and public sectors alike should reside with one or more independent statutory officers - sectoral bodies appointed by and responsible to businesses in that sector run the constant risk

[1] Benchmarks for Industry-Based Customer Dispute Resolution Schemes, published by the Consumer Affairs Division of what was then known as the Department of Industry, Science and Tourism (August 1997). Stated in Explanatory Memorandum - page 1

of adopting convenient interpretations which favour industry practices over a robust defence of individuals' rights.

Ideally, the decisions *of* the Privacy Commissioner in the default jurisdiction should also be able to be appealed on their merits (not just on points of law).

Modification of the law should be subject to Parliamentary scrutiny

Paragraph 166 of the Explanatory Memorandum confirms that Codes approved by the Privacy Commissioner will not be disallowable instruments. Given the Commissioners' ability to approve not only initial Codes, but also variations and to revoke Codes, which amount to the law for the relevant sector, the safeguard of potential disallowance is essential. Judicial review is no substitute for the ability of Parliament to control the specification of legal obligations.

Definition of personal information

We strongly urge that the definition of personal information be modified to *include* 'potentially identifiable' information (as the current Privacy Act definition does), but should not continue to *exclude* information in a generally available publication.

Many of the recent privacy controversies, concerning collection of information on-line, have revolved around the collection of e-mail addresses or IP addresses, which can either be used to communicate directly with a person or can be subsequently matched with other information to add to a profile of a particular individual.

However, it is arguable that an email address or IP address is not 'personal information' as defined in the legislation, as they do not unambiguously identify an individual. The same applies to telephone numbers, even though these are routinely used as a surrogate identifier for either the subscriber to the line, or a regular user.

It is essential that the definition of personal information is clarified, to put beyond doubt that it applies to such 'indirect identifiers' and to the information collected and held in association with them. One way of doing this would be to adopt the definition in the UK Data Protection Act, which includes "identified from the information itself or from other information in the possession of the data user".

The definition of health information relies on the definition of personal information and is therefore subject to the same limitation. This weakness is especially worrying in the health context, in that it would potentially exclude information from which names or dates or birth had been removed, even if other information in the possession of, or easily obtained by, the data user could, in combination with the 'de-identified' data, readily identify individuals.

Generally available publications

The existing Privacy Act regime already contains the weakness of an unjustifiable exclusion for information in a 'generally available publication'. This occurs because of the interaction of the definitions of "personal information" and of "record". The Bill fails to take the opportunity to simplify the way the Act works by removing

intervening concept of 'record' - we have long argued that 'Plain English' legislation would simply subject any handling of personal information to the Principles.

The Bill compounds the exemption by adding 'however published' to the definition of a generally available publication. It has never been clear if the effect of the exclusion is to exempt only a generally available publication itself, or the information contained in a generally available publication. The Attorney-General's department argued for the latter view in relation to Telstra's application for a public interest determination in 1990-91, but the then Commissioner took the former view in his Determination[2]. It would be helpful to put the former view beyond doubt, and at the same time to review the intention and practical effect of the provision.

We agree that published information (including public register information) needs some special rules, but there is no need or rationale for excluding information from the application of the principle simply because the same information is also published - in the private sector context there is also the possibility that an organisation might seek to legitimise a clearly undesirable practice by publishing the personal information concerned, thereby gaining the benefit of this exemption (and also perhaps the media exemption - see above).

These are fundamental issues and it is a major weakness of the Bill that it stands by the narrow definition of personal information, and does not deal at all with the related issue of protection for public register information.

Outsourcing

The Bill generally deals well with the issue of outsourcing. But the further delay of 12 months before the provisions take effect is unacceptable. We have consistently argued for the re-introduction, passage and implementation of the Privacy Amendment Bill 1998 which would have had the same effect. With major data processing and other functions of government due to be contracted out over the next year, further delay is inexcusable. Unless the government is prepared to freeze any further contracting out until the new legislation is in place and operational, the 1998 Bill should be passed as soon as possible to ensure that Australians do not continue to lose the limited privacy protection that they currently enjoy. Alternatively, the new Bill could provide for the law to apply to contractors to Commonwealth government agencies immediately.

The longer term issue of harmonising private and public sector regimes is discussed further below.

There is one particular issue relating to contracting which we do not fully understand. Proposed s.6A(2) (and Item 37) appear to allow Commonwealth agencies by contract to authorise acts and practices which would otherwise be a breach of the NPPs - we assume that this is only to ensure that the IPPs in the existing Act continue to prevail? We would like to see this confirmed. (see also comments below about harmonisation).

[2] Public Interest Determination - Application No 6, September 1991

Scope

We welcome the provisions in Item 42 for reviewing the existing exemptions for certain government agencies and business enterprises imported from the FOI Act. We would however like to see the agencies and activities to be brought under the NPPs specified in the Act rather than left to regulations. There will no doubt be vigorous rearguard actions fought by currently exempt government entities in an attempt to avoid prescription.

We are not sure if the effect of Item 42 is confined to commercial activities. If so, then there should also be a review of some of the other exemptions in the FOI Act schedules, which appear to have been the arbitrary outcome of successful lobbying rather than of any reasoned justification.

Rights of non-residents

We note that the legislation re-affirms the limitation on correction rights only to Australian citizens and permanent residents (item 87, amending s.41(4)). This is a major flaw that will clearly contribute to the Bill failing to meet the European Union's 'adequacy' test. The whole point of the EU 'overseas transfer' provisions is to try to ensure that EU citizens can take advantage of similar privacy protection wherever in the world their information is transferred. Limiting the jurisidiction of the law, in respect of correction rights, to Australians does not make sense in this context and there are no apparent benefits.

We note that the New Zealand Privacy Commissioner, in his recent review of the New Zealand Privacy Act 1993, recommended extending all of the rights under that Act to non-residents as one essential amendment to ensure the law is acceptable to the EU and other jurisdictions (such as Hong Kong) with overseas transfer provisions.

The National Principles

We have some significant concerns about the Privacy Commissioner's National Principles, as incorporated into the legislation. The Principles represent the Commissioner's best efforts rather than a consensus between the parties involved in the consultations. Apart from the matter of Principle 10 already mentioned above, we have concerns about the following:

- The ambiguity of the application of Principle 2 to direct marketing. 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 to give individuals a choice in most circumstances as to whether they continue to receive unsolicited communications from organisations about goods and services other than those they have already contracted.
  It is particularly important that direct marketing by e-mail, and arguably also by telephone and fax, is only permitted on an opt-in basis, because of the additional intrusion, and often some cost to the recipient. This standard has already been

accepted for e-mail by the Internet industry in their Code of Practice[3] and it would be very undesirable for the legislation to undermine this initiative by legitimising a lower standard.

- The anonymity principle (NP8) is being misinterpreted in some sectors as imposing unrealistic restrictions. It is important in our view to incorporate into the principle itself some reference to pseudonymity, which is likely to be a common means of implementing the intention of the principle, as a complement to genuine anonymity in as many circumstances as possible.

- The second part of the identifiers principle (NP7.2) does not apply if many of the exceptions to NP 2 apply. This leaves too much scope for organisations to construct reasons of their own for using and disclosing 'official' identifiers. We think the principle underlying this protection should be clearly stated as restricting use and disclosure of identifiers to purposes which have been expressly sanctioned by law.

- The correction principle (NP 6.5-6.7) should also include an obligation to take reasonable steps to communicate corrections to anyone to whom the original uncorrected information has been disclosed. This is a common feature of overseas privacy laws and is also found in the New South Wales Act (section 15(3)).

- It is regrettable that the Bill has dropped some important explanatory notes from the National Principles - in particular the reminder that accompanied NPP2 that nothing in the Principle prevents an organisation from insisting on a legal authority for disclosure. All the various exceptions in NPP2 except 'required by law' are permissive, not mandatory, and organisations need to be re-assured that in difficult circumstances which will occasionally arise, they can protect an individuals privacy up to the point where they are served with some legal instrument requiring them to disclose personal information.

- National Privacy Principle 6.1 (k) provides that an individual may be denied access to his or her personal information where an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia. This is in our view an unnecessary hangover from an earlier version of the NPPs where this clause also applied to intelligence agencies. There is no definition of 'lawful security function' and enforcement agencies, as defined, do not include intelligence agencies. An exception from subject access may well be necessary, but should be more narrowly defined and explained (see also comments below about Schedule 3).

Other new elements to the principles

Since 1994, the Australian Privacy Charter, devised and now promoted by the Council, has espoused several principles which go beyond the limited, though valuable framework of the OECD guidelines. Some of these principles deal with aspects of privacy other than information privacy. Since the current proposal only

[3] Internet Industry Association Code of Practice v5 -

purports to deal with information privacy, we will reserve our position on these other aspects of privacy for other forums.

There are however three principles in the Charter which are relevant to information privacy but which are missing from both the government's proposals and from the existing Privacy Act. Charter Principles 1 ('prior justification') and 18 ('no disadvantage') can often be effectively argued in the context of particular privacy intrusive initiatives. It would however be desirable to have both these principles enshrined in legislation to lend support to the Privacy Commissioner's 'watchdog' role.

The best way of implementing the 'prior justification' principle would be through a requirement for privacy impact statements for proposals (whether in the private or public sectors) which met certain criteria for potential privacy intrusion. There is already a precedent for such statements in Commonwealth law – the program protocols required under the Data-matching Program (Assistance and Tax) Act 1990.

Consideration should be given to including in the Bill a requirement for privacy impact statements in appropriate circumstances.

The 'no disadvantage' principle is becoming increasingly important as individuals are faced with the offer of goods and services on favourable terms on condition that they waive some privacy rights (usually the right to prevent secondary uses and disclosures). In order to ensure that individuals are not put under pressure to 'sell' their privacy, this principle needs to be enshrined in law so that it is able to be invoked against unreasonable 'contractual' waivers of privacy.

Charter Principle 7 deals with public register privacy. This is a complex issue which deserves separate consideration, as it receives in many overseas privacy laws. It is also related to the definition of personal information and the inclusion or exclusion of material in 'generally available publications' discussed above (see under Definitions).

Retrospectivity

The proposed section 16C disapplies Principles 1, 2, 6, 8 & 10 from information collected, or transactions entered into, prior to commencement. While this is sensible for Principles 1 and 10, there is no reason why organisations should not be required to use best endeavours to comply with at least the spirit of Principles 2, 6 and 8 in respect of information already held, accepting that it would be unreasonable to enforce the same standards as would apply to information collected subsequently. Experience overseas suggests that many organisations will in any case find it easier to apply the same regime to all data than to make an administrative distinction.

Timing

The twelve month delay after Royal Assent before organisations are required to comply with any of the NPPs (cl.2), and the further twelve months grace for small businesses in respect of some principles (proposed s.16D), are an unnecessarily long phasing in period. The principles are well known and understood by many larger

businesses, and relatively easy for smaller businesses to come to terms with and implement.

While a shorter phased introduction for mandatory compliance with some of the principles is acceptable, there is no reason why the Privacy Commissioner could not be given the power to investigate complaints during Stage One, albeit without the power to find breaches of the principles or award remedies. A recommendatory ombudsman role during this stage would complement the educational and promotional roles, and would help to ensure that organisations took their responsibilities seriously as they prepared for full implementation. Without it, it will be difficult to generate public interest in the new rights.

We therefore urge the Committee to recommend an earlier commencement, with only delayed application of selective provisions where a strong case can be made.

Functions & Powers of the Privacy Commissioner

One important function under the existing Act which is not extended to the new private sector/NPP jurisdiction is the audit power (s.27(1)(h); 28(1)(e) and 28A(1)(g)-(j)). There is no good reason why the Commissioner should not be empowered to conduct audits of compliance with the NPPs, and every reason why he should. While the number of audits conducted by the Commissioner in the tax file number and credit reporting jurisdictions has been modest, it has over the years built up into a very useful 'sample' of compliance.

The existence of the audit function sends a message to organisations that they cannot just take the risk of doing nothing with the only 'threat' being the receipt of a complaint. It is the nature of many privacy breaches that the individuals affected may not become aware of the breach, or be able to trace an adverse consequence back to a privacy compliance issue. The Australian Privacy Act has been one of only a few laws, internationally, to include a significant pro-active audit role for the Commissioner and as such it is widely admired.

We strongly urge the Committee to recommend the extension of the audit function to the new private sector jurisdiction.

The government also proposes to disapply the Commissioner's powers to direct persons to attend a conference from NPP complaint cases (proposed amendment to s.46(1) (Item 92). We can see no reason for so limiting the Commissioner's powers in this way, While the power has rarely been used in the existing jurisdictions, it is a necessary and desirable tool to support the authority of the Commissioner.

Relationship between private and public sector schemes

It is clearly not intended to significantly amend the existing regime of Information Privacy Principles applying to Commonwealth agencies. Given the increasingly blurred distinction between public and private sectors, it would be unfortunate if the government left the Australian community with two different regimes other than as a short term expedient. Harmonisation was one of the recommendations of the 1998 Senate Committee report.

The Charter Council acknowledges that any change to the public sector regime would require further consultation with Commonwealth agencies and representatives of affected individuals and third parties. It is understandable, and desirable, that the need for such consultation should not hold up the implementation of a private sector scheme. The Council therefore supports the early passage of the Bill (subject to the many amendments suggested in this submission) to implement a private sector scheme.

The government should however also commit itself to a firm timetable for review of the existing public sector regime, with a view to bringing the IPPs in section 14 of the Act into line with the private sector principles. Contrary to a commonly held belief, the National Principles developed by the Privacy Commissioner, which are to form the basis of the private sector scheme, were not designed exclusively with the private sector in mind. The fact that they were adopted by the previous Victorian government for application to its State public sector bears this out. We also disagree with the claim in the Explanatory Memorandum that the IPPs set a higher standard than the NPPs - this may be true in some respects but in others the NPPs were deliberately designed to address some of the weaknesses of the IPPs (such as the exemption for disclosures simply on the basis that individuals had been notified (IPP11(1)(a)).

The review of the public sector principles should also include consideration of the relationship between the access and correction provisions of the Commonwealth Freedom of Information Act 1982 and of the Privacy Act. A government response to the recommendations of the joint ALRC/ARC report in 1995 on the FOI Act is long overdue. In the Charter Council's view, there is a strong case for transferring the access to personal information provisions of the FOI Act to the Privacy Act, leaving the FOI Act to emphasise openness and access to government information. There would need to be close co-operation between the Privacy Commissioner and the agency responsible for implementing the FOI Act (an Information Commissioner?). There would also need to be further consideration given to the definition of personal information and its application in FOI and Privacy contexts.

Amendments of other Acts

Schedule 2 contains proposed amendments to other Acts consequential on the introduction of the private sector privacy regime.

The amendments to the *Customs Act* seem appropriate although it is odd that Customs have been singled out – are there not other Commonwealth agencies whose authority to request information (as opposed to requiring it) is uncertain? And why is Customs not adequately covered by the exception for enforcement bodies in NPP 2.1(h)?. We note that that explanatory memorandum makes it clear that the new section of the Customs Act does not require persons to give information – it simply ensures that if they choose to do so in response to a request, they are not in breach of NPP 2.

We note the argument in the Explanatory Memorandum that the *Telecommunications Act* regime needs to continue in place because of the value of a reserve power (of the ACA) to require the production of a Code of Practice.

> "it is useful to retain this power as it is not possible to foresee all eventualities. This power may also provide a useful goad to industry to act under the Privacy Act". (paragraph 385(a))

We wonder why this logic has not been extended to other sectors and a similar power given to the Privacy Commissioner to initiate a Code (as is the case under the New Zealand Act).

Disclosures to intelligence bodies

Schedule 3 provides for disclosures to intelligence bodies to be now to be dealt with exclusively by amendments to the *ASIO Act* rather than, as in the National Privacy Principles, in the use and disclosure principle. This will have the effect of 'masking' the actual availability of the exemption, which will no doubt only be pointed out to organisations as and when an intelligence agency needs to seek personal information. There are strong accountability arguments for putting the exemption 'up front' in the Privacy Act where it can be seen and widely understood. On the other hand, the exemption will hopefully only be required rarely and in relation to very few organisations, and it may be argued that it is better not to 'clutter up' what should be simple and easily understood principles (see elsewhere for our general view that the Bill has in any case failed to meet this objective). It could be argued that this is simply one of a large number of 'special cases' where particular disclosures are authorised or required by other laws – covered generically in the Privacy Act by NPP2.1(g).

Our other concern about the intelligence agency exception is the failure to provide for a record to be kept by organisations of such disclosures - similar to the requirement applying to law enforcement exceptions (NPP 2(2). While it would clearly be appropriate for such records to be kept secure and confidential, the absence of any record, reviewable by an independent officer such as the Privacy Commissioner or Ombudsman (or perhaps the Inspector General of Intelligence and Security) is an open invitation for abuse. While the intelligence agencies themselves may be accountable (through the Inspector-General) for their use of the exception, what is to stop other organisations (such as private investigators, or police forces) from purporting to be an intelligence agency in order to obtain personal information to which they would not otherwise be entitled?

* * *

Submission ends

Nigel Waters
Convenor, Australian Privacy Charter Council
12A Kelvin Grove, Nelson Bay, NSW 2315
E-mail: nigelwaters@primus.com.au
Telephone 02 4981 0828 or 0407 230342

Appendix

The Australian Privacy Charter

The Meaning of Privacy

Australians value privacy. They expect that their rights to privacy be recognised and protected.

People have a right to privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person), and freedom from surveillance.

'Privacy' is widely used to refer to a group of related rights which are accepted nationally and internationally. This Charter calls these rights 'privacy principles'.

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

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

Privacy is important

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

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

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

Interferences with privacy must be justified

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

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

Aim of the principles

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

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

Privacy Principles

1. Justification and exceptions

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

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

2. Consent

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

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

3. Accountability

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

4. Observance

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

5. Openness

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

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

6. Freedom from Surveillance

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

7. Privacy of Communications

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

8. Private Space

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

9. Physical Privacy

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

10. Anonymous Transactions

People should have the option of not identifying themselves when entering transactions.

11. Collection Limitation

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

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

12. Information Quality

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

13. Access and Correction

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

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

14. Security

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

15. Use and Disclosure Limitations

Personal information should only be used, or disclosed, for the purposes specified at the time of collection, except if used or disclosed for other purposes authorised by law or with the meaningful consent of the person concerned.

16. Retention Limitation

Personal information should be kept no longer than is necessary for its lawful uses, and should then be destroyed or made anonymous.

17. Public Registers

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

18. No Disadvantage

People should not have to pay in order to exercise their rights of privacy described in this Charter (subject to any exceptions), nor be denied goods or services or offered them on a less preferential basis. The provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost.