Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Implementing privacy principles: After 20 years, its time to enforce the *Privacy Act*

Submission to the Australian Law Reform Commission
on the Review of Privacy Issues Paper

Graham Greenleaf, Nigel Waters & Lee Bygrave*

Graham Greenleaf
Professor of Law
University of New South Wales

Nigel Waters
Principal Researcher, Interpreting Privacy Principles Project
Cyberspace Law & Policy Centre, UNSW Faculty of Law

Lee Bygrave
Associate Professor, Department of Private Law
University of Oslo
Visiting Fellow, Faculty of Law, University of New South Wales

31 January 2007

Research for this submission is part of the Interpreting Privacy Principles Project, an Australian Research Council Discovery Project

* We would like to thank Matthew Lee and Abi Paramaguru, Research Assistants on the *Interpreting Privacy Principles Project*, who have helped develop the Privacy Law Library we have used for research on the submission; Abi also for assisting with references; AustLII Executive Director Philip Chung for supervising the development of the Library; and David Vaile, the Project's Manager.

Contents

Introduction

Structure of Submission

This submission follows the order of chapters in the *Issues Paper*. Where we do not wish to make a submission at this stage on a question, or a Chapter, or have been unable to do so in time for the completion of this submission, we have deleted the question or Chapter. Otherwise, to increase the utility of this submission to the ALRC and others, the order of questions asked in the Issues Paper has been followed for the most part. However, it was difficult to do this in relation to Chapter 4 on privacy principles, because more detail was required, so those submissions are not strictly in the order of questions asked. However, there is a consolidated list of submissions made at the end of the submission. Where we wish to raise issues that do not seem to be covered by any of the questions asked, we have listed them following the most relevant question and using its numbering.

We have not made submissions on quite a few of the Chapters of the Issues Paper, not because of their lack of importance but because we have limited ourselves to those Chapters where we were able to provide support and argument for the submissions made. We are otherwise in general agreement with the submissions made by the Australian Privacy Foundation, to which we contributed, and by Lee Bygrave in his earlier submission on a number of issues.

Background – the iPP Project

Research for this submission has been undertaken as part of a Discovery project funded by the Australian Research Council, 'Interpreting Privacy Principles'. The home page for the project, and other publications relating to the project, are at <http://www.cyberlawcentre.org/ipp/>The *iPP Project* is based at the Cyberspace Law & Policy Centre at UNSW Law Faculty. The principal objective of this research is to conduct over the course of the project (2006-09) a comprehensive Australian study of (i) the interpretation of information privacy principles (IPPs) and 'core concepts' in Australia's various privacy laws, particularly by Courts, Tribunals and privacy regulators; (ii) the extent of current statutory uniformity between jurisdictions and types of laws, and (iii) proposals for reforms to obtain better uniformity, certainty, and protection of privacy.

Concerning the first element, a small but rapidly growing body of cases has developed in Australia over the last few years. Around a hundred Tribunal decisions, a similar quantity of mediated complaint summaries, and relatively small number of relevant Court decisions have become available. There has been little systematic analysis of this material. The relative scarcity of Australian interpretative materials means that the objective necessitates consideration of the interpretation of similar IPPs and core concepts in the privacy laws of other Asia-Pacific countries (particularly New Zealand, which has the largest quantity of reported cases) and European jurisdictions. The iPP Project, as it develops this analysis, will aim to make further inputs into the ALRC's review and similar privacy reform projects at State level.

General considerations

In developing this submission, we have been influenced by a number of general considerations. First, while the Privacy Act can be improved considerably, more effective enforcement of the Act's provisions is needed as much as reforms to the Act itself – hence the title of this submission. Any reforms to the Act must improve its enforceability and responsiveness as regulation, or they will be a waste of time.

Second, consistency with international standards for privacy protection is a desirable goal for Australia's privacy laws, as with other areas of regulation of activities which cross national borders, provided this is also consistent with Australian interests.. For this reason we have examined wherever appropriate the extent to which the Privacy Act and its enforcement seems consistent with

this international standard. These standards, and the approach that Australia should take to them, are discussed at the start of Chapter 4, and again in Chapter 13.

In this submission we have not yet taken into account in any detail the recently revised Guidelines by Privacy Victoria to the IPPs made under their legislation in 2006[1]. We would like to draw this very valuable source to the ALRC's attention.

The ALRC Review is still at an early stage, as is the iPP Project. Some of our submissions are recommendations that the forthcoming Discussion Paper canvasses particular issues, rather than stating any concluded view of our own on those issues.

Terminology

In this submission, we have used the following terms:

- *'Data user'* is used to mean both (government) agencies and (non-government) organisations under various Australian privacy laws. Where we are talking about either or both, this avoids the need to say 'agency or organisation'. Where the distinction is significant for our comments, we revert to the separate terms.

- *'Data subject'* is used to mean the individual to whom personal information relates. This avoids the need to use this convoluted wording to distinguish the data subject from other individuals.

These two terms are used in European privacy or 'data protection' laws. By using them as shorthand in this submission, we do not mean to suggest that they be adopted in Australian legislation – they carry an undesirable implication of limitation to computerised information, and the broader concept of 'personal information' is preferable to 'personal data'. The ALRC may wish to canvass views about whether a hybrid term such as 'information user' might be desirable in the context of a single set of principles (see below).

- *'Privacy Commissioner'* is used to refer to the Australian Commonwealth (Federal) Privacy Commissioner unless preceded by another jurisdiction label e.g. 'NZ Privacy Commissioner' or 'Victorian Privacy Commissioner'.

- *'NPPs' and 'IPPs'* refer to the relevant Commonwealth principles. In discussing privacy laws, it is easy to confuse the different acronyms. In this submission, we use NPPs and IPPs on their own to mean the two sets of principles in the Privacy Act 1988. Where we refer to other sets of principles we preface them with the jurisdiction e.g. Victorian, NSW or NZ IPPs. We also use the generic term 'privacy principles' or just 'principles' where appropriate, and in the context of this submission those terms will always mean *information* privacy principles.

References used in Submission

Where this submission draws on previous publications and submissions by any of us, we have referred to those earlier publications by notes in the text. We request that the earlier publications or submissions as well as the current submission be cited where appropriate, to make it clear that much of the argument about the deficiencies of the Privacy Act has been known for many years.

---

[1] Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles*, edition.02, September 2006.

Overview of privacy and the Act (Chs. 1-3)

Action for breach of privacy

> *1–2 Should a cause of action for breach of privacy be recognised by the courts or the legislature in Australia? If so, and if legislation is preferred, what should be the recognised elements of the cause of action, and the defences?*

Whether a cause of action for breach of privacy should be recognised by the Courts is something about which it is irrelevant to speculate and pointless to wait for resolution, which could take another 50 years. Consideration of the justification for a statutory privacy tort is independent of this question.

A statutory privacy tort is desirable because of the inadequacy of other tortious and equitable remedies. The elements of such a tort are to be addressed by the NSW Law Reform Commission, and we will not discuss them here. A useful guide to the potential elements of such a tort are the provisions recommended by the Hong Kong Law Reform Commission.

> ***Submission 1-2: A statutory privacy tort is desirable because of the inadequacy of other tortious and equitable remedies. A useful guide to the potential elements of such a tort are the provisions recommended by the Hong Kong Law Reform Commission.***

> *Where should the cause of action be located? For example, should the cause of action be located in state and territory legislation or federal legislation? If it should be located in federal legislation, should it be in the Privacy Act or elsewhere?*

Given that the Commonwealth has asserted constitutional power in relation to the protection of privacy in the private sector, it may be consistent with this for the Commonwealth to also legislate, in the Privacy Act, for a statutory tort or torts to protect other aspects of privacy in relation to the private sector. It will be necessary to carefully align the elements of a statutory privacy tort with what is already protected by privacy principles. If this approach is adopted, it would start to resemble a comprehensive privacy code such as is attempted in the Asia-Pacific Privacy Charter.

The danger of this approach is that, since it will also overlap the regulation of surveillance activities, it could easily be used to diminish the ability of States and Territories to apply higher standards of protection against surveillance activities in the private sector than the Commonwealth is willing to provide. National consistency is preferred here, but not by Commonwealth *fiat* prohibiting higher standards at State level.

> ***Submission 1.2.1: The preferable location for such statutory privacy torts, insofar as they apply to the private sector, is the Privacy Act. Such legislation should preserve the right of States or Territories to enact higher standards of privacy protection. At the same time, national consistency by agreement should be sought.***

National consistency

> *2–1 Is national consistency in the regulation of personal information important? If so, what are the most effective methods of achieving nationally consistent and comprehensive laws for the regulation of personal information in Australia?*

Consistency is a valuable objective, but should not be pursued to the detriment of the level of protection. Levelling down to the lowest common denominator of State or Territory willingness to protect privacy is undesirable. It would also not be desirable to have a referral of powers, leaving only a federal law. At least where there are separate fields of activity being regulated, such as the activities of the various public sectors, to have several privacy regulators is a healthy way to ensure

that different standards of performance of regulators can be compared, and to observe the effects of different regulatory arrangements and learn from them.

> ***Submission 2-1: National consistency is a valuable objective, but should not be pursued to the detriment of the level of protection. Agreement on model or uniform laws to be implemented in all jurisdictions would be the best way forward, at least in regard to the various public sectors.***

Important aims in reform of privacy laws in addition to national consistency are discussed at the start of Chapter 4 concerning privacy principles. They include the desirability of international consistency, and reasons why privacy principles may have fallen below community expectations.

Structure of the Privacy Act 1988 (Cth)

> *3–1 Is the structure of the Privacy Act logical? Does the Privacy Act need to be redrafted to achieve a greater degree of simplicity and clarity?*

It should be possible to simplify the Act. Some of the definitions and their interaction with the application provisions and exemptions are particularly opaque. Only one set of principles should apply to both private and public sectors. Although there is justification for some specific sectoral rules (eg for credit reporting and TFNs), it is preferable if there is only one 'core' set of privacy principles, plus a set of specific legislative variations of those principles to the extent needed for special sectors.

> ***Submission 3-1: The Act should be simplified by providing one 'core' set of principles applying to both the private sector and the (Commonwealth) public sector. To the extent that there needs to be special sub-sectoral rules, they should be be legislative exception to the 'core' set of principles.***

> *3–2 Insofar as the Privacy Act is primarily concerned with data protection, is the name of the Privacy Act accurate and appropriate?*

'Data protection', though used in Europe and elsewhere, is not familiar to the public in Australia and runs the risk of misleading. The law is not and should not be just about computerised information, and 'data protection' also reinforces the unfortunate perception that it is just about security.

> ***Submission 3-2: 'Information Privacy Act' (as in Victoria) would be a better name, given the current scope of the Act. However, if the scope of the Act is broadened to make it more comprehensive (eg include privacy torts), then 'Privacy Act' is appropriate.***

We acknowledge that the ALRC has chosen to focus primarily on information privacy, and to a lesser extent on communications privacy (paragraph 1.89). However, we note that the terms of reference are not so restricted, being as broad as 'an effective framework for the protection of privacy in Australia'. We submit that the ALRC should either separately review wider aspects of privacy such as bodily and territorial privacy and surveillance, or recommend to the government that this wider review be conducted as a subsequent exercise. Such a review should address the desirability of a general presumption in Australian law against unreasonable search and seizure, as embodied in the Fourth Amendment to the US Constitution. The Asia-Pacific Privacy Charter is one attempt to develop such a comprehensive code (see Greenleaf and Waters, 2003).

> ***Submission 3-2.1: The Discussion Paper should consider whether a more comprehensive legislative code is desirable to cover all aspects of privacy, including bodily and territorial privacy and surveillance as well as information privacy.***

Privacy principles - Threshold issues (Ch 4)

The ALRC's questions 4-34 to 4-36 should be answered before those on the individual principles.

Specificity of principles

> *Q4–36 asks 'Should federal privacy principles be prescriptive or should they provide high-level guidance only? Should they aim for a minimum or maximum level of protection of personal information or aim to adopt a best practice approach?'*
>
> ***Submission 4-36: The starting point is that it is desirable to adopt principles (i) which are consistent, at least within Australia, and (ii) which represent best practice in terms of promoting internationally accepted privacy standards.***

Comparative study of the different formulations of the principles, and of the way in which they have been interpreted, should be used to 'level up' or raise standards, where doing so can be demonstrated to strengthen the effectiveness of the principles. Weakening or 'levelling down' should only be accepted if there is clear evidence of a particular standard being unworkable in practice or demonstrably inefficient (e.g. by imposing significant compliance costs for little benefit).

Uniform principles

> *Q4–34 asks 'Should the Privacy Act provide a uniform set of privacy principles that are to apply to both the public (currently covered by the IPPs) and private (currently covered by the NPPs) sectors? If so, what model should be used? Are there any particular principles or exceptions to principles that should apply only to either the public or private sector?'*
>
> ***Submission 4-34: There should be a single set of principles to apply to both Commonwealth agencies and private sector businesses (and ideally to all State and Territory public sector agencies and to all other organisations including those currently exempt from any of the existing laws). We submit that there are no particular principles that should apply only to either the public or private sector, but that there are exceptions which will be more or less relevant to different sectors. As argued above, there is no single existing model which should be preferred as all have been shown to have weaknesses – a new set of common principles should be derived from analysis of the various precedents. In some cases the resulting principles will be very close to the existing NPPs or IPPs, thereby minimising any adjustment of compliance requirements.***

The question of additional principles (Q.4-35) is addressed separately below.

International consistency

Australia's interests in the better protection of human rights, and in the facilitation of the free flow of personal information between countries consistent with privacy protection, will be advanced if it is possible for Australia's privacy laws to be consistent with the privacy laws of as many other countries as possible. This can be achieved to some extent by consistency with the main international privacy agreements.

Three such agreements are of particular significance to Australia, and we will set out briefly our views concerning them:

- *The European Union's privacy Directive* – The standards on which the Directive is based have been implemented (however imperfectly) in legislation by more countries than any other privacy standard. While they do embody the highest standard of privacy protection of any international agreement, they are only modestly in advance of Australia's existing privacy legislation, at least in relation to those aspects of the European standard that seem to be regarded as most important to the notion of 'adequacy'. Consistency between Australian and European privacy standards is therefore quite a realistic goal. This submission therefore discusses differences between this European standard and current Australian legislation in some detail, to help identify these differences.

- *The OECD's privacy Guidelines* – The Privacy Act probably implements what the Guidelines require, as they are a modest set of requirements now over twenty years old. However, other than in relation to a more prescriptive approach to data exports, along with provision for special safeguards on sensitive data, the Council of Europe's privacy Convention requires legislation of a standard broadly similar to that required by the OECD guidelines. In our submissions on Chapter 13 we also refer to the Council of Europe's privacy Convention, and submit that consideration should be given to Australia becoming a party to that Convention, as a means of facilitating transfers of personal information with a high standard of privacy protection between Australia and European countries, potentially some APEC countries and some other countries such as South Africa which are neither European nor in APEC.

- *The APEC Privacy Framework* – The APEC Privacy Framework is largely irrelevant to the further development of Australian privacy standards because we already implement a higher standard. The APEC Framework is the weakest of all international privacy standards to date (Greenleaf 2005, 2005a, 2006). Its wording in a number of places may be worth consideration, and that is noted where relevant. Its standards are 'a floor not a ceiling', and any APEC member is able to have higher standards (Greenleaf 2005).

Submission 4-34.1: Wherever possible and consistent with Australian interests, Australian privacy principles should be consistent with the main international privacy standards, of which the three most important instances for Australian interests are the European Union's privacy Directive, the OECD's privacy Guidelines and the APEC Privacy Framework.

In addition to these agreements, the Issues Paper notes at [13.86]-[13.90] that the Asia-Pacific Privacy Charter provides another standard to which Australia's privacy laws may be compared, a 'high water mark' synthesis of privacy principles emerging primarily from the strongest aspects of existing privacy laws in the Asia-Pacific region. We refer to the Privacy Charter where appropriate, as we consider it is more useful, for Australia's purposes, than the 'low water mark' of the APEC Privacy Framework, which is a standard that Australian privacy protection already exceeds.

Reasons for reform of information privacy principles

There are additional general reasons why there is a need for reform of information privacy principles.

Submission 4–34.2: There are three reasons, apart from the important objective of consistency, why the information privacy principles in Australian Privacy Laws may need to be revised: (i) where a principle as currently legislated clearly falls short 'on its face' of meeting community expectations; (ii) where the practice of government agencies or businesses in complying with the principle have exposed shortcomings; and (iii) where courts or tribunals have 'read down' the meaning of a principle (often

> ***in conjunction with interpretation of core concepts) so that it does not in law have the anticipated effect.***

The first is where a principle as currently legislated clearly falls short 'on its face' of meeting community expectations. This may in turn be either because it was never adequate – most often because of compromises to meet government or business efficiency objectives – or because community expectations have become clearer.

The second reason for reform is where the practice of government agencies or businesses in complying with the principle have exposed shortcomings – i.e. where the principle has not operated as anticipated. To some extent this category of failure could in theory be addressed by the exercise of discretion by the regulator, but the history of privacy law in Australia is mostly of timidity on the part of Privacy Commissioners both in interpreting principles and of enforcing their interpretations. While more effective privacy protection could be achieved by more assertive regulation, this is an unreliable solution and some reform of the principles themselves will in some cases be a more satisfactory approach.

The third reason is where courts or tribunals have 'read down' the meaning of a principle (often in conjunction with interpretation of core concepts) so that it does not in law have the anticipated effect. The role of the judiciary is properly to decide what the law actually says and requires – informed to some extent by the legislative intent as expressed in Explanatory Memoranda and second reading speeches. It is not the role of the courts to decide whether the statutory principles as enacted strike the right balance in terms of community expectations – that is ultimately the prerogative of legislatures. But we submit that it is an important objective of the ALRC review to make recommendations directed to meeting community expectations in light of experience.

We acknowledge that all three of these reasons are based on a perception that information privacy principles have not delivered expected outcomes. Other stakeholders, in business and government, may have different perceptions.

Collection principles

The collection principles raise a number of important issues, only some of which are explored in the Issues Paper.

Methods of receiving information

It seems clear that in most privacy jurisdictions, collection of personal information can be in the form of photographs, video or sound recordings.[2] The position in relation to bodily samples, and to information receive by the use of tracking devices or thermal imaging[3] has yet to be tested in Australia, but there is no 'in-principle' reason why these would not all involve 'collection', as well as, in some cases, being subject to specific surveillance laws. This hinges more on the definitions of personal information than of collection itself (see our responses to Chapter 3).

At least the following methods of receiving information about a person require separate consideration as to whether they are 'collection' for IPP purposes, and if so what obligations should apply:

- Information solicited from the data subject;
- Information solicited from third parties;
- Unsolicited information (whether from data subject or third parties);
- Information obtained from observations ('surveillance') of the data subject;
- Information extracted from documentary or other sources;
- Information generated as a result of transactions with an individual

Solicited information

The first two categores are clearly within the meaning of 'collected', whether solicited from the individual to whom the information relates (data subject) or from a third party. It is implicit from the distinctions between IPPs 2 and 3 in s.14 of the PA, between NPPs 1.4 and 1.5 in Schedule 3, and between s.9 and ss. 10-11 of PPIPA, that there can be collection from both the data subject and from third parties.

However, the distinction between solicitation from the data subject and from third parties can be important in two respects:

- the consequential obligations may differ depending on whether information is solicited from the data subject or from a third party (e.g. requirements to give notice).
- some laws require collection from the data subject where feasible (i.e. solicitation from data subject in preference to from a third party)

Collection directly from data subject

The Commonwealth *Privacy Act 1988* imposes requirements on *private* sector organisations concerning collection from third parties but imposes no such requirement on Commonwealth

---

[2] See *Harder v The Proceedings* Commissioner [2000] NZCA 129 and *Eastweek Publisher Ltd & Anor v Privacy Commissioner For Personal Data* [2000] HKCA 140.

[3] In the USA, the Federal Court has found that the use of thermal imaging is subject to the fourth amendment protection against unreasonable search and seizure: *United States v Cusumano*, 67 F.3d 1497 (10th Cir. 1995).

agencies. National Privacy Principle 1.4 provides: 'If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.' This requirement contributes to the fairness and transparency of processing personal data by helping to ensure that the data subjects participate in that processing. The requirement may also promote accuracy, relevance etc of personal data.

Under the NSW PPIPA, IPP 2 (s9) requires that personal information must be collected 'directly from the individual to whom the information relates' unless, inter alia, 'the individual has authorised collection of the information from someone else' (s.9(a)). In *DO v University of New South Wales* [2002] NSWADT 211 the Tribunal held that a declaration the complainant had signed authorising the respondent to obtain information 'from any tertiary institutions previously attended by me' was not qualified in any way and therefore did authorise the collection that took place. It is not clear if, having obtained personal information directly from an individual, it is then permissible under PPIPA to 'check' the information with a third party source. The preferable view is that the individual must give express authority for verification (unless another exception applies).

Unlike the obligation on NSW agencies under PPIPA, there is no obligation under NPP 1.4 to obtain the individual's authorisation to collect from third parties. The NSW agency provisions impose a higher standard than the Commonwealth private sector provisions while the Commonwealth agency provisions impose none.

> *Q 4– 3 (first part) asks '... In particular, should agencies also be subject to a general requirement that where reasonable and practicable, they should collect information about an individual only from the individual concerned?'*
>
> ***Submission 4-3.1: Commonwealth agencies should have an obligation to collect wherever possible directly from the data subject, as is currently the case with NSW, Victorian and NT government agencies, and private sector organizations.***

However, the NPP 1.4 wording is to be preferred as it allows for third party collection from third parties where it is unreasonable or impracticable to collect directly. The NSW principle is too 'absolute' and the many circumstances where it is not reasonable or practicable have had to be addressed through very broad and sweeping exemptions – an unsatisfactory solution (see separate section of this submission on Chapter 5 – Exemptions).

> ***Submission 4-3.2: The wording of a 'direct collection' principle should be based on NPP 1.4 but should omit 'only' which does not readily accommodate situations where some information can be obtained directly with supplementary information justifiably obtained from a third party.***

Unsolicited information

Drawing a clear line between solicited and unsolicited information can be very difficult. When is unsolicited information 'collected' (if at all)?

Australian commentators suggest that under the *Privacy Act 1988* unsolicited information, whether obtained from the data subject or from third parties, can be 'collected'.[4] The Australian Privacy Commissioner took a similar view in the *IPP 1-3 Guidelines*. The leading commentators on the HK Ordinance also accept that unsolicited information can be 'collected', but not 'until the data user takes active steps to incorporate them into the official working material of the organisation' (Berthold & Wacks, 1997, p. 97). This 'trigger' has its equivalent in the *Privacy Act 1988* concept

[4] Patrick Gunning, *Collection of personal information* in Gunning, 2001; and Graham Greenleaf, in Greenleaf, 2001.

of 'collection for inclusion in a record or generally available publication' (IPP 2(a) and s16B (for the NPPs).

In contrast, the NSW PPIPA expressly excludes unsolicited information from 'collection' (s4(5)). And in NZ a majority of the Court of Appeal has held unsolicited information is not 'collected' under their *Privacy Act 1993*.[5]

In light of the NZ decision, and in the absence of court or tribunal decisions on the *Privacy Act 1988*, the question of whether unsolicited information is 'collected' must also be considered open in Australia.

Under the NSW PPIPA, and under the Commonwealth PA if the *Harder* approach is adopted, any contact with an organisation initiated by the data subject will result in any information so provided not being regarded as 'collected', limiting the application of collection principles. (However, it is still personal information, and other principles may still apply).

> *Q4– 4 asks 'Should any obligations attach to an agency or organisation which receives unsolicited personal information that it intends to include in a record or generally available publication? If so, what obligations should be imposed?'*
>
> ***Submission 4-4: The law should make it clear that collection principles apply, to the maximum practicable extent, to unsolicited information.***

Observations / surveillance of the data subject

Personal information is obtained and recorded in many situations from observations of the data subject:

- A doctor observing a patient's symptoms and taking notes.
- A private investigator or police Officer taking notes about a person's movements or actions.
- A photographer or film crew or CCTV recording a person's movements.[6]
- A social worker observing the conditions in which a person lives, or how that person treats his or her children or spouse.
- Anyone recording their opinions about a person's truthfulness, sanity or any other opinion.

The observation may take place in the presence of and/or with the knowledge of the data subject, but may also be 'remote' and without their knowledge.[7] In many cases, observation will be by audio or video/CCTV. Given that most laws define personal information and/or records to include

---

[5] See *Harder*, supra n 2 and Paul Roth, *Whether there had been a 'collection' of information*, in Roth, 2000. The recording of the complainant's first telephone call was not 'collection' as the call and her comments were unsolicited. However, when she called back following Harder's request and answered his questions, this was 'collection'.

[6] In *Eastweek*, supra n 2, a case of obtaining information by photographic observation, the HK Court of Appeal majority found that there was not 'personal data collection' but only because of the intent of the recipient of the information. The case is better viewed as about 'personal data' not 'collection', and is therefore not significant on the question of whether observations can constitute 'collection'.

[7] Raymond Wacks considers that the covert filming of domestic employees is 'collection' under the Hong Kong Ordinance – see Wacks, 2000.

different storage media, it seems that the collection of personal information may also be in any medium, such as sound[8], photo[9] or video, and not only text.

Most privacy laws are silent as to whether such observation constitutes 'collection', leaving the question to the ordinary meaning of collection. If the obtaining of these types of observed personal information did not constitute 'collection', then data protection laws would be drastically limited in scope and would ineffective in a wide range of practical situations. The requirements of minimum collection and fair collection methods should apply to collection by observation as much as to other forms of collection. The remedial nature of privacy laws suggests that observation should be included as collection. The practice of Privacy Commissioners seems to assume that such observation constitutes collection, and case law to the contrary is not known.

> ***Submission 4-4.1: The law should make it clear that the collection principles apply to the maximum practical extent to information obtained from observation or surveillance.***

The more difficult question is whether the obligations to give notice on collection do apply in relation to collection by observation, or should apply. The IPP notice requirements only apply if data is 'solicited… from the individual', so it is unlikely that collection by observation requires notice. Similarly, the Hong Kong DPP 1(3) requires collection 'from' the data subject before notice is required, and DPP 1(3)(a)(I) also refers to 'supply' of the data by the data subject. The NPP 1(3) notice requirement is that there be collection 'from the individual'. NSW IPP 3 (s10) is similar. Whether observation is collecting 'from' a person seems uncertain.

Whatever the position is under the current privacy principles, there is also uncertainty about under what circumstances notice should be required when information is collected by observation. One of the main functions of surveillance regulation laws is to specify under what circumstances notice of surveillance must be given, and under what circumstances covert surveillance is permitted. Should information privacy laws leave this question to separate surveillance laws? Some surveillance laws make a distinction between covert and overt surveillance, with lesser controls applying to 'overt' surveillance – defined as surveillance about which the individuals concerned have been made generally aware.[10] Whatever position is taken on this question, the collection principle needs to clarify whether it requires notice to be given on collection by observation.

> ***Submission 4-4.2: Further consideration needs to be given to the policy issues concerning a requirement of notice when information is collected by observation, and the law needs to be clarified on this point.***

Information extracted

Much personal information is extracted from documentary or other sources. If information is not solicited from, or observed in relation to, any person, but extracted from a book or a database, is it 'collected'? This is a similar question to the one above concerning information collected by observation or surveillance. In relation to Australian Federal legislation, commentators have differed as to whether 'extracted' information is collected (Greenleaf 2001). The preferable view is that extraction is collection under current law, but the law would benefit from clarification on this point.

---

8 In *Harder,* supra n 2, the collection was by sound recording.

9 In *Eastweek,* supra n 2, the collection was by a photograph in a public place.

10 See for example *Surveillance Devices Act* 1999 (Vic) and *Workplace Surveillance Act* 2005 (NSW).

From a policy perspective, it is desirable that collection includes extraction, so that the principles concerning minimum collection and fair collection will apply.

> ***Submission 4-4.3: The law should make it clear that the collection principles apply to the maximum practical extent to information extracted from other records.***

As with collection by observation, it may however be appropriate to modify the notification requirements where information is obtained by extraction. Current privacy principles do not seem to require notice when information is collected by extraction, though this is not free from doubt. NPP 1.5 only applies to collection 'from someone else', and collection from a book or (less clearly) a database is unlikely to be considered to be collection from another person. IPP 2 only applies to collection from the data subject, and NSW IPP 3 (s10) requires collection 'from an individual'. In Hong Kong, it is not 'from' the data subject, and not 'supply'.

The question remains whether there are situations where collection by extraction should give rise to an obligation to give notice. It could be argued that while the default position should be 'no', the actions of some types of large scale data aggregators should give rise to an obligation to give notice.

> ***Submission 4-4.4: Further consideration needs to be given to the policy issues concerning a requirement of notice when information is collected by observation, and the law needs to be clarified on this point.***

Information generated as a result of transactions with an individual

A possible further category of information held about individuals is information generated by the data user in the course of transactions – eg records of enquiries, service provision, purchases etc. In some instances this could be described as collection by observation, but in others that does not seem apt. Our provisional view is that it is appropriate for all forms of collection of personal information to comply with the collection requirements that the collection be lawful, necessary, not unduly intrusive. However, whether it is practical to apply the notification aspects of collection principles to generated information is a more difficult question, as it is in relation to information collected by observation or extraction.

> *Q 4– 5 asks 'Should the obligations imposed on an organisation or agency at or soon after collection apply irrespective of the source of personal information?'*
>
> ***Submission 4-5: All collection obligations should apply to all forms of collection, irrespective of the source from or means by which the data is collected. However, different requirements of notice may apply depending on how the data is collected, with the default position being that notice is required unless an exemption is provided.***

This approach avoids the need to exhaustively address all of the possible modalities of collection, except that certain types of collection will be defined where the requirement of notice is reduced or removed.

Lawful purpose(s)

Most privacy laws share a common requirement that collection of personal information be lawful, necessary, relevant and 'minimal'[11], but there are significant differences in the precise wording, and consequently the meaning, of each of these component requirements. The Issues Paper does not

[11] Expressed variously as 'relevant and not unreasonably intrusive' (PA IPP 3(c) & (d)) and PPIPA s11(a) & (b); and 'adequate but not excessive in relation to that purpose' (HK DPO DPP 1(1)(c)).

enquire into this aspect of collection principles[12] and yet it is fundamental to the concepts of purpose specification (an express element of the OECD Guidelines) and proportionality (an implicit element underlying all sets of privacy principles).

NPP 1.1 only requires collection by a private sector organisation to be 'necessary for one of more of its purposes'. The reference to 'purposes' could imply 'lawful purposes'. IPP1, PPIPA s.8 and HKDPO DPP 1(1) include the specific additional requirement that the collection must be for 'a lawful purpose directly related to a function or activity of the collector'. The law should make it clear that collection can only be for a lawful purpose.

This does not of course mean that there would need to be express legal authority for the collection. In common law jurisdictions any action that is not unlawful is, by default, lawful. It will generally only operate as a negative condition preventing collection of personal information to further an unlawful purpose.

Data users also need to consider express prohibitions on the collection of certain information. In Australia, for example, Federal and State legislation aimed at rehabilitation of offenders prohibits the collection of some information about old criminal convictions. Telecommunications and Surveillance legislation also prohibits collection of certain information by specified means (see below under fair and lawful means of collection).

> ***Submission 4-5.1: The law should make it clear that collection can only be for a lawful purpose.***

Purpose justification

'Purpose justification' essentially means that there should be some test of public interest which is satisfied before a personal information system is established at all. A key weakness of the collection principles in most laws is shown by the question : 'how do you define the function or activity of the collector?' In the absence of a 'purpose justification principle', it is largely self-defined. While the negative requirement of a 'lawful purpose' is in most privacy principles, positive tests of justifiable purposes of collection can be found in the EU Directive and Canadian laws.

The European privacy Directive has a form of 'purpose justification' principle in Article 7 which requires that, where legitimate processing has to be justified by the interests of the data collector or a third party, it must be 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject ...'.[13] A 'purpose justification' principle seems also to be expressed in Article 6(1)(b), which stipulates, inter alia, that the purpose(s) of data collection shall be 'legitimate'.[14]

A clearer recognition of such a principle is found in the Canadian private sector law, which requires that: 'An organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.'[15] This effectively limits the purposes for which information systems may be developed with a form of public interest test. This has no counterpart in other Asia-Pacific legislation.

---

[12] There is only a passing reference in paragraph 4.15.

[13] See Graham Greenleaf, 'Purposes' and the Directive in Greenleaf, 1996.

[14] See further discussion of what 'legitimate' connotes in Bygrave, 2002a, pp. 338–339.

[15] Personal Information Protection and Electronic Documents Act 1999 (Can) s.5(3).

There is no purpose justification requirement[16] in the *Privacy Act 1988* either in IPP1 or in NPP 1. Data users are not required to have 'legitimate' purposes for establishing a system (beyond the requirement of a lawful purpose in relation to the IPPs), but instead they measure privacy protection against how well it adheres to the original purpose for which the system operator declared that it collected the information, which Europeans often call the 'finality' test (see also discussion under Use & Disclosure below).

Submission 4-5.1: Consideration should be given to whether Australian law should adopt any form of 'purpose justification' test, along Canadian, European or other appropriate lines.

Excessive collection

IPP 1 requires that collection be 'necessary for or directly related to [the purpose]'. HK DPP1 uses the IPP wording but adds a requirement that 'the data are adequate but not excessive in relation to [that purpose]'. PPIPA s.8(1) requires collection to be reasonably necessary for [that purpose] ((1(b)). NPP1 says 'necessary for one or more of its functions', without any express linkage to the purpose of collection.

Limiting the amount of personal information collected about a person is one of the cornerstones of data protection. The most effective limitation is the purpose of collection, because that limits it to what is relevant to the transaction at hand and prevents stockpiling of personal information. Limitation to what is 'necessary' for the transaction is a strong and appropriate measure of relevance.

In one of the Determinations on the TICA tenancy database operation[17], the Privacy Commissioner concluded that assessing whether a collection by TICA was 'necessary' "requires consideration of whether or not it is clearly appropriate and relevant to the functions or activities of the organisation' - can they be done without it? - how sensitive is the information?" The Commissioner concluded that the TICA Enquiries Database was necessary on this basis (without considering the overall privacy detriment that its operation might cause).

In a NZ case, a trade union's complaints that a company's introduction of finger-scanning of employees was unnecessary and 'overkill' was dismissed by the Privacy Commissioner In a useful discussion of the same issue, the HK Commissioner discourages the use of fingerprints in an employment context.[18]

Minimality and purpose limitation are key aspects of the EU's notion of 'adequacy'. APEC Privacy Principle III is weak on this point, limiting collection only to what is 'relevant to' the purpose of collection, not what is necessary for it, and should not be followed.

These requirements all relate to the *quantity and relevance* of collection, not the means (which are addressed separately – see below for discussion of *fair* collection). Quantity and relevance are important aspects of proportionality.

---

16 This is called 'prior justification' in the Australian Privacy Charter – see <http://www.privacy.org.au/About/PrivacyCharter.html> and 'justification and proportionality' in the draft Asia Pacific Privacy Charter – http://www.worldlii.org/int/other/PrivLRes/2003/1.html. Cf. the 'social justification principle' proposed by the former NSW Privacy Committee in its *Guidelines for the Operation of Personal Data Systems*, Background Paper 31, 1977.

17 *Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd* v *TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 4.

18 See <http://www.pcpd.org.hk/english/casenotes/case_enquiry2.php?id=184>.

Submission 4-5.2: The collection obligations should expressly link the amount of personal data that may be collected to the purpose of collection, and limit it to what is necessary for that purpose.

Anonymity

A strong, albeit under-utilised, aspect of the Australian law concerning minimality and purpose limitation is NPP 8 which provides:

> 'Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organization'.

It is appropriate to locate an anonymity principle within 'collection', as it is a form of collection limitation. Only the NPPs and the Victorian IPPs currently include an anonymity principle , which was codified for the first time in the Australian Privacy Charter in 1993, then adopted in the Privacy Commissioner's voluntary privacy principles of 1997. While an anonymity requirement arguably may be *implied* by certain provisions of the EU Directive (particularly the combination of Articles 6(1)(c), 6(1)(e), 7 and 8), (see further Bygrave, 2002a, p. 346) NPP 8 provides a much stronger statement.

An anonymity principle can be seen as conflicting with a perceived 'right' of a business (or government agency) to 'know its customers'. Leaving aside the increasing range of circumstances where there is a statutory 'know your customer' requirement (e.g. financial services, telecommunications), a plain meaning interpretation of NPP 8 suggests that it denies the existence of such a 'right'. Unless an organisation can show that it needs identifying information to perform a transaction, it must offer an anonymous option.

However, experience shows that it would be better to include the concept of 'pseudonymity' in this principle. There are only a limited range of transactions where true anonymity is both lawful and practicable (e.g. making simple enquiries). There is a much wider range of circumstances where it would be possible to 'protect' individuals identity through the use of 'known as' pseudonyms or codes. Such devices would allow transactions to proceed, without the identity being obvious to most parties, and yet retain the ability to identify an individual (customer or client) only when and if necessary (e.g. for processing payments, making official returns or in the event of justified investigations).

Anonymous or pseudonymous options need to be 'designed' in to information systems (see further, eg, Bygrave, 2002a, p. 371). It will be all too easy for data users to argue that it is impracticable to offer these options once design decisions have been made that preclude them. An obvious example is cashless toll roads, where the opportunity for anonymous travel has been removed by the removal of cash booths and the choice of tolling systems and business models that require vehicles (and their registered owners) to be identified. Had sufficient attention been paid to an anonymity/pseudonymity principle at the outset, it should have been possible to design automated toll roads that either respected the right of anonymous travel (through the use of pre-paid debit tags) or at least offered 'pseudonymous' accounts where identification of the actual user would only be triggered by exceptional events, (such as non-payment, accidents or crime).

The need for this principle to be incorporated in systems design also exposes one of the weaknesses of the complaints based model of enforcement – complaints that toll roads in Australia do not comply with NPP 8 are wasted because the operators can legitimately argue that it is 'too late' and now impracticable. The principle can only effectively be enforced by a pro-active regulator anticipating the compliance issue and intervening at the design stage of information systems.

4–29 Should NPP 8, the anonymity principle, be redrafted to impose expressly an obligation on organisations to give an individual the option of remaining anonymous when entering into transactions with those organisations?

Submission 4-29: The anonymity principle should be retained but redrafted to include the concept of pseudonymity as an alternative where appropriate. The principle should also clarify that it applies at the stage when an information system is being designed, not only 'after the event' when a person wishes to enter a transaction with a data user.

Submission 4-29.1: The anonymity principle should impose an obligation on organisations to give an individual the option of remaining anonymous or pseudonymous (as appropriate) when entering into transactions. The touchstone remains 'minimum collection necessary for the purpose of the transaction'.

Another enhancement of the anonymity principle would be to make it clear that the obligation extended to facilitating anonymous transactions with third parties. As an example, a representative complaint about charging for 'silent' telephone lines (unlisted numbers) failed because a telco itself needs to identify its subscribers (both for billing and as a statutory requirement. If NPP 8 required telcos to facilitate the ability for subscribers to remain anonymous in their interaction with third parties then it would be possible to argue that charging for silent lines breached the principle.

Submission 4-29.2: The anonymity principle should impose an obligation on organisations to facilitate, where practicable and lawful, anonymous or pseudonymous transactions between individuals and third parties.

4–30 Is it appropriate or desirable for agencies to be subject to an anonymity principle? In what circumstances, if any, might this be appropriate?

There is currently no equivalent provision in the IPPs. The obligations of governments to expressly limit their collection of personal information to the minimum necessary should be recognized by this explicit principle.

Submission 4-30: The anonymity/pseudonymity principle should also apply to the public sector.

Relationship between disclosure and collection

How is the purpose of collection of personal information to be determined, so that it can be 'used' in the operation of the various principles that refer to purpose? In some circumstances, such as where collection requires and can accommodate notification, the purpose will need to be specified by the data user. However there are other circumstances, such as where information is obtained by observation or generated by transactions (see above) where there may not be an opportunity for notice. In such cases, the purpose of collection will have to be inferred from the circumstances and context, including any related prior notification (e.g. when individuals initially enter a relationship, such as becoming a welfare beneficiary, taxpayer, insurance policy holder or other customer). An important example is where information is disclosed from one organisation to another.

Where personal information is obtained from a third party which is also subject to privacy principles, what is the relationship between the purpose for which the information was held by the discloser, their intended purpose for disclosing, and the recipient's purpose of collection? Which purpose governs the recipient's subsequent obligations, including under the collection principles? The obligations of those who receive personal information are complex, and derive from a number of sources.

Privacy principles do not simply say 'those who receive personal information are bound by the same obligations as the organisation from which they received it'. In fact, privacy principles rarely say anything direct about the obligations of the recipient of personal information (some exceptions are discussed below). Nor do privacy principles require a disclosing organisation to even state the purposes for which information is being disclosed, although they would, if challenged, need to be able to justify the disclosure under the relevant principle (see Use & Disclosure below).

Where a data user *receives information legitimately disclosed* under a privacy principle, and the recipient is aware of the basis of the disclosure, then that should condition and limit the purposes of their collection. It may be that purposes which would be lawful if the information was obtained elsewhere would not be acceptable under collection principles if they were not compatible with the disclosure authority of the source. But it is not clear if this would be based on the purpose being unlawful, or on the means of collection being unlawful or unfair.

Where a data user *knowingly receives information disclosed in breach* of a disclosure principle (i.e. the source has no legal basis for the disclosure, and the recipient is aware of that fact) then it would seem clear that the collection is also in breach, in that the collector would be complicit in the unlawful disclosure (or in some cases may even have expressly solicited the unlawful act), and this would constitute unfair collection.

If the recipient data user is *unaware of the basis of disclosure*, then it cannot be expected to make this judgment, but the question arises 'is it under any obligation to enquire?' This would almost certainly depend on the circumstances. It might be reasonable, when collecting from established data users such as government agencies and large corporations, to rely on an assumption that they have a lawful basis for disclosure. In contrast, if there was any good reason to doubt that a disclosure is lawful (perhaps because it is inconsistent with previous experience, or where it was from a questionable source), then there might be an onus on the recipient to enquire or this would make the method of collection unfair. However, this is uncertain.

If a recipient's intended purpose(s) of collection are narrower than the purposes for which the source could disclose, the narrower purposes will be the relevant ones for privacy compliance purposes. Similarly, it the source only agrees to release information for a narrow purpose, even if they could themselves use the information for other purposes (e.g. where a finance company discloses data to a debt collector), it is the narrower purposes that will constrain the recipient.

The above propositions would make the law workable, but there is no authority for them. This is a key area where the meaning of privacy principles is uncertain.

> ***Submission 4-5.3: Australian law should clarify the relationships between collection and disclosure of personal information, and in particular the limitations that the purposes of collection of a first organisation play in limiting the uses of a second organisation to which the information is disclosed.***

Obligations of confidence – role in limiting use and disclosure

The law of breach of confidence can play a role in determining the purpose of collection and subsequent use and disclosure options (assuming circumstances of confidence apply and the information is confidential). The relationships to which confidentiality attaches is (surprisingly) still uncertain for many modern commercial and professional relationships beyond the well known relationships such as banker/customer and doctor/patient. We will not go further into this issue here as it is more relevant to the parallel Inquiry by the NSW Law Reform Commission, but the ALRC should ensure that its Discussion Paper takes account of developments in relation to statutory powers and duties of confidence.

There is less uncertainty about the role of obligations of confidence is relation to government. Statutory obligations of confidence may also constrain uses and disclosures. The High Court's decision in *Johns v Australian Securities Commission* (1993) 178 CLR 408 that, in effect information obtained through the use of compulsory powers by a statutory body could not be used for purposes inconsistent with those powers has considerable but largely unexplored potential for interaction with privacy principles. Recently, the government has flagged its intention to seek legislative amendments to remove this constraint, but it would be appropriate for the ALRC to canvass views about the desirability of such a change, which would represent a significant undermining of the purpose specification and limitation foundations of privacy law.

> ***Submission 4-5.4: The Discussion Paper should consider the role that the law of breach of confidence plays in determining the circumstances under which the use or disclosure of personal is limited, and in particular whether the principles in Johns v ASC and similar cases needs to be supported by statutory provisions .***

Fair collection principles

The IPPs require that agencies shall not collect personal information 'by unlawful or unfair' means (IPP1.2), and, where the information is solicited, that the collection 'does not intrude to an unreasonable extent upon the personal affairs of the individual concerned' (IPP 3(d)). For the private sector, NPP 1.2 requires that organisations collect 'only by lawful and fair means and not in an unreasonably intrusive way'. HK DPP 1(2) requires that 'Personal data shall be collected by means which are - (a) lawful; and (b) fair in the circumstances of the case.' Intrusiveness is not mentioned specifically.

Lawfulness of means of collection - Means of collection can be unlawful because of a breach either of criminal law or of civil law requirements (such as by trespass, inducing breach of contract etc). A government agency acting *ultra vires* in collecting information beyond the scope of express collection powers would be another basis for unlawful collection. As noted above, data users also need to be aware of telecommunications and surveillance legislation which prohibits or regulates the obtaining of particular types or information and/or by specified means.

Fairness of covert data collection - Some means of data collection might not be illegal, but they may still be a breach because they are unfair. This is particularly likely to be the case where the means of collection are covert (i.e. the subject is unaware of them). In several complaint cases under the HKDPO, the Commissioner has found examples of unfair collection practices.[19] But the NZ Court of Appeal has taken a much more restrictive view, stressing in *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 that the purpose of the fairness requirement 'is to prevent people from being induced by unfair means into supplying information which they would otherwise not have supplied'.[20] There have been no Australian privacy law cases to date on unfair means of collection. The Australian Privacy Commissioner has issued Guidelines on covert surveillance.[21]

> ***Submission 4-5.7: The Discussion Paper should give more attention to issues concerning fair collection, which are of considerable practical importance.***

---

19 HKPCO Case No.: 200009383 – 'Surveillance on a domestic helper's workplace activities'; HKPCO Case No.: 200112506 – 'recording by a debt collection agency of conversations with debtors'; HKPCO Case No.: 199804574 – 'recording of telephone conversations between customers and staff'

20 Roth, 2000.

21 Cf. the discussion of the 'fairness' criterion in European law, in Bygrave, 2002a, p. 335–336.

Notification requirements in collection principles

Notification when collecting

> *Q 4– 1(generic part) asks: 'Are the obligations imposed on* ***organisations*** *at the time of collection of personal information adequate and appropriate?'*

NPP 1.5 states that 'If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual'.

Required notice of collection

All the Australian privacy principles require the collector of personal information to take reasonable steps to ensure that the subject of the information is aware of certain matters. While the principles do not expressly require the data user to give notice, that is the most common way of complying (see below for exceptions), and these principles are often referred to as requiring 'notification'.

The requirement to ensure that the data subject is aware of certain matters when collecting personal information is one of the most significant practical aspects of privacy principles. It is significant element of privacy protection because it puts the data subject is put on notice that he/she may need to protect his/her interests.

It is also however a principle that in many cases imposes significant costs on data users, not only for the initial analysis and design of awareness measures, but also their ongoing delivery. In order to comply with the awareness requirements, data users must put in place a system for reviewing every means by which they collect personal information – such as application forms, web sites and callcentres, as well as arrangements with third parties, and ensuring that where appropriate, adequate notice is given.

Relationship with openness principles

There is a close relationship between awareness/notification requirements as part of collection principles and the more general separate openness or transparency principle found in most privacy laws. There is a strong argument for dealing with these two overlapping sets of requirements together. This would allow for a more pragmatic discussion of the desirable levels of awareness, and how and when these can be created. This would also sit more comfortably with the concept of layered notices, discussed further below.

> ***Submission 4–1: The Discussion Paper should canvass the possibility of a combined 'awareness' principle, covering both notification requirements at the time of collection and more general information provision.***

Application of awareness/notification principles

The application of the awareness/notification requirement varies. IPP 2 only applies if 'the information is solicited from the individual concerned', and a similar condition applies under the HK DPO (DPP 1.3). In NSW, the Tribunal decided that notice requirements of PPIPA did not apply to information collected from third parties. [*HW v DPP (No 2)* [2004] NSWADT 73][22]. NPP 1.3 applies where information is collected 'from the individual' (potentially even when it is unsolicited – see discussion above), but in addition, where information is collected 'from someone

[22] See case summary at <http://www.austlii.edu.au/au/other/AUPrivCS/2004/19.html>.

else' (potentially including from documentary sources, public registers and by observation – see discussion above), NPP 1.5 requires the organisation take reasonable steps to ensure the individual is or has been made aware of the matters listed in 1.3

In Determination 2004/4, the Privacy Commissioner found that the tenancy database operator TICA had failed to comply with NPP 1.5, by, amongst other things, giving misleading and incomplete information.[23]

When is notice not required?

> *Q 4– 2 asks 'Should NPP 1 be amended to clarify that there may be circumstances in which it is reasonable for organisations to take no steps to ensure that an individual is aware of specified matters relating to the collection of personal information?*

The aim of the principle is to ensure that individuals are aware of certain matters. If a data user can be satisfied that individuals about whom it is collecting personal information are aware of these matters there need be no specific notification. This might be because they have been made aware in some other way or by some other party (e.g. generic advertising campaigns), or where they have previously been informed by the same data user.

The HK DPO contains a specific exemption for 'repeated' collections (s.35) within 12 months – notice does not have to be given again if all the matters are unchanged. Whilst this may seem like a sensible relief, such a provision can easily be abused if data users deliberately omit privacy notices from routine communications where there is minimal marginal cost in repeating it. It is asking too much of individuals to expect them to remember the details of a privacy notice several months after they have received it, and in most contexts no good reason why notice should not be repeated

A better way of ensuring that the objective of this principle is met consistently would, perhaps paradoxically, be to change this principle from one of 'ensuring awareness' to 'specifically notifying', with a conditional exception where the data user could establish that at least the typical data subject had been made aware by other means.

> ***Submission 4-2: Consideration should be given to changing the 'notice' principle from one of 'ensuring awareness' to 'specifically notifying', with a conditional exception where the data user could establish that at least the typical data subject had been made aware by other means.***

Timing of notice

IPP3, PPIPA s.10 and NPP 1.3 both require the reasonable steps (to ensure awareness) to be taken before[24] collection or, if that is not practicable, as soon as practicable after.[25] In contrast, there is no timing condition on NPP 1.5, where information is collected from a third party. Clearly the objective of awareness – to put the individual in a position of knowledge before they decide whether to give up their personal information - is severely compromised if the information is not provided beforehand. On the other hand there clearly are some circumstances where it is simply not practicable to convey all, or in some cases any of the information in advance. The risk of providing a 'if impracticable then later' exception is that it can be abused, with data users who could provide

---

[23] See <http://www.worldlii.org/au/cases/cth/PrivCmrACD/2004/4.html>.

[24] NPP 1.3 includes 'at or before'.

[25] The HKDPO DPP 1.3 says on or before without a 'where impracticable' exception, but does have an exemption for repeated collection.

the information prior to collection, perhaps with some cost or creativity, spuriously claiming 'impracticability'.

Submission 4-2.1: Strong justification should be necessary where notice is not provided before or at the time of collection.

Technology constraints on notification

There may be particular difficulties in communicating detailed privacy messages with certain modes of communication such as telephone calls, SMS and television advertising. If communications by these modes invite direct response – for instance by the customer calling or texting, then in theory they should include information about the matters listed in the applicable notification principle.

This is impracticable in many increasingly common scenarios, and the common approach to compliance in relation to the various forms of direct response advertising is to rely on the 'if impracticable then later' exception – providing the relevant information either in later contact with the individuals concerned (e.g. when finalising a purchase, or sending a contract) or by reference to a website. Neither of these is satisfactory – both because, as explained above, they deny individuals relevant information at the point of decision, and because there is even less chance than usual of the individuals locating and reading the relevant details.

Privacy laws face a major challenge in addressing 'non-traditional' means of communication. An extreme conclusion is that data users cannot comply and should not therefore use such channels to collect personal information, but this is unlikely to be acceptable either to consumers or business/government data users.

Submission 4-2.2: The Discussion Paper needs to canvass a more radical re-appraisal of the awareness and notification requirements in the context of new communications technologies.

One approach to this problem is to accept that there will be an increasing incidence of personal information being collected without the preferred level of awareness, but strictly limiting the use that can be made of that information until such time as further information has been given. This approach is explored further under Use and Disclosure.

Content of notice

Q 4– 3(second part), asks: 'Should agencies also be required to notify an individual of his or her rights of access to the information, the consequences of not providing the information, the various avenues of complaint available, and the source of the information, where it has not been collected directly from the individual?'

The Australian and other privacy principles vary in the precise information that needs to be communicated. It includes the following:

(i) *The identity of the data user and contact details* (NPP 1.3 (a), PPIPA s.10(f)[26], HK DPP 1.3). - While IPP 1 does not include this requirement, this is presumably because the identity of the data user was assumed, in 1988, to be 'already' communicated in the context of transactions with government agencies. If this was ever a safe assumption it is now clearly unreliable – understanding which government agency you are dealing with can be very difficult, particularly with the

[26] Including both collector and holder, where they are different.

increasing use of campaign names and brands by the public sector and with ever-changing administrative arrangements and 'portfolios'. The same difficulty has always applied in the private sector, where the true identity of businesses is often deliberately obscured, for marketing or other reasons.

> ***Submission 4-3: The law should require all data users to identify the party or parties to the transaction, and to expressly require operative contact details to be given.***

(ii) *The purpose(s) for which the information is collected* (IPP 2 (c), NPP 1.3(c), PPIPA s.10(b)) - Specification of purpose is critical in relation to limiting subsequent use and disclosure (determining 'finality' – see discussion under Use and Disclosure). The issues involved in identifying purpose have already been explored above.

(iii) *Details of any third parties to whom the collector 'usually' discloses this information* (IPP 2(e)[27]; NPP 1.3(d), PPIPA s.10(c)[28])

> *Q 4-1 in part asks: 'For example, should an organisation also be required to make an individual aware of (a) the types of people, bodies or agencies to whom the organisation usually discloses information of that kind?'*

Privacy Commissioners have taken the view that these principles should not be interpreted literally to mean that each specific agency or organisation to which personal information may be released has to be individually named. In recognition of this, the more recent NPP 1.3(d) expressly allows for this information to refer to 'types of organisation'. This of course means that individuals are not necessarily notified of particular recipients – knowledge of whom may affect their decision to proceed with a transaction. Most privacy notices use generic descriptors such as contractors, business partners, or government agencies, which are of limited value to the individual. For example, in A v Insurer [2002] PrivCmrA 1, the Commissioner found an insurer's travel insurance claim form was deficient in not identifying 'other consultants' to whom information was disclosed, and in N v Private Insurer [2004] PrivCmrA 1 that 'any other person necessary for claims determination purposes' was too broad a description. A possible approach to addressing this dilemma would be for the principle to expressly allow generic descriptors (as NPP 1.3(d) does now) but to add an obligation to answer specific enquiries about whether a particular named agency or organisation is a recipient. In some laws, this is arguably the intention of separate transparency/openness principles (e.g. NPP 5.2) – see later discussion of those principles.

> ***Submission 4-1: The Discussion Paper should consider whether, if notices use generic descriptors of recipients, there should be an additional obligation to answer specific enquiries about the identity of actual recipients.***

As already suggested, the Discussion Paper should expressly address the relationship between notification and openness principles in terms of the best way of achieving the objective of awareness, with specific attention to the respective roles of proactive notice vs obligations to respond to enquiries.

(iv) *Whether the supply by the individual is required by law or voluntary* (IPP2 (d)[29], NPP 1.3(e)[30], PPIPA s.10(d), HK DPP 1.3) - If interpreted strictly, this could require an explanation about each 'field' of information requested, which is unreasonable if not impracticable. The commonly

---

[27] Including any known 'second stage' onward disclosures.

[28] 'intended recipients'.

[29] 'required or authorised' – see discussion of this distinction under Use and Disclosure.

[30] Only whether it is required – no positive requirement to explain if voluntary although this could be seen as implied?

accepted approach to this principle is to indicate clearly which fields are mandatory – usually by means of an asterisk. Best practice is to ensure that the explanation of the asterisk precedes the first field in which it is used, rather than having it 'hidden' in 'fine print' elsewhere. There should also be an explanation of the basis of any 'mandatory' requirement – this is typically given as part of a privacy notice also covering the other matters. While it is clear that there is widespread non-compliance, this is an issue of guidance and enforcement. We do not see it as appropriate to suggest a more prescriptive requirement.

(v) *Any consequences for the individual if the information (or any part of it) is not provided* (NPP 1.3(f), PPIPA s.10(e), HK DPP 1.3) - This is typically covered in a privacy notice – generally associated with the information about mandatory and voluntary information. It does not need to be too detailed but at the least should clearly indicate to individuals that if they don't give some information then they may not, for example, receive the services in question. As with the mandatory/voluntary information, there is widespread non-compliance, but again this is an issue of guidance and enforcement. We do not see it as appropriate to suggest a more prescriptive requirement.

(vi) *The existence of any right of access and correction* (NPP 1.3 (b), PPIPA s.10(e), HK DPP 1.3) - This is very important information in relation to the overall scheme of statutory privacy protection. Gaining access is often the key to subsequent challenges about collection, quality, use and disclosure, and correction rights make an important contribution to data quality as well as being of critical importance to the individual. Unless individuals are aware of access and correction rights, they are not in a position to exercise their other rights. Raising awareness is beyond the resources of Privacy Commissioners, and having data users inform individuals of these rights when collecting personal information is by far the most efficient way of meeting this objective.

Additional matters about which 'awareness' measures could be required

> *Q. 4-1 asks specifically if organisations should be required to ensure individuals are aware of (b) the various avenues of complaint available; and (c) the source of the information, where it has not been collected directly from the individual?*

Awareness of avenues of complaint is clearly desirable, and a specific requirement to notify individuals of these would be consistent with developments in general consumer protection law and practice – this is now a common requirement in the financial services, telecommunications and utilities sectors.

> ***Submission 4-1.1: The law should require all data users to notify individuals of both internal and external dispute resolution options. Used appropriately, this can be assisted by layered privacy notices.***

Notification of sources is a more complex issue. Where collection is only from third parties, any direct contact with the data subjects will typically be after collection, and any such requirement would need to be built into a version of NPP 1.5, which is currently the only principle to apply to third party collection. Where there is some direct collection from the individual and some from third parties, it would be easier to include notice of the third party collection in the obligations at the time of direct collection.

Layered or staged provision of notice

Privacy Commissioners around the world have increasingly been accepting, and even promoting, the concept of layered or staged provision of information. In August 2006, the Australian Privacy Commissioner launched a new presentation of her own office's privacy policy as an example of a 'layered notice' approach. The objective of such approaches is to avoid overloading individuals

with too much information initially, but to retain easy options for them to find out more detail if interested.

Many consumer representative organisations, while acknowledging an 'information overload' problem, view trends towards layered and short form privacy notices with suspicion, as they can too easily omit information which should be relevant to an individual's decision whether to proceed with a transaction. Discussion of this issue inevitably involves wider 'political' judgments about the extent to which legislators and regulators should 'force' information on consumers which they may well not generally welcome or make use of (e.g., because it is perceived as paternalistic and patronising).

> ***Submission 4-1.2: Concerning layered privacy notices, the Discussion Paper should canvass views about the minimum set of information which needs to provided at or before the time of collection to achieve the objective of the awareness principle, and the minimum standard of transparency of links to more detailed information.***

These points are also relevant to the openness or transparency principle – see below.

Use and Disclosure principles

Single or separate principles?

> *Q 4– 6 asks: 'Is it desirable for the IPPs to deal separately with the principles relating to the use and disclosure of personal information or should use and disclosure be provided for in one principle?*

There are competing arguments. A single principle avoids arguments about whether an action is a use or a disclosure and therefore which principle applies. On the other hand, separate principles allow each to deal with issues that arise specifically in the context of internal use or disclosure to third parties. But the concept of a third party is slippery, particularly with large multi-function data users. Corporate entities can have many different 'business lines' and government agency boundaries are constantly changing with new administrative arrangements and portfolios. The NSW ADT has ruled that under PPIPA, in relation to agencies with disparate functions, some internal uses can be disclosures[31]. Even with a single principle, it is still necessary to understand the meaning of the two concepts.

> ***Submission 4-6: There are competing arguments. This question deserves to remain open in the Discussion Paper.***

Meaning of 'use'

The UK case of *R v Brown* [1996] 1 AC 543, a case on UK privacy legislation, held that merely reading personal information is not 'use' of that information. In contrast, the Federal Privacy Commissioner's *Plain English Guidelines to Information Privacy Principles 8-11* (1996) states that 'As a general rule, any accessing by an agency of personal information in its control is a "use"', and this includes 'searching records for any reason'. Even if it is not a breach of an IPP or NPP to merely access (or read) a person's file, it can easily be a criminal offence under the 'computer crime' laws of most jurisdictions.[32] The result in *Brown* was unfortunate, because evidence was lacking that the information had then been disclosed, though the circumstances raised this suspicion. However, if mere access does constitute use, organisations may be faced with unnecessary requirements to prevent innocuous and/or inadvertent access to files by their staff. It may be better for serious instances where this should be prevented to be regulated by the criminal law, or the regulations of particular institutions (e.g., Police, tax or Centrelink files) as is often currently the case.

> ***Submission 4-6.1: The use principle should clarify whether accessing personal information, without further action being taken as a result of that access, is 'use' of personal information.***

As noted in paragraph 4.33, the *Privacy Act 1988* s.6 provides that '***use***, in relation to information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication.' The meaning of this has always been unclear. In relation to Commonwealth agencies, the Federal Privacy Commissioner has considered many situations where an agency passes personal information to an outside organisation or agency to be a 'use' not a 'disclosure', applying a test of 'whether or not the agency maintains control over that personal information'. It seems that outsourcing of processing of personal information has been dealt with in this way. See Federal Privacy Commissioner, 'When is passing personal information outside an

---

[31] *KJ v Wentworth Area Health Service* [2004] NSWADT 84.

[32] *Crimes Act 1914* (Cth), s.76B(1) and 76D, and *Crimes Act 1900* (NSW) s.309(1).

agency a use?' in *Plain English Guidelines to Information Privacy Principles 8-11* (1996). It is questionable whether this interpretation would be upheld by a Court if challenged, and it would be unwise to simply apply it in the private sector context without further consideration.

Meaning of 'disclosure'

The IPPs refer to information being disclosed, not records. Disclosures can be verbal, or by actions (e.g., allowing another person to read a file). The Victorian Privacy Commissioner has noted that disclosure does not necessarily mean physical transfer: 'To disclose is to reveal. Personal information can be disclosed even though it remains in the possession or control of its original collector. The act of sending the original or a copy to another person is not a necessary element of a disclosure, although it will be a common feature' (IPP Guidelines Part 1). In Hong Kong 'disclosing' 'includes disclosing information inferred from the data' (s2). It also of course includes information explicit in the data. No issues seem to have arisen where the form of disclosure has been unnecessarily limited.

Australian commentators are divided on whether 'disclosure' includes information already known to the recipient,[33] but in our view it should be so regarded. It is of considerable practical importance. Information received from an earlier non-authoritative source means less than the 'same' information confirmed by a later more authoritative source[34]. Organisations could abuse this by simply asking whether other organisations could 'confirm' some item of information they purported to know, and the 'confirmations' would not be disclosures. Where a recipient of information really does learn nothing from information received, any compensation resulting from that breach by disclosure is likely to be reduced, as the disclosure has had no effect on the data subject. On balance, therefore, it is better for 'disclosure' to include previously know information.

> ***Submission 4-6.2: Privacy laws should make it clear that even information already known to the recipient can still be 'disclosed'.***

Limits on use and disclosure

> *Q 4– 7 starts by asking 'Are the circumstances in which agencies and organisations are permitted to use and disclose personal information under IPPs 10 and 11, and NPP 2, adequate and appropriate?'*

The starting point in considering what should be the allowed uses (and/or disclosures) of personal information is the 'original purpose of collection', referred to variously as 'obtained for a particular purpose', 'the primary purpose of collection', or the purpose 'for which it was collected'. Common to all these formulations is the key principle ('finality' in European nomenclature) that uses and disclosures should prima facie be limited by the purposes of collection. If applied strictly, this is not an 'efficiency' measure (in James Rule's terms) from the point of view of data users – it is not in a data user's objective interests to have to re-collect information from data subjects when they could re-use what they have or use their `information capital' for exchanges with other data users. In Rule's analysis, 'finality' principles do place objective limits on the surveillance capacity of organisations, but their significance depends on the exceptions to and exemptions from them.

---

[33] Patrick Gunning, *Disclosure of personal information* in Gunning, 2001 and Graham Greenleaf, *Does disclosure include information already known?* in Greenleaf, 2001.

[34] Contra what is implied in *EG v Commissioner of Police, New South Wales Police Service* [2003] NSWADT 150 where the NSW administrative Decisions Tribunal rejected an argument that information published in a newspaper should be distinguished from the communication of similar facts in the letter to the Legal Practitioners Board.

(i) Meaning of 'purpose of collection'

Can there be more than one distinct original purpose of collection? NPP 1.3(c) refers to notice of 'the purposes for which the information is collected', but the Commissioner has taken the view that there will only ever be one primary purpose, with all other purposes being secondary (Guidelines to the NPPs - NPP 2.1(a)) The problem with this view is that it invites data users to define their purpose broadly so as to avoid the constraints on secondary purposes. The EU Directive, by contrast, stipulates that the purposes for which data are collected shall be 'specified' and 'explicit' (Article 6(1)(b)). This is generally taken to mean that the purposes must be delineated in a relatively concrete, precise way (see further Bygrave, 2002a, p. 338).

> ***Submission 4-7: The law should be clarified to expressly allow for the declaration of multiple specific purposes, where collection is necessary for each of these purposes (but see discussion of bundled consent).***

How broad an original purpose is allowed is discussed in relation to permitted purposes and purpose justification under Collection above. Disclosure to third parties can be a purpose of collection in itself, i.e. a data user may well have as one of its purposes, or even a sole purpose, the disclosure of personal information.[35] Media organisations are the obvious candidates for this. Other issues relating to purpose specification that have been identified (Berthold & Wacks, 1997, pp. 123–124) include:

- How does one deal with purposes not anticipated at the time of the collection?[36]
- Are 'purposes' distinct from processes or activities?
- Can purposes can be implied by relationships (vendor/purchaser, employer/employee etc) whether stated at the time of collection or not?
- What is the effect of a data subject expressly limiting the purposes for which data can be used – does the data user have to respect that preference (see discussion of consent under Chapter 3)?

A number of specific questions in the Issues Paper about use and disclosure are part of the wider issue of what secondary purposes should be permitted. We choose to deal with this wider issue by discussing each of the main exceptions in turn.

(ii) Related purposes exceptions

IPP 10 allows only 'directly related' secondary uses, but IPP 11 does not include any similar provision for directly related disclosures, and may therefore provide more protection than the Directive. NPP 2 requires that the secondary use or disclose be 'related' to the purpose of collection (or 'directly related' in the case of sensitive information), but also requires that 'the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose'. The meaning of these terms has not yet been clarified by case law in Australia, or by reported interpretations by the Privacy Commissioner.

---

35 Three HK complaint decisions support this view of the equivalent DPP: Case No.: 199806115 – Purpose of collection of ID database maintained by the Registration of Persons Office included disclosures authorised under s24; Case No.: 199805978 – 'Whether disclosure of results of Teaching Evaluation to students is a contravention of the Ordinance' - Advised 'no', as this was a purpose of collection; Case No.: 199806288 – 'Whether posting a list of competitors on website is a breach of the Ordinance' – Skating competition. Disclosure was not the problem (it was a purpose of collection).

36 HKDPO DPP 3 expressly requires an objective test of what purposes are intended at the time of collection.

> *Q 4-8 asks 'Are the criteria in NPP 2.1(a) for using personal sensitive and non-sensitive information for a secondary purpose adequate and appropriate? For example, is it necessary or desirable that there also be a 'direct' relationship between the secondary and primary purpose of collection before non-sensitive personal information can be used or disclosed for a secondary purpose?*

Most privacy principles include some use and disclosure for purposes 'related' or 'directly related' to the purpose of collection.

- *Commonwealth public sector* - s14 IPP 10: '(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.'
- *Private sector* - NPP 2.1(a): 'unless (a) both of the following apply: (i) the secondary purpose is *related to* the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; (ii) the individual would *reasonably expect* the organisation to use or disclose the information for the secondary purpose; or …'
- *NSW public sector* - s17 '(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected'
- *Victorian public sector* - IPP 2.1(a) - identical to Commonwealth private sector NPP 2.1(a)
- Hong Kong – all sectors - DPP 3 (b) a purpose *directly related* to the purpose referred to in paragraph(a) [the purpose of collection].

NPP 2.1(a) makes a distinction between 'related'and 'directly related' meaning that for non-sensitive information, a secondary purpose need only be *indirectly* related to the primary purpose, although the Federal Commissioner says that the secondary purpose must be something that arises *in the context of* the primary purpose (emphasis added) (Guidelines to the NPPs - NPP 2.1(a)). The Victorian Commissioner says of the identical IPA principle that it must be 'connected or associated with the primary purpose'. 'Directly related' is therefore the test most commonly applied in Australian legislation and that of other Asia-Pacific legislation. Commissioners and Tribunals are not known to have had difficulties in applying a 'directly related' test.

International standards have little impact here. The EU Directive allows secondary uses and disclosures (further processing) of personal information in ways which are 'not incompatible' with the purpose(s) of collection (Art. 6(1)(b)). The NPP's additional 'reasonable expectations' test seems to impose a standard at least as high as the Directive.[37] There is room for disagreement about the precise meanings of 'incompatible', 'related' and 'directly related', but it is fairly certain that the Directive does not set a clearly higher standard here than the Australian provisions. The APEC Framework principle IV uses the less precise test of 'other compatible or related purposes'. Neither the APEC test nor the EU 'not incompatible' test should be adopted, as they will be more difficult to apply consistently.

> ***Submission 4-8: The general adoption of 'directly related' in the related purposes test is appropriate.***

(iii) Related purposes – 'reasonable expectations test'

> *Q 4– 9 asks 'Is the scope of IPP 10(e) (which allows agencies to use personal information for a purpose other than the particular purpose of collection, if the purpose for which the*

[37] Cf. Bygrave, 2002a, p. 340 (arguing that, under Art. 6(1)(b) of the Directive, 'any secondary purposes will not pass the test of compatibility/non-incompatibility unless the data subject is objectively able to read those purposes into the primary purposes, or the secondary purposes are otherwise objectively within the ambit of the data subject's reasonable expectations').

> *information is used is directly related to the purpose of collection) adequate and appropriate? For example, should there be an additional requirement that the individual concerned would reasonably expect an agency to use the information for that other purpose?*'

The NPPs and Victorian IPPs contain an additional 'reasonable expectations' test for secondary use and disclosure in addition to the 'related/directly related' test. It is the 'individual concerned' who must have the 'reasonable expectations'. This might suggest that the level of knowledge of industry practices by the individual may be relevant although the Federal Commissioner says the test will be applied 'from the point of view of .. an individual with no special knowledge of the industry or activity', and the Victorian Commissioner agrees: 'What would a reasonable person, without special knowledge, reasonably expect'. The Commissioners' views accord with the traditional administrative law concept of reasonableness set out in the *Wednesbury* case.[38] The Victorian Commissioner states that it is an objective test, and that 'the expectations of the actual individual involved are a consideration, but they are not determinative'.

Even for those principles which do not expressly include them as an additional test, the 'reasonable expectations' of the data subject may affect interpretation of what is 'directly related' (or, for that matter, on what is objectively determined to be the 'purpose ... of the collection'). Hong Kong commentators consider that, where the data subject has not been given notice of the purpose of collection, these reasonable expectations will affect the objective determination of purpose (Berthold & Wacks, 1997, p. 147).

> ***Submission 4-9: The 'reasonable expectations' test is desirable as part of a test of related purposes.***

(iv) Direct marketing 'opt out' exception

In considering the direct marketing exceptions, it is now appropriate to take account of the two specific laws applying to particular forms of direct marketing – the *Spam Act 2003* and the *Do Not Call Register Act 2006*. Both of these, in response to particular public concerns, impose much more rigorous and prescriptive requirements on direct marketing using email, SMS or voice calls. While the Spam Act is ostensibly an 'opt-in' regime, the exceptions and definitions combine to make it in effect an 'opt-out' scheme, which is what the Do Not Call Register Act is by express design. Given the wide exceptions and exemptions in both these Acts – particularly for political and charity marketing but also for 'established business relationships' – it is doubtful if they will fully meet community expectations. Many 'unwelcome' marketing approaches will continue to be lawful even where individuals have registered their preference not to receive approaches.

As the ALRC found from its national phone-in, direct marketing is the single most 'visible' manifestation of privacy concerns in the community and there is no reason to doubt that individuals would like the same control over traditional postal direct mail as they have now been given over some sources of electronic and telephone marketing.

The specific provision in NPP 2.1(c) for direct marketing is the source of much confusion. Ford seems to be incorrect in asserting that under the Privacy Act 'Australian consumers are given an unqualified right to 'opt out' of receiving direct marketing' (Ford, 2003, p. 147) As the Commissioner points out in the NPP Guidelines, it is open to organisations to avoid the specific constraints of exception (c) by relying instead on exception (b) - consent - but warns that in most cases express consent will be required (see below). Some businesses, particularly the direct marketing specialists, maintain that much of their activity can be carried out without either express

---

[38] *Associated Provisional Picture Houses Ltd. v. Wednesbury Corporation* [1948] 1 K.B. 223.

consent or even an opt-out opportunity by relying on the related purpose exception (a), arguing that most consumers have a 'reasonable expectation' that organizations they have dealt with before will try to sell them other goods or services. It remains to be seen if litigation in due course pushes most direct marketing into exceptions (b) and (c), with their conditions, or allows it to operate relatively unconstrained under exception (a).

In terms of international standards, the adequacy criteria adopted by the EU's Article 29 Working Party single out the need for a right to opt-out of direct marketing when personal data are used for direct marketing, in accordance with Art. 14(b) of the Directive, as one of the additional principles needed for adequacy of certain types of processing. In its Opinion 3/2001, the Working Party observes that it has previously stated that 'allowing personal data to be used for direct marketing without an opt-out being offered cannot in any circumstance be considered adequate', so this is clearly a significant issue. Hong Kong has a direct marketing provision that is closer to requiring a universal 'opt-out'.[39]

The Privacy Commissioner's 2005 private sector review report recommended:

> '23. The Australian Government should consider amending the Privacy Act to provide that consumers have a general right to opt-out of direct marketing approaches at any time. Organisations should be required to comply with the request within a specified time after receiving the request.' (OPC, 2005, p. 103)

The OPC notes that a general right to opt-out of direct marketing is supported by both consumer and business groups (including the Australian Direct Marketing Association) in Australia, (OPC, 2005, p.100) and in fact appears to be the current practice of most businesses (OPC, 2005, p. 102). The Senate Committee went somewhat further than the OPC and recommended in 2005 that the review it proposed 'should consider the possibility of an 'opt in' regime for direct marketing in line with the *Spam Act 2003*' (Bolkus Report, 2005, recommendation 15, p. 158). As noted above, it is arguably misleading to describe the overall effect of the Spam Act regime as 'opt-in'.

Another recommendation by the Commissioner for a national 'Do Not Contact' Register[40] has now been partially implemented in the form of the *Do Not Call Register Act 2006* (Cth). This is limited to telephone voice calls, and the breadth of exemptions from the scheme mean that it will not address many of the concerns about direct marketing uses. It is therefore still appropriate for a direct marketing 'opt out' to be dealt with in a general use and disclosure principle.

---

[39] The HK DPO s34 requires data users to inform data subjects, the first time they use particular personal data 'for direct marketing' to (i) inform the data subject of his/her right to request the data user to cease further use of that data, and (ii) to cease to use the data if so requested. This is a very convoluted way of expressing a right to 'opt out' of direct marketing approaches. But it at least has the merit of clearly applying to all direct marketing uses, with the issue of compliance with the use and disclosure principle clearly separate. This is much more like the relevant provision in the EU Directive Article 14. Hong Kong commentators make the point that notice must be given every time a data user makes use of some new item of personal data for direct marketing (and in their argument 'use' can merely include looking at the data). In effect, this means that an opt-out notice would be needed with every contact after data changed. Alternatively, it could be argued that notice was only needed if the data item was used to initiate or change the direct marketing, not merely viewed (a separate use) in the course of direct marketing. In practice, many organisations would simply give the opt-out notice on every contact, at least if it was written, and this would not seem to be too onerous a requirement.

[40] A 'Do Not Contact' register is maintained already by the Australian Direct Marketing Association for the voluntary use of its members, but is not well-known in the community.

> *Q 4– 12 asks: 'Is it appropriate that NPP 2 allows for personal non-sensitive information to be used for the secondary purpose of direct marketing? If so, are the criteria that an organisation needs to satisfy in order to use personal information for direct marketing purposes adequate and appropriate?'*
>
> ***Submission 4-12: NPP 2 should be amended to contain a sub-principle dealing expressly with direct marketing, broadly defined, unequivocally giving individuals a right to opt-out of receipt of further communications. No alternatives should be allowed. Such a principle needs to be designed to be consistent with other more specific legislation, which may however continue to apply a higher standard in relation to particular types or modes of communication.***

The IPPs governing the federal public sector do not include any opt-out right, which is a gap of increasing significance as government agencies adopt commercial direct marketing techniques to promote government policies and programmes. Given that there are other means by which governments routinely communicate the availability of services (such as general advertising), it is difficult to see why government agencies should not have to respect a clearly expressed preference of individuals not to be contacted. It would greatly assist the exercise of privacy rights if the Do Not Call Register (and any extension to other means of contact) gave individuals choices as to what sources of direct marketing they agreed to (e.g. commercial, fundraising, government information).

> ***Submission 4.12.1: Consideration should be given to providing a right to opt-out of direct marketing from government agencies – subject perhaps to limited exemptions for public health and safety campaigns or where government agencies had specific knowledge of individuals' eligibility.***

A related issue is the ability of individuals to find out from where the contact details used by direct marketers have been obtained. The Privacy Commissioner recommended in 2005 that:

> '24. The Australian Government should consider amending the Privacy Act to require organisations to take reasonable steps, on request, to advise an individual where it acquired the individual's personal information.'

This would be a significant reinforcement of individuals' privacy rights, without being too onerous for data users. Such a requirement could already be read into NPP 5.2, but there is no evidence that it is being interpreted in this way, and there would be merit in making it express.

> ***Submission 4-12.2: Privacy law should require that data users take reasonable steps, on request, to advise an individual from where they acquired the individual's personal information.***

(v) Consent exception

Privacy principles always allow data to be used for purposes other than the purpose of collection with some form of consent of the data subject, but what form of consent suffices differs widely. Australian privacy laws all have exceptions for use and disclosure where 'the individual concerned has consented'. PA IPP 10(a), IPP 11(b) and NPP 2.1(b), Vic IPA IPP 2.1(b) and PPIPA s.17(a) and s.26(2)). The HK PDPO DPP 3 requires 'prescribed consent' for data to be used for a different purpose. PDPO s2(3) provides that 'prescribed consent' '(a) means the express consent of the person given voluntarily'; and (b) may be withdrawn in writing.

Implied consent - The PA and Vic IPA define 'consent' as including express consent or implied consent (PA s.6 Vic IPA s.3).

In relation to international standards, the EU Directive requires that 'the data subject has unambiguously given his consent' (Art. 7(a)) as one of the bases for any processing of personal data. Insofar as any implied consent is also unambiguous, IPPs 10–11 and NPP 2 are compatible with the standard adopted in the EU Directive, provided they are interpreted as requiring free and informed consent.

Consent vs acknowledgement of conditions - Many data users seek 'consent' for uses and disclosures in circumstances where individuals are required to consent in order to proceed with the transaction or receive the service. This is from one perspective not 'free' consent, but from another the individual is free not to go ahead with the transaction. Privacy Commissioners have issued advice that in these circumstances data users should not pretend that they are seeking consent, but should instead ask the individual to simply acknowledge that the uses and disclosures specified will take place and are a condition of the transaction.[41] Whilst more 'honest', acknowledgement alone might not then be a sufficient basis for the use or disclosure (other than under the IPPs – which have a 'prior notice' exception discussed below). One of the other exceptions to the use and disclosure principle would have to apply. The credit reporting provisions of the Privacy Act (Part IIIA) refer expressly to consent in relation to transactions where individuals do not have any choice, other than not to proceed with their application for credit.

> ***Submission 4–12.3: The Discussion Paper should consider the implications of the confusion caused by the lack of any distinction in the Privacy Act between uses or disclosures justified by consent and those justified by acknowledgment of notification.***

Bundled consent - Bundled consent means the practice of seeking consent for multiple uses and/or disclosures at the same time (OPC, 2005, p. 85) – typically when collecting personal information. Individuals are given no choice as to the particular uses or disclosures to which they are consenting, or not consenting – it is in effect 'all or nothing'. The issue of bundled consent has been well canvassed by the Privacy Commissioner. Bundled consent exposes a major flaw in the practical efficacy of the principles in meeting the objective of participation by individuals.

Organisations employ this practice for reasons of efficiency and cost reduction. However, the practice undermines the interests served by the consent requirements of the *Privacy Act*. Yet the Act gives some leeway for the practice due to the reference in NPP 1.3(c) to a plurality of purposes and the omission of guidance as to the meaning of 'primary purpose' in NPP 2.1 (see above). Where secondary uses or disclosures are necessarily incidental the primary purpose e.g. disclosure to a mailing contractor for delivery, or to another agency for verification of details provided, then it may be appropriate to make this a condition of a transaction. But too often, data users seek consent for secondary uses which are neither necessary for nor even necessarily related to the primary purpose – most commonly for marketing other goods or services, but also for more significant and potentially even more unwelcome purposes.

In its 2005 private sector review report, the OPC notes that there is a need to clarify the limits for bundling consent under the Act. The OPC states that it will 'develop guidance' on the issue (OPC, 2005, recommendation 22, p. 93), but this has yet to appear. What needs to be made more clear is the extent to which data users are allowed to rely on consent obtained in this way and conversely, the extent to which individuals must be given separate opportunities to consent to different uses/disclosures.

---

[41] See for instance Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles*, edition.02, September 2006, KC 52, p.17.

4–11 Are there particular issues or concerns arising from the practice of organisations seeking bundled consent to a number of uses and disclosures of personal information? If so, how are these concerns best addressed?

Submisison 4-11: The law needs to be clarified concerning 'bundled consent' in order to prevent abuse of the practice.

In relation to international standards, the ability to bundle consent is arguably reduced (though not extinguished) under the EU Directive, given that the purposes for collecting personal data must be delineated in a relatively concrete, precise way (*viz*. the reference to 'specified' in Art. 6(1)(b))[42] and consent must be 'specific' (Art. 2(h)). Canadian legislation, by contrast, places more direct restrictions on the practice.[43]

(vi) Prior notice / mere awareness exception

Information Privacy Principle 11(1)(a) includes an additional exception allowing disclosure where 'the individual concerned is reasonably likely to have been aware, or made aware under Principle 2 [notice at the time of collection], that information of that kind is usually passed to that person, body or agency'. In this situation, notice is considered sufficient even if it does not amount to implied consent.[44] This exception seems to be an extremely broad 'bootstrap' clause by which government agencies can, in effect, write their own exemptions from the disclosure limitation principle, simply by notifying individuals about the disclosures at the time of collection. It has the same effect as the ability to self-define purpose of collection (see above) and means that there is no need for agencies to justify the purpose of disclosure, beyond showing that they are not acting *ultra-vires*. IPP 11(a) assumes some disclosure practices can be so notorious as to not require specific notice, and may be based on an assumption of implied consent. But this is already provided for in the exceptions for consent (defined as express or implied), and for related secondary uses within reasonable expectations (see above).

It is an anomalous exception. There is no equivalent exception in the NPPs, the EU Directive, or even the APEC Privacy Framework. A separate prior notice exception is at best a historical anachronism and cannot be defended. It should be possible to identify any and all countervailing private or public interests in advance and write a specific exception where this can be justified. There should be no place for a broad discretion to disclose solely on the basis that individuals are notified.

Submission 4-11.1: The exception for mere awareness of disclosure practices without consent to them or acknowledgment of them should be removed.

(v) Exceptions for prevention of harm to the person or others

The following exceptions are intended to cover exceptional situations, and appear to have operated largely satisfactorily, in the case of the *Privacy Act 1988* for nearly 20 years:

- *Commonwealth public sector* - s14 IPP 10(b)), s14 IPP 11(c): 'necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person';

---

[42] See further Bygrave, 2002a, p. 338 and references cited therein.

[43] See *Personal Information Protection and Electronic Documents Act* 2000, Schedule 1, clause 4.3.3: 'An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes'.

[44] On normal principles of statutory construction, this exception would not be needed if it was the same as implied consent, so it must be taken to mean something different.

- *Private sector* - NPP 2.1(e); 'necessary to lessen or prevent: (i) a serious and imminent threat to an individual's life, health or safety; or (ii) a serious threat to public health or public safety';
- *Victorian public sector* - as NPP 2.1(e) but adds 'welfare' (IPP 2.1(d));
- *NSW public sector* - s.17 IPP 10(1)(c) and s.18 IPP 11(1)(c) – 'necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person'.

> *Q 4– 7 goes on to ask specifically 'In particular, should agencies and organisations be permitted expressly to disclose personal information: (a) to assist in the investigation of missing persons; (b) where there is a reasonable belief that disclosure is necessary to prevent a serious and/or imminent threat to an individual's safety or welfare, or a serious threat to public health, public safety or public welfare; and (c) in times of emergency? What mechanism should be adopted to establish the existence of an emergency?'*

This question appears to relate to concerns expressed by some data users in previous reviews and enquiries, based partly on experience of emergencies such as the Bali bombings and the East Asian Tsunami of early 2006. These concerns have subsequently been addressed by amendments to the Privacy Act in late 2006. [45]

In relation to these questions, it is necessary to clearly distinguish situations where the use and disclosure principles form a genuine barrier to a sensible outcome, and spurious claims to that effect. Most of the examples of what has become known as 'BOTPA' (Because of the Privacy Act…) involve a misinterpretation of the constraints – sometimes out of ignorance but too often from laziness; unwillingness to explore the statutory exceptions and discretions or a wilful desire to blame the law for something that the data user does to wish to do for some other reason.

The recent amendments to the Privacy Act 1988 to address this perceived 'problem' were arguably unnecessary. The Minister in his Second Reading speech admitted that:

> "…, the bill serves to clarify and enhance what is largely already permissible under the Privacy Act."

In the rare circumstances where a collection, use or disclosure may technically not be permitted by the Act, it is unlikely that the individuals concerned would complain, and in any case, both the Privacy Commissioner and the Courts would have the discretion to treat any such complaint as trivial.

The amendments were drafted so broadly that they could have the unintended consequence of allowing 'emergency' declarations to be used to as a loophole for other purposes.

> ***Submission 4-7: The ALRC should canvass the justification for the recent amendments concerning emergencies, which were given relatively little scrutiny in Parliament.***

(vi) Exception where authorised under law

The Australian principles allow secondary uses where 'required or authorised by or under law' (IPPs 10 and 11, and NPP 2.1(g)). However, the meaning of 'law' in the exception under the IPPs appears to differ from that in NPP 2.1(g). The reference to 'law' in NPP 2.1(g) may include

---

[45] *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).

Commonwealth, State and Territory legislation, together with the common law, (OPC, 2005, p.41) while the reference to 'law' in IPPs 10.1(c) and 11.1(d) embraces only Commonwealth Acts, Commonwealth delegated legislation and documents with the force of Commonwealth law, such as industrial awards, but does not include State laws (unless the Commonwealth has submitted to a state law), the common law, requests for personal information from foreign governments, Cabinet decisions, agreements between government agencies or contracts between an agency and other parties (unless the agreements or contracts are specifically given the force of law by legislation).[46]

This is an area where consideration of international standards is significant. There have been European criticisms of the 'authorised by law' exception. The EU Directive allows secondary processing 'necessary for compliance with a legal obligation to which the controller is subject' (Article 6(1)(c)). The Article 29 Working Party states (in footnote 5 to Opinion 3/2001) in relation to the 'authority of law' exception that '[t]he reference to law (instead of legislation) is broad and may include any binding act'. In light of the above, the claim that 'law' means 'any binding act' oversteps the mark.

The Article 29 Working Party concluded that 'such a wide exemption would virtually devoid the purpose limitation principle of any value'. Their specific concerns were that 'to widen the exception to cover all options offered by sector specific laws, past present and future, risks undermining legal certainty and devoid the content of the basic protection'; and that 'The wording 'authorized' as opposed to 'specifically authorized' which existed in the January 1999 edition of the National Principles can also be read to mean that all secondary purposes that are not forbidden are allowed'. Ford characterised these concerns as a 'fundamental misreading of Australian law' (Ford, 2003, p. 144) but does not give a clear explanation of reasons.

While the 'authority of law' exception has considerable breadth, it can be argued that the result is in fact little different from the Directive:

- It includes disclosures which are not required but only permitted ('authorised') in the sense that the disclosing party has a discretion whether to disclose. This is clearly broader than the Directive's reference to a 'legal obligation'.
- It includes, primarily with respect to the private sector, disclosures which are authorised by common law or equity, not only those authorised by statute. The wording of the Directive seems to be broad enough to encompass non-statutory obligations (though not mere permissions).
- It includes obligations which may arise by law in future. So does the wording of the Directive.
- It includes obligations which do not necessarily state in express terms that they are exceptions to a data protection principle. This would also seem to be in line with the wording of the Directive.

There is no case law on NPP 2.1(g), but some interpretations by the OPC in various sets of Guidelines[47]. The Revised Explanatory Memorandum notes, however, that NPP 2.1(g)

> 'is intended to cover situations where a law *unambiguously* requires or authorises the use or disclosure of personal information. There could be situations where the law requires some actions which, of necessity,

---

[46] See OPC, 1996, pp. 40-41, A document may have the 'force of law' if violation of its provisions is an offence or may attract imposition of a penalty: *id*.

[47] See Federal Privacy Commissioner's Plain English Guidelines to Information Privacy Principles 8-11 (1996) and Guidelines to the National Privacy Principles - 2.1(g) and Privacy Victoria IPP Guidelines Part 1.

> involve particular uses or disclosures, but this sort of implied requirement would be conservatively interpreted'.[48]

The Working Party's suggestion that any secondary uses which are not forbidden by some other law are allowed (on the basis that conduct not forbidden by law is permitted) does not seem correct. Such an interpretation is at odds with the Revised Explanatory Memorandum and would make the whole purpose of these provisions ineffective, which is contrary to the principles of statutory interpretation. The better reading of these exceptions is that they are in the context of an obligation of non-disclosure imposed by the IPP or NPP, and that the exception therefore requires some positive legal obligation or permission to overcome that obligation of non-disclosure.

The exception is still broader than its equivalent in the Directive, in that permissions (not just obligations) to disclose are sufficient. And it is particularly problematic in the light of legislation providing government bodies with broad powers of disclosure.[49]

In relation to other international standards, the Use Limitation Principle in the OECD Guidelines allows secondary uses 'by the authority of law', so it is arguable that the Australian approach does not go beyond what the OECD permits. Further, s.7(3) of Canada's *Personal Information Protection and Electronic Documents Act 2000* includes the exception '(i) required by law' but also includes a number of other exceptions where disclosure is only 'allowed' (not 'required') including (c.1) where a government authority has requested the information under a lawful authority and '(iii) the disclosure is requested for the purpose of administering any law of Canada or a province'. As Perrin *et al* note, such requests can only be for relatively innocuous information, or Canadian law requires that a warrant be obtained (Perrin et al, 2001, pp. 75-76). Hence, the Canadian statute, which has received a finding of adequacy, does allow disclosures which are only permitted by other laws, but only in enumerated circumstances, not in general terms such as in the Australian principles.

> ***Submission 4-7.1: The Discussion Paper should consider whether, in light of international standards and examples from other jurisdictions, the 'authorised by law' exception could be made more specific.***

Disclosure exceptions are not requirements to disclose, nor general justifications

Although it is trite to state this, the exceptions to the use and disclosure principles can only be relied upon to show one thing: that there has not been a breach of these privacy principles. The exceptions are not in themselves *requirements* to disclose (or use) personal information. Organisations may choose not to disclose information even if it is not a breach of a principle to do so, unless some other law compels them to disclose. Nor are exceptions *general authorisations* to disclose: a disclosure compliant with an exception may still leave the discloser open to other actions for wrongful disclosure, whether because of some breach of another statute, or a breach of confidence, or a breach of copyright, or some other action. If the discloser has an obligation not to disclose which arises outside privacy laws, an exception to a disclosure principle cannot act as a defence. The same applies to uses which breach other duties.

---

[48] Parliament of the Commonwealth of Australia, Senate, *Privacy Amendment (Private Sector) Bill* 2000, Revised Explanatory Memorandum (1998-1999-2000), Notes on Clauses, p. 144 (para. 358)(emphasis added).

[49] See, e.g., s. 130(2) of the *Veterans' Entitlements Act 1986* (Cth) which reads: 'The Secretary or another officer of the Department [of Veterans' Affairs] may provide any information obtained in the performance of his or her duties under this Act (whether before or after the commencement of this subsection) to the Secretary of another Department of State of the Commonwealth or to the head of an authority of the Commonwealth for the purposes of that Department or authority'. As Bygrave notes (in Bygrave, 1990, p. 146), 'this sort of provision renders nugatory the restrictive effect of IPP 11.'

It is very easy for data users or data subjects to overlook or not understand this limited role of exceptions to privacy principles, and it may be valuable to remind them of this. Those who wish to encourage data users to disclose information in circumstances where an exception applies may not point out this limited role, resulting in data users mistakenly believing they have an obligation to disclose, or that they need no consider other legal obligations before they do so.

The NSW PPIPA contains a specific provision making clear that exceptions do not constitute obligations to disclose (s.23(6)).

> ***Submission 4-7.2: There should be a clear statement in privacy laws that an exception to a use or disclosure principle is neither a requirement nor an authorization to use or disclose.***

Data matching

Data matching is an increasingly prevalent technique, particularly in the public sector, whereby data users compare two data sets to identify apparently data relating to the same data subject. It generally involves both use and disclosure, and any data matching *prima facie* breaches use or disclosure principles since it involves information collected for one purpose being used for another, usually not for the benefit of the individuals concerned (although there are some examples of beneficial matching).

IPP 11 provides little restraint on the spread of data matching practices because (i) many agencies have broad powers to require information and/or disclose it, so either the receiving agency or the disclosing agency can satisfy the requirements of the 'authorised by law' exception (11.1(d); (ii) even if they have no such powers, the disclosing agency under a data matching practice could 'bootstrap' disclosures by simply informing individuals at time of collection that disclosure will occur (11.1(a)), and (iii) some agencies have also tried to argue the law enforcement/public revenue exception (11.1(e)) applies to mass disclosures without any knowledge of the individual case to support it being 'reasonably necessary' (this remains untested).

The Privacy Commissioner has no power to regulate such data matching. If an exception allows for the activity, then conditions cannot be imposed. The Commissioner issued 'voluntary data matching guidelines' in 1992, and subsequently recommended legislation to make them mandatory. This call was endorsed by a Parliamentary Committee in the mid 1990's, but the government did not respond. The federal Privacy Commissioner does of course have specific responsibilities in relation to some data matching under the *Data matching Program (Assistance and Tax) Act 1990 (Cth)*, which regulates specified programs involving mainly the Australian Taxation Office and Centrelink.

Other jurisdictions have more extensive controls over data matching. New Zealand has quite extensive data matching controls, based on the Australian model but of more general application.[50] The Hong Kong Ordinance makes provision for general data matching controls but these have not been 'activated' by the Commissioner, who makes case-by-case decisions on applications from agencies.[51] The Hong Kong regime also applies, at least in theory, to the private sector.

The Issues Paper does not address the data-matching provisions of the Privacy Act in any detail.

> ***Submission 4-7.3: The Discussion Paper should give consideration to the inclusion of a definition of 'data matching' and to empowering the Privacy Commissioner to regulate all data matching practices according to a set of statutory principles.***

---

[50] Privacy Act 1993 Part X

[51] HK DPO Part VI.

Consideration should be given to whether such regulation should also apply to the private sector .

Trans-border data transfers

4–31 Should the transfer of personal information offshore by agencies be regulated by privacy principles?

Submission 4-31: Yes, the same principles regulating data exports should apply to both public sector agencies and private sector organisations.

The 'export' of personal information across jurisdictional boundaries, whether it involves use or disclosure, raises specific issues which are very significant in the context of international privacy instruments. These issues are addressed separately in Chapter 13 of the Issues Paper, and our discussion of those issues is found in that part of this submission .

Data quality principles

Scope of principles

> *4–14 Is the scope of the data quality principle in NPP 3 (which requires an organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date) adequate and appropriate? For example, should the principle expressly apply to information that an organisation controls?*

The question of whether this principle should apply to information a data user 'controls' is applicable to all principles and is discussed in the part of our submission responding to Chapter 3

> *4–15 Is there a need to amend NPP 3 to clarify the extent of the obligations of an organisation under the data quality principle or is this best dealt with by way of guidance issued by the Office of the Privacy Commissioner?*
>
> ***Submission 4-15: The data quality obligations should only be expressed at a general level in the principles, as is the case at present.***

When data quality obligations apply

> *4–16 Should agencies be subject to a stand-alone data quality principle that extends to the collection, use and disclosure of personal information*

Data quality principles variously apply to collection and/or use, and contain a selection from the following criteria: accurate, complete, up-to-date, and relevant. The Hong Kong Ordinance defines the obligation negatively[52], but this is not preferable.

It is beneficial that a data quality obligation applies at the time of collection of data, provided it is coupled with a 'reasonable steps' requirement. Some principles link data quality requirement expressly to 'use'[53]. These requirements are intended to ensure that personal information is only used for purposes for which it is appropriate, which is another 'view' of the more general data quality requirement that information be 'fit for purpose' (IPP 3(c)). It is particularly important to check quality at the time of use where different definitions can apply in different contexts e.g. income (gross, net, taxable), occupation etc, and where matching of data collected in different contexts may lead to action adverse to the individual. If a data quality obligation applies at the time of the collection, and at the time of use/disclosure, it may be unduly onerous for there to also be an additional obligation that data quality obligations be observed in the intervening period when the data is 'held' as this might imply the need for continuous monitoring of the data.

> ***Submission 4-16: A data quality principle should refer expressly to a wide range of criteria of quality, including accurate, complete, up-to-date, and relevant. It should apply both at the time of collection and at the time of use and disclosure, but should otherwise not apply independently to the 'holding' of the data. Retaining the 'reasonable steps' qualifier in such a principle will ensure that the obligation is not unreasonably onerous.***

---

[52] 'Inaccurate' in relation to personal data 'means the data is incorrect, misleading, incomplete or obsolete' (s 2) – see Berthold & Wacks, 1997, p. 114 for examples of each of the criteria 'incorrect, misleading, incomplete or obsolete'.

[53] E.g. IPP 8 - Record-keeper to check accuracy etc. of personal information before use and IPP 9 - Personal information to be used only for relevant purposes.

International considerations

The equivalent European standard is Article 6 of the EU Directive which requires, in the paraphrase of the Article 29 Working Party, that 'data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed'. The relevant provisions of the IPPs (see IPPs 3, 8, 9 and 10(e)) impose, for the most part, similar requirements as Arts. 6(1)(c) & (d) of the Directive, but some differences exist. A potentially significant difference is the omission in the IPPs of any reference to 'adequate and not excessive'. In our opinion, however, the Directive's requirement that data collected be 'not excessive' is addressed to a large extent by the requirement of IPP 1 (that collection be limited to what is 'necessary for or directly related to that purpose'), in conjunction with the requirement of IPP 9 (that information be used only for relevant purposes) and of IPP 10(e)(that purpose of secondary usage – at least in the absence of application of IPPs 10(a)–(d) – 'be directly related to the purpose for which the information was obtained').[54] In relation to the private sector, NPP 3 omits the requirement in Art. 6(1)(c) that data be 'adequate, relevant and not excessive'. We take the view, however, that these criteria will be largely met by the requirement of NPP 1.1 that '[a]n organisation must not collect personal information unless the information is necessary for one or more of its functions or activities'.

[54] Bygrave notes, though, that the sense of IPP 9 is difficult to grasp as its reference to 'purpose' is not qualified (unlike in the other IPPs). See Bygrave, 1990, p. 145.

Data security principles

Detailed discussion of this principle, and a comparative analysis of security principles, is found in Nigel Waters and Graham Greenleaf, 2006, *Interpreting the Security Principle*, v.4, which we will not repeat in this submission, but which should preferably be read with it. Only the submissions arising from that paper are listed here.

> *4–17 Is the scope of NPP 4 relating to the obligations of an organisation to secure data adequate and appropriate?*

Based on a comparative analysis of various privacy instruments, the draft Asia Pacific Privacy Charter proposed the following model security principle:

> 'Organisations should protect personal information against unauthorised or accidental access, use, modification, loss or disclosure, or other misuse, by security safeguards commensurate with its sensitivity, and adequate to ensure compliance with these Principles'.

The Security Principle in the more recent APEC Privacy Framework is arguably even more comprehensive:

> 'Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.'

> ***Submission 4-17: A security principle constructed from the security principles in the the draft Asia Pacific Privacy Charter and the APEC Privacy Framework should apply to all data users.***

Contractors and outsourcing

In its 2005 private sector review report, the OPC registers considerable uncertainty amongst businesses as to their duties and liabilities with respect to organisations to which they outsource data-processing operations (OPC, 2005, p. 86). The OPC also states that its guidance on 'the issues relating to private sector contracting' should be clarified (OPC, 2005, p.188).[55] It recommends that the Australian Government 'consider amending NPP 4 to impose an obligation on an organisation to ensure personal information it discloses to a contractor is protected', and 'consider, in the context of the wider review of the Privacy Act, (see recommendation 1) whether there should be a distinction between data controllers and data operators' (OPC, 2005, recommendations 54 and 55, p. 189).

The Australian Government has recently signalled that it will look closely at imposing clearer obligations on Australian companies which outsource data processing to foreign companies. This comes in the wake of a television documentary screened on ABC on 15.8.2005, revealing that information on Australians is being sold on the black market after being outsourced to India for processing (Shaw, 2005).

[55] Cf. its existing guidance in Information Sheet 8-2001, available at <http://www.privacy.gov.au/publications/IS8_01.doc>.

4–17 (2nd part) For example, should NPP 4 be amended to impose an obligation on organisations to take reasonable steps to ensure that personal information they disclose to contractors is protected?

Submission 4-17: The security principle should also require organisations to take reasonable steps to ensure that personal information they disclose to contractors is protected.

Comparison with European standards

By comparison with European standards, the security provisions in IPP 4 and in NPP 4.1, though stated briefly, cover the essential aspects of security required by the Directive in Articles 16 and 17. However, NPP 4.1 omits express consideration of what is required of data controllers when they employ a third party (a 'processor' in the terms of Art. 2(e) of the Directive) to carry out processing of personal data on their behalf.[56] By contrast, IPP 4(b) requires in such a situation that 'everything reasonably within the power of the record-keeper [be] done to prevent unauthorised use or disclosure of information contained in the record'. This aspect of NPP 4.1 was not raised as a point of concern by the Article 29 Working Group in Opinion 3/2001. In our view, there are good grounds for holding that a requirement similar to that in IPP 4(b) can be read into NPP 4.1. Moreover, the law of agency may give rise to liability on data controllers for the acts of their data-processing agents. However, the amendment proposed above would put this beyond doubt, with the additional benefit of ensuring consistency with European standards.

[56] Generally, the *Privacy Act* does not operate with the same formal distinction between 'controllers' and 'processors' (or functional equivalents) as the Directive.

Retention and disposal principles

Retention and disposal are currently dealt with within security principles (NPP 4, PPIPA s.12)[57] NPP 4.2 has a requirement to "take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed" under NPP 2. The IPPs do not have any such requirement in relation to the public sector.

Detailed analysis of these principles is found in Nigel Waters and Graham Greenleaf, 2006a, *Interpreting Retention and Disposal Principles*, v.1, which we will not repeat in this submission, but which should preferably be read with it. Only the submissions arising from that paper are listed here.

The current formulation of NPP 4.2 allows organisations to justify retention on the basis of the myriad secondary purposes for which NPP 2 allows the information to be used and disclosed, whether or not they bear any relationship to the original purposes of collection. This is very dangerous. The single greatest protection for personal information against unexpected and unwelcome secondary uses, and 'function creep' is to delete or de-identify it. If it no longer exists in identifiable form, it can no longer pose a risk to privacy.

The increasing demands of law enforcement, revenue protection and intelligence agencies for personal information to be kept 'just in case' for their prospective access should be addressed through specific legal requirements, which can be debated and justified as clear exceptions to a general presumption of disposal.

> *4–18 Are there any circumstances in which agencies should be under an obligation to destroy or permanently de-identify personal information when it is no longer needed?*
>
> ***Submission 4-18: Privacy law should address retention and disposal in an independent principle applying to all data users.***
>
> *4–19 Should the IPPs and the NPPs regulate the deletion of personal information by organisations and agencies? In what circumstances might this be appropriate? Should an individual have the right to request that an agency or organisation destroy personal information that it holds or controls concerning the individual? If so, in what circumstances or upon what conditions should this be permitted?*
>
> ***Submission 4-19: Privacy law should address retention and disposal in an independent principle applying to all data users.***
>
> ***Submission 4-19.1 A retention and disposal principle should require data users to destroy or permanently de-identify personal information when it is no longer needed either for the purpose of collection or for any other purpose required by law, or for any secondary purpose for which it has already legitimately been used. Secondary purposes for which personal information may be used or disclosed in future should not provide an alternative justification for retention.***

Comparison with international standards

The EU Directive requires information to be kept in identifiable form "no longer than is necessary" (Art. 6(1)(e)), so the change recommended above would have the additional benefit of increasing consistency between Australian and European standards. The APEC Privacy Framework does not include any deletion principle.

---

[57] The HKDPO deals with it in a combined accuracy and retention principle – DPP 2.

Openness and transparency principles

> *4–20 Is the scope of NPP 5 relating to openness adequate and appropriate? For example, is it necessary or desirable for organisations to be given greater legislative guidance about their obligations under the principle? Does the more prescriptive approach to the openness principle in IPP 5 provide a suitable model?*
>
> *4–21 Is it appropriate that certain obligations under the NPPs relating to openness are triggered only upon an individual's request?*
>
> *4–22 Is there a need to clarify the relationship between the obligation of an organisation under NPP 1.3 (which imposes an obligation on organisations to take reasonable steps to ensure that an individual is aware of specified matters at or before the time of collection) and NPP 5.1 (which imposes an obligation on organisations to set out in a document clearly expressed policies on its management of personal information)? If so, how is this best achieved?*

All privacy laws include some version of an openness or transparency principle, requiring information to be provided - either generally publicly available and/or on request. (e.g. IPP 5, NPP 5, PPIPA s.13). As already noted under Collection principles above, there is a close relationship between these general openness or transparency principles and the specific awareness/notification requirements as part of collection principles. As already suggested, there is a strong argument for dealing with these two overlapping sets of requirements together.

> ***Submission 4-20 The Discussion Paper should canvass the possibility of a combined 'awareness' principle, covering both notification requirements at the time of collection and more general information provision, and with specific attention to the respective roles of proactive notice vs obligations to respond to enquiries.***

The laws that apply to public sector agencies often contain additional requirements, to develop, and in some cases make publicly available, a more detailed account of their personal information holdings (IPP 5.3 & 5.4) or a privacy management plan or policy (Vic IPA IPP 5.1, PPIPA s.33). There is considerable value in these requirements, not only because of their contribution to transparency and accountability but also because they require agencies to periodically and systematically review their activities involving the use of personal information.

While no-one expects a private sector business to need a management plan or policy with the degree of detail that is expected of government agencies, they will need to be able to produce some document in order to satisfy NPP 5, and in many cases a formal plan or policy may well be the easiest way of complying with that principle.

The central publication of agencies' detailed accounts which is a feature of the IPPs (IPP 5.4 and s.27(1)(g)), and for which provision is also made in PPIPA (s.40) and in the HKPDO (Part IV) (neither of which have been activated to date) is of questionable value. There has been relatively little use of the Commonwealth (and ACT) Personal Information Digests over the 17 years they have been published. While they are a potentially valuable resource for the media and public interest groups to make comparisons and hold governments to account, in practice they have rarely been used in this way. However, the marginal cost of maintaining them now that processes have been established is unlikely to be significant, and the savings from removing the requirements are unlikely to outweigh their potential value.

> ***Submission 4-20.1: The Digest provisions should remain. Even if the compilation and publication of a central Digest were to be discontinued, the obligation on agencies to***

> ***maintain individual records and make these available for public inspection. IPP 5.4(a)) should remain.***

No strong argument has ever been made for an equivalent to the Digest for the private sector data users. The registration requirements that are a feature of many European Data Protection laws are largely discredited – they impose substantial costs and have yielded few benefits. The HK Commissioner has considered activating the data user return provisions of the HKDPO but has not done so to date. Commissioners already have the power to require information from data users in the course of investigations, audits etc. It would however be useful for Privacy Commissioners to have express powers to require private sector data users to compile and publish explanations of particularly significant personal information handling projects, on an exceptional basis, independently of the exercise of other powers.

> ***Submission 4-20.2: Privacy law should give the Commissioner the discretion to require organisations to publish further information about particular personal information handling projects. (See also Submission 6-8)***

Further submissions on this point are made in response to Question 6-8.

Access and correction principles

Access – relationship to FOIA

> *4–23 Are the circumstances in which organisations can deny an individual access to his or her personal information under NPP 6 adequate and appropriate? If the circumstances are inadequate, should this be addressed by legislative amendment to the principle or by guidance issued by the Office of the Privacy Commissioner?*
>
> *4–24 Should IPP 6 more clearly set out the circumstances in which agencies can deny an individual access to his or her personal information? If so, what circumstances should be included?*

Assessing the adequacy of the access and correction principles in the Privacy Act is made complex by the uncertain interaction of the Privacy Act and the *Freedom of Information Act 1982* (Cth) in relation to access to and correction of personal information. The overlap is confusing both to the public and to the agencies with obligations under both Acts and should be rationalised – taking account of the useful recommendations of ALRC Report 77 in 1995, to which the government has yet to respond. These issues are discussed further in response to Questions 7-6 (a)-(c).

> ***Submission 4-23 and 4-24: This needs to be answered in the context of a rationalisation of the Privacy and FOI Acts. We support generally the ALRC's 1995 recommendations in Report 77.***

Intermediary access

Exemptions from access are inherently potentially prejudicial to interests more important than the data subject's knowledge of what data is being held. Data exempted from access is often the most prejudicial and important data about a person. Refusal of access prevents the person putting a counter-case concerning the accuracy or relevance of the data, and prevents them stopping, or even becoming aware of, abuse of other rights (eg improper uses and disclosures). At present, even a right of correction is often tied to right of access (see below), and this compounds the problem of lack of direct access. A second aspect of this problem is that access exemptions are more absolute than they need to be, because it is impossible to define the line clearly that defines when access is excessively prejudicial to the interests of the data user. The line therefore tends to be drawn to exclude access in many situations where in fact no harm would be done.

The problems cause by refusal of access can be reduced if access to some of all of the information can be provided to a third party acceptable to both sides, who inspects the data on the data subject's behalf. NPP 6.3 is a defective attempt to provide such intermediary access, too limited because the data user is only required to 'consider' the use of 'mutually agreed intermediaries'. There are no similar provisions in other regional privacy legislation. The Privacy Commissioner has limited powers to act as such an intermediary because the complainant will first have to credibly allege a breach of an privacy principle before the Commissioner can investigate.

Further consideration needs to be given to what steps such an intermediary should be able to take to protect the interests of the data subject, but in many cases the mere provision of a right to an intermediary would be likely to have the effect that data users would simply not bother to apply an exemption that existed in theory, because it easier to simply give access directly to the data subject. Exemptions from access would be more likely to be enforced only when the data user considered that direct access would have undesirable consequences in reality.

> ***Submission 4-23.1: Privacy principles should provide that, wherever possible, a data subject whose data is exempt from access by the data subject should be able to have***

that data accessed by a mutually agreed third party intermediary who is able to ensure that the data subject's privacy rights have been observed. In default of agreement, the Privacy Commissioner should be empowered to be such an intermediary. NPP 6.3 is not a adequate implementation of such a principle.

Access - Comparison with international standards

In relation to European standards, the EU Article 29 Working Party summarises the adequacy requirements derived from these principles as 'the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.' Both the IPPs and the NPPs provide the basic rights of access and correction required under Article 12. The sole concern of the Article 29 Working Party relating to the Australian access and correction rights was that s.41(4) of the *Privacy Act 1988* only allowed the Privacy Commissioner to investigate a breach of these rights if the complainant was an Australian citizen or permanent resident. This has now been resolved by changes to s.41 made by the *Privacy Amendment Act 2004*. European standards do not raise issues concerning access under Australian law.

APEC's access and correction rights (APEC Privacy Framework, principle VIII) are more explicit than the OECD's, but are also subject to explicit exceptions where (i) the burden or expense would be disproportionate to the risks to privacy; or (ii) for legal, security, or confidential commercial reasons; or (iii) the privacy of other persons 'would be violated'. These exceptions are very broad and it does not seem that APEC's requirement of proportionality for exemptions applies to them. However, APEC says individuals should have the right to challenge refusals of access. The dangers of incorrect information are greater where access is prevented by an exception, but APEC has not addressed the question of whether the right of correction depends on there being a right of access. Nor have most existing laws.

Notification of inaccuracies to third parties

The Hong Kong Ordinance DPP2(c) requires that, where practicable, once a data user is aware that data which has previously been disclosed to a third party are 'materially inaccurate' (and were so at the time of disclosure), then there is an obligation to inform the third party of this and provide the corrected data. Such a requirement for notification may arise either as a result of a data user's internal procedures picking up a previous inaccurate disclosure, or as a result of a data user exercising their rights of access and correction under DPP 6. This obligation to notify third parties of material inaccuracies is a valuable addition to the Hong Kong principles, not currently found in any Australian privacy principles.

In principle, there is no reason why this obligation should not also apply to inaccuracies of which the data user becomes aware *after* the date of disclosure. To the data subject, it is just as important that inaccuracies are brought to the attention of anyone that holds the information.

In order to comply with any notification obligation, organisations would have to have kept records of disclosures – see discussion of this complementary requirement under Use and Disclosure above.

4–25 Should the Privacy Act be amended to impose an obligation on both agencies and organisations to notify third parties, where practicable, that they have received inaccurate information and to pass on any corrected information? Should an obligation to notify third parties apply where agencies or organisations have refused to make a correction?

Submission 4-25: The law should require data users to notify third parties, where practicable and at the express request of the individual concerned, that they have received inaccurate information and to pass on any corrected information.

By comparison with European standards, Article 12(c) of the Directive requires notification to third parties who are previous recipients of data which are now subject to rectification, erasure or blocking under Art. 12(b). As discussed above, neither the IPPs nor NPPs currently include such a requirement, and it is unclear whether any notation added pursuant to s. 35 (see above) need be communicated to prior third party recipients. The Article 29 Working Party did not stress this aspect of Article 12 in its adequacy criteria, and did not raise this point in its criticisms of the NPPs. The change proposed above would therefore have the additional benefit of making Australian and European standards more consistent.

Correction- dependence on access rights

A problem which applies to the correction right in the IPPs (but not the NPPs) is that the right of correction depends on a person first obtaining access to their record, under the provisions of the legislation. So where a person's record is exempt from access because of some exemption, the data subject has no right to insist on rectification if they find out by informal means, or reasonably suspect, that the non-accessible record is incorrect.

The above problem is reduced slightly, though, by the fact that the Privacy Commissioner is given certain powers to order amendment of a record or to order that a notation be attached to it setting out details of any amendments the Commissioner thinks should be made (ss. 35, 52(3A), 52(3B)). These powers may be used in relation to determination of a complaint concerning application to amend a record, and extend to circumstances where an individual has been unable to obtain access to the record under FOI legislation *and* the following conditions have been satisfied:

- the individual has applied for review of the decision refusing access to the record, the application has been finally determined and can no longer be appealed;
- the individual has complained to the Commissioner about the refusal to amend the record;
- the Commissioner recommends that the agency concerned should make the amendment; and
- at least 60 days have passed since the Commissioner's recommendation was served on the agency, the Commissioner remains of the opinion that amendment should occur and is not satisfied that amendment has been carried out.

This is an unsatisfactory state of affairs, which could be dealt with by making the IPP right of correction not conditional on the right of access.

This problem does not seem to have an equivalent in European standards: on the face of it, the rectification right in the EU Directive Art. 12(b) does not depend on the data subject being able to exercise the access right in Art. 12(a).

Submission 4-25.1: Correction obligations should apply independently of rights of access – i.e. the right of individuals to seek correction should apply whether they have

> ***obtained access through formal processes (such as under the Privacy or FOI Acts) or have become aware of the information by other means.***

Correction – other improvements

For a review of the correction principle as it applies in privacy legislation, see Waters and Greenleaf 2005 'IPPs examined: The correction principle'.

> ***Submission 4-25.2: The principle should make it clear that correction can take the form of amendment, deletion or addition, as appropriate in the circumstances. There are many situations where there is a legal requirement to keep a historical record of actual transactions, but this should not prevent the correction of 'operational' records, leaving the original incorrect information only in an archive.***
>
> ***Submission 4-25.3: The principle should specify that the obligation in relation to disputed information has to be performed in a way which ensures that any annotation is made available to any subsequent user of the disputed information.***

Identifiers (NPP 7 and Ch 12)

The draft legislation for the proposed 'access card' national identification system is too recently available for us to include submissions specifically concerning it in this submission. This needs to be properly taken into account before usuful final submissions can be made on NPP 7 or on identifiers generally. We intend to publish later work concerning the relationship between the Privacy Act, privacy principles and the ID system. This work will also relate to NPP 7. Some preliminary comments are made below.

Q 4– 26 asks: 'Is there a need for a separate privacy principle regulating the adoption, collection, use and disclosure of identifiers by organisations? Should NPP 7, the principle regulating identifiers, be redrafted to deal more generally with the issue of data-matching?'

Submission 4-26: Identifiers and data-matching are separate issues and should be dealt with in separate provisions. (See earlier re data-matching)

12–1 Are the schemes that regulate Tax File Numbers appropriate and effective?

Submission 12-1: Tax file number principles should be dealt with consistently with unique multi-purpose identifiers - See submission 12-3 below.

12–3 What role, if any, should the Privacy Act play in the regulation of unique multi-purpose identifiers?

Submission 12-3: The privacy principles in the Privacy Act, and methods for adjudication concerning breaches of them, should apply to any unique multi-purpose identifiers adopted in Australia. Any variations from the application of any of the principles should be defined by specific legislative provisions stating exceptions or variations, and not left to inference from the existence of a different set of principles. Such an approach will (i) ensure that variations are obvious; (ii) facilitate a consistent body of law emerging on both the core principles and the exceptions.

Additional Principles

The ALRC asks (Q.4-35) if additional principles are required – specifically if there should be principles relating to accountability, prevention of harm, consent and security breach notification. We address each of these in turn below, and then suggest some further possible principles deserving consideration

> *4–35 Apart from the principles contained in the IPPs and NPPs, are there any other principles to which agencies and organisations should be subject? For example, should the IPPs and NPPs include expressly: an 'accountability' principle; a 'prevention of harm' principle; a 'consent' principle; or a requirement that agencies and organisations notify persons whose personal information has been, or is reasonably believed to have been, accessed without authorisation? If so, what should be the content of these principles?*

Accountability

At first sight the addition of an express accountability principle would be welcome. But the existing models seem to add little of substance. The OECD accountability principle (14) is nothing more than a 'motherhood' statement, while the APEC Framework Accountability principle (IX) seems to be more to do with onward transfer obligations that are arguably best covered in security and transborder data principles, and also seems confused about the role of consent.

Prevention of harm

A separate principle of 'preventing harm' which is found in the APEC Framework (Principle I) is not much more than re-statement of the overall objective of information privacy laws. It has been criticised (Greenleaf 2006) as follows:

> 'The sentiment that privacy remedies should concentrate on preventing harm ('should be designed to prevent the misuse of such information' and be 'proportionate to the likelihood and severity of the harm threatened') is unexceptional but it is strange to elevate it to a privacy principle because it neither creates rights in individuals nor imposes obligations on information controllers. To treat it on a par with other Principles makes it easier to justify exempting whole sectors (eg small business in Australia's law) as not sufficiently dangerous, or only providing piecemeal remedies in 'dangerous' sectors (as in the USA). It is not clear from APEC's Principles whether 'harm' covers distress, humiliation etc. It is also arguable that there should be a right to privacy in some situations independent of any proven harm, such as where there is the intentional large-scale public disclosure of private facts. This 'principle' would make better sense in Part IV on implementation, as a means of rationing remedies, or lowering compliance burdens.'

If read as imposing an additional harm test for a breach of any of the other principles to be taken seriously, then this would be unfortunate. The NZ *Privacy Act 1993* already contains such an additional test for complaints (s.66(1)(b)), which means that a complainant has to demonstrate actual detriment to themselves. This means that mere failure to comply with, for instance, security or notification requirements in the NZ IPPs cannot be dealt with under the complaint handling mechanisms, but only through the Privacy Commissioner's advisory functions.

> ***Submission 4-35: A separate 'prevention of harm' principle should not be adopted.***

Consent or 'choice' principle

We have commented extensively on the issue of consent in other sections of this submission. One version of an express consent principle is a right to object to processing. Bygrave notes that 'The EC Directive contains important instances of such a right, namely in Art 14(a) (which provides a right to object to data processing generally), Art 14(b) (which sets out a right to object to direct marketing) and, most innovatively, Art 15(1) (stipulating a right to object to decisions based on

fully automated assessments of one's personal character)' (Bygrave, 2002a, p. 66). The merits of an additional automated decision-making principle are canvassed below.

The APEC Privacy Framework includes a separate 'Choice' principle (V) which has been criticised (Greenleaf 2005) as adding little of value:

> 'APEC requires that, where appropriate, individuals should be offered prominent, effective and affordable mechanisms to exercise choice in relation to collection, use and disclosure of their personal information. Since consent is already an exception to the collection and use and disclosure Principles, this Choice Principle only adds an emphasis on the mechanisms of choice, and could be seen as redundant. It is not in other sets of Principles. The elevation of choice to a separate principle poses some risk of interpretations that would support bundled consent. However, the wording of the Choice Principle does not (and should not) imply that consent can override other Principles, so it does not imply that individuals should be able to 'contract out' of the security, integrity, access or correction Principles.'

NPP 2.1(c) is in effect a limited right to object to direct marketing, although it is highly conditional, and an organisation may well be able to carry out direct marketing based on one of the other exceptions to NPP 2. We have already addressed the direct marketing issue under the Use and Disclosure principle.

> ***Submission 4-35.1: There should not be a separate principle concerning consent or choice.***

Security breach notification

The idea has of a principle requiring that data subjects be advised by data users of security breaches which may affect them has emerged only recently. There is specific legislation in a number of US States, following well-publicised security lapses by major corporations (as discussed in the Issues Paper at paragraphs 4.204 - 4.207). Notification is considered important to allow individuals to take or seek remedial action and/or make informed decisions about whether to continue a relationship.

Businesses, and to a lesser extent government agencies, have traditionally been reluctant to publicise security lapses, both because of the potential for reputational damage and, it is sometimes claimed, to avoid giving clues about vulnerabilities that could be used in 'copycat' attacks. Government agency security lapses have sometimes become public knowledge 'after the event' either in their own Annual reports, or through reporting by Auditors-General, Ombudsmen or Privacy Commissioners. The first reason for not publicising security breaches is precisely one of the main justifications for new security breach notification requirements: the risk of reputational damage to the data user will act as a stimulus for improved security measures. The second reason is largely spurious: there is no reason why notification of lapses has to go into the technical detail, and in any case this 'excuse' applies only to third party attacks, and is not valid for breaches that result from carelessness by the data user.

> ***Submission 4-35.2: The Discussion Paper should canvass the role of a Security Breach Notification Principle, drawing on the US experience. We agree with the ALRC (paragraph 4.206) that the threshold criteria for triggering a notification requirement is critical. There should by now be enough experience of the US State laws to guide a sensible rule.***

No disadvantage principle

The Australian Privacy Charter and the Asia Pacific Privacy Charter identify a separate principle entitled as 'no disadvantage' in the first[58], and 'Non-Discrimination' in the second[59]:

> 'People should not be denied goods or services or offered them on unreasonably disadvantageous terms (including higher cost) in order to enjoy the rights described in this Charter' (Principle 5)

The only provision like this in Australian privacy laws is the specific requirement that there be no charge for access to a person's own personal information in some principles Without a broader 'no disadvantage' principle, it is all too easy for data users to levy a charge for the exercise of privacy choices and rights, either directly, or by differential pricing, or to impose some other non-financial barrier. However, it can be difficult to distinguish actions deliberately designed to deter the exercise of privacy rights from the incidental effect of new services or technologies. For example electronic toll payment systems or delivery of services by SMS can limit the privacy choices of consumers. To what extent should data users be prevented from using new delivery channels solely because they may not readily 'accommodate' traditional privacy rights? Is the answer simply to require other more traditional means of interaction to be available? This may not be realistic as business and government increasingly move to new service delivery channels, with many benefits to consumers.

> ***Submission 4-35.3: Privacy law should include an additional no-disadvantage principle to ensure that data users do not use pricing or other sanctions to deter individuals from exercising their privacy rights. Such a principle would need to designed carefully to avoid becoming a constraint on innovation.***

Automated decision-making principles

Neither the IPPs nor NPPs include any direct equivalent of Art. 12(a) of the Directive giving data subjects a right to knowledge of the 'logic' behind automated decisions, particularly of the kind described in Art. 15(1). The Australian principles also omit any direct equivalent of Art. 15(1), which provides persons with a qualified right not to be subject to certain forms of fully automated decision making (further on the provision, see Bygrave, 2002a, pp. 319–328). However, vestiges of these rights are present in guidelines issued by the Privacy Commissioner to regulate data-matching programs initiated by federal government agencies.[60]

The Article 29 Working Party includes in its criteria for adequacy a reference to these sorts of rights as "examples of additional principles to be applied to specific types of processing". However, the existence of such rights does not seem to be regarded as a necessary precondition for a finding of adequacy. Neither the Safe Harbor Agreement nor Canadian data protection legislation make specific provision for such rights, yet both regimes have been deemed adequate.

---

[58] Principle 18 – see <http://www.privacy.org.au/About/PrivacyCharter.html>.

[59] Calling such a principle 'non-discrimination' may be unwise as it has specific connotations of a set of actions prohibited under separate anti-discrimination laws such as age, sex or disability. 'No disadvantage' is preferable.

[60] See *Guidelines on the Use of Data-matching in Commonwealth Administration* (February 1998), paras. 63–66, available at <http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_23.15.pdf>. Adherence to the guidelines is voluntary and breach of them will not incur legal penalties. A large number of agencies subscribe to them. See further overview in the Office of the Privacy Commissioner, Annual Report 2003–2004, pp. 69–70 available at <http://www.privacy.gov.au/publications/04annrep.pdf>. Somewhat similar, though slightly weaker, provisions on point are contained in paras. 5.1–5.5 of the Data Matching Program (Assistance and Tax) Guidelines (available at <http://www.privacy.gov.au/publications/p6_4_21.doc>) issued by the Commissioner pursuant to s. 12 of the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth). The latter Guidelines are mandatory for the (more limited number of) agencies concerned.

The Asia Pacific Privacy Charter includes an 'automated decision-making' principle (17):

> 'An organisation must not make a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human)'

There is a precedent in Australian law for an 'automated decision-making' principle, in the *Data matching Program (Assistance and Tax) Act 1990* (Cth) for individuals to be notified before any adverse action can be taken against them (s.11, and Guidelines 5.1-5.2). This may have much the same effect as an objection to processing, as it gives an opportunity to object before a decision based on automated processes is made.

> ***Submission 4-35.4: Consideration be given to an automated decision-making principle which requires human intervention before any adverse action is taken in relation to any individual based solely on automated processes.***

Privacy impact assessments principles

See discussion in relation to Question 6-6

> ***Submission 4-35.5: The Discussion Paper should canvass the merits of an additional principle requiring Privacy Impact Assessments for significant projects***

Exemptions from the Privacy Act (Ch 5)

Policy concerning exemptions – avoid 'privacy-free zones'

> *5–1 Is it appropriate for certain entities to be exempt, either completely or partially, from the operation of the Privacy Act? If so, where should the exemptions be located?*

Too many exemptions to the Privacy Act create 'privacy-free zones' where an organisation, or a class of organisations, are given a complete exemption from all IPPs/NPPs, whereas in fact all that is justifiable is an exemption from, or more likely a modification of, some IPPs/NPPs. Examples are given below, and the 'privacy free zones' of the private sector are also criticized in Greenleaf (2000). The only two exemptions which we think have merit are those relating to personal use (see our response to Q 5-14) and State & Territory authorities (see our response to Q 5-4).

> ***Submission 5-1: Exemptions should as far as possible be limited to, and where possible located within, the principle(s) to which they are applicable. Organisations should not be given a blanket exemption from privacy principles, because at least some privacy principles are applicable to all organisations, even if their application needs to be modified. This approach (i) will help avoid a plain reading of a principle creating misleading expectations of coverage, and (ii) help avoid organisations being able to claim that they 'comply' with a principle, when in fact an exemption located elsewhere means the exact opposite outcome.***

Exempt Commonwealth agencies

> *5–2 Should the following defence and intelligence agencies be exempt, either completely or partially, from the Privacy Act: * Defence Imagery and Geospatial Organisation; * Defence Intelligence Organisation; * Defence Signals Directorate; * Australian Security Intelligence Organisation; * Australian Secret Intelligence Service; and * Office of National Assessments?*
>
> *If so, what is the policy justification for the exemption? Are there any other defence and intelligence agencies that should be exempt, either completely or partially, from the Privacy Act?*

There may need to be specific exemptions from some privacy principles (principally the collection and access principles) for some intelligence agencies, but there is no justification for these agencies not to be subject to all of the principles in respect of administrative and employment information, or for them to be exempt from, for example, the security and quality principles, even for the personal information they collect operationally.

The fact that access, correction and review and complaint rights might need to be qualified for operational data does not justify lifting the obligation to keep information secure, maintain data quality and delete information once no longer required. The reasonable steps qualification to these principles should adequately deal with the special circumstances of these agencies. Similarly there is no reason why the use and disclosure principles should not apply, with a specific exception similar to that provided in the context of access in NPP 6.1(k) in addition to the normal range of required by law and 'prejudice to law enforcement' exceptions – see our response to Chapter 4.

> ***Submission 5-2: The agencies listed in Q5-2 should not be completely exempt. The extent of any justifiable exemptions to or modifications of specific IPPs should be stated in the Act.***

*5–3 Should the following agencies be exempt, either completely or partially, from the Privacy Act: * Australian Government ministers; * federal courts; * agencies specified in Schedule 1 to the Freedom of Information Act 1982 (Cth)—namely, the Australian Industrial Relations Commission, the Australian Fair Pay Commission, the Industrial Registrar and Deputy Industrial Registrars; * Australian Crime Commission; * royal commissions; * Integrity Commissioner; * agencies specified in Schedule 2 Part I Division 1 of the Freedom of Information Act 1982 (Cth) other than the intelligence agencies, the Australian Government Solicitor and the Australian Industry Development Corporation; and * agencies specified in Schedule 2 Part II Division 1 of the Freedom of Information Act 1982 (Cth)?*

If so, what is the policy justification for the exemption? Are there any other agencies that should be exempt, either completely or partially, from the Privacy Act?

There is no justification for such broad exemptions for any of these agencies. Any difficulties that compliance with privacy principles might cause for any of these agencies should be dealt with by means of selective exceptions to particular principles and provisions, but only on the basis of detailed justification. If the concern is about one 'watchdog' having oversight of another, we reject any suggestion that this a bad thing – no agency, however important the public policy purpose it is performing, should be exempt from the obligation to comply with fundamental human rights and administrative law principles.

Submission 5-3: No, the agencies listed in Q5-3 should not be so broadly exempt. The extent of any justifiable exemptions to or modifications of specific IPPs should be stated in the Act.

State and Territory authorities

5–4 Should state and territory authorities be exempt from the privacy principles in the Privacy Act?

The *Privacy Act* should not be a pretext for the extension of Commonwealth powers into areas that are otherwise the constitutional responsibility of the States and Territories. State and Territory authorities should be exempt from the Privacy Act to the extent that they are able to be covered by State or Territory laws. Whether or not they are so covered is a matter for the State and Territory legislatures. If they are not, then there will be implications arising from the transborder data flow principle NPP 9 and any extension of it to Commonwealth agencies – see our responses to Q 4-31 and Chapter 13.

Submission 5-4: State and Territory authorities should be exempt from the Privacy Act, except to the extent discussed in 5-5.

5–5 In addition to the energy distributors owned by the New South Wales Government, which are the only state authorities prescribed under the Privacy (Private Sector) Regulations 2001 (Cth), are there any other state or territory authorities that should be covered by the privacy principles in the Privacy Act? If so, to what extent should they be covered?

There is no reason why State or Territory business enterprises should have an arguable commercial advantage over private sector organisations because they can avoid the costs of compliance with privacy laws. On the other hand, there is no reason why the Commonwealth should monopolise power to establish appropriate privacy standards. Consistency in privacy standards across Australia is desirable, but that is a separate issue. The best balance is struck simply by ensuring that some enforceable privacy standard applies. This is somewhat similar to the solution reached in Canada, at

least in spirit, where federal law would apply unless the provinces legislated for themselves (and many have now done so).

The law should make provision for coverage of any state or territory authorities 'by agreement' (effected through Regulations) to cover the increasing number of 'hybrid' organisations involved in the delivery of public services and to ensure no organisation can 'fall between the gaps'.

> ***Submission 5-5: Any State or Territory authority that competes with private sector organisations should be subject to the Privacy Act unless they are subject to a State or Territory Act which includes a set of privacy principles of comparable scope and a means by which individuals may enforce them by law including by appeal to a Court.***

See our response to Chapter 13 for a fuller discussion of 'equivalence'. We note that the current Tasmanian law, and the unenforceable 'standards' of South Australia and Queensland, would not meet the test we suggest in 5-5 – and that would be a good thing.

Small business operators

> *5–6 Should the small business exemption remain? If so: (a) what should be its extent; and (b) should an opt-in procedure continue to be available?*

The small business exemption threshold is completely arbitrary, and in any case is a misnomer as many medium sized businesses would have lesser turnovers. It is impossible to envisage any sensible size or other criteria which would capture potentially significant personal information handling while excluding 'mundane' processing. Even one-person businesses can be at the forefront of privacy intrusion (e.g. private investigators, or specialised websites).

Small businesses lose their exemption as small business operators if, amongst other things, they collect or disclose personal information for a consideration (s.6D(4)). The meaning of this 'clawback' has always been unclear, and there are no known examples of it being tested. Examples of where the exemption might be lost, unless care is taken to obtain the data subject's consent, are where an otherwise 'small' business is involved in: obtaining consumer information from a credit reference agency; cooperative swapping of personal information in relation to commercial credit transactions through reference agencies; a real estate agent obtaining information from a tenancy database operator; a purchase (or exchange) of a mailing list ; operation of a merchant facility on any credit card; or payment to a carrier for Caller ID to be enabled. It seems that if s6D(4) is not complied with on even one occasion, the exemption is lost forever. What confidence can anyone have that an apparently exempt 'small' businesses has not in fact lost its exempt status? Yet the Privacy Commissioner appears to have been content to allow a broad interpretation of the small business operator exemption to circulate. This is too uncertain a criterion by which to determine that consumers lose all their privacy rights.

An alternative and less dangerous approach would be to make the Act apply to those defined as exempt 'small business operators', but to require the Commissioner to make a Code which could modify or exempt those eligible from bureaucratic aspects of the principles or any other aspects of the Act (even though this would weaken the principles and Act), so that, in effect, they would only be liable for serious substantive breaches of privacy. 'Reasonable steps' requirements in the Act already provide considerable protection, and the Commissioner could also be empowered to cover these aspects in a Code. For most small businesses, removal of . While a promotional campaign could encourage small businesses to review their operations, some may only become aware of their obligations if and when they receive a complaint. This would be a satisfactory situation for most low-risk, low-sensitivity business relationships, and is better than a blanket exemption from the Act.

In its 2005 private sector review report, the OPC notes that the exemption is problematic. While it does not recommend abolishing the exemption, the OPC does recommend altering somewhat the criteria for what constitutes a small business in order to add clarity and certainty to its application. The proposal is that the reference to annual turnover be replaced by a reference to number of employees (20 or fewer) (OPC, 2005, recommendation 51, p. 185). The OPC also recommends that the scope of the exemption be narrowed in relation to operators of tenancy databases, Internet service providers and producers of Public Number Directories.(OPC, 2005, recommendation 52, p. 185) The OPC recommends further that the consent provisions in ss. 6D(7) and 6D(8) be removed (OPC, 2005, recommendation 53 p. 185).

Submission 5-6: The Small Business Operator exemption should be removed.

Submission 5-6.1: If special provisions for small businesses are needed, the definition of exempt Small Business Operator should only define who comes within a Code made by the Privacy Commissioner which can relax or remove bureaucratic aspects of the principles and the Act.

The exemption as it is now poses particular difficulties for consistency between Australian and European law. The essence of the criticism by the Article 29 Data Protection Working Party in Opinion 3/2001 is that 'the complexity of this exemption is such that it makes it very difficult to determine: a) what Australian business is a small business and b) whether or not it is exempt from the provisions of the Act' and that 'this uncertainty renders it necessary to assume that all data transfers to Australian businesses are potentially to a small business'.

The Australian Government's justification for this exemption is that it is only exempting those small businesses which are deemed to pose little or no risk to privacy interests.[61] According to Ford, the exemption 'was based on a considered view that the risk of privacy breaches from a sector that rarely trades in personal information is small and does not justify the costs of regulation in this area' (Ford, 2003, p. 146). Their point of view has been that, in reality, most Australian businesses trading with European businesses will not be small businesses, and that 'the assumption should be that businesses are covered rather than the reverse' (Ford, 2003, p. 146). It has also been argued that 'one easily identifiable way to know whether a business is covered or not is to check its privacy statement on its website (or other documentation)', and that prosecutions could follow for false statements to this effect (Ford, 2003, p. 146).

It is arguable that no assumptions can be made as to whether an Australian business with which a European company is dealing is an exempt small business. Cheap international communications make it quite possible for Australian businesses with turnover under AUD3,000,000 to engage in international transactions, albeit on probably a smaller scale than would be the case with large businesses. If personal data are transferred from Europe to some proper recipient in Australia, there is nothing in the *Privacy Act* except the normal rules governing secondary purposes to prevent the data being disclosed to an exempt small business operator. There is no special 'onward transfer principle' to prevent disclosure of data to such organisations exempt from the Act (of which exempt small business operators are just one category); nor could there be as it is not possible to know the original source of all personal data. Perhaps the secondary use and disclosure limitations in the *Privacy Act* could be seen as sufficiently strict to ensure that such 'leakage' to exempt bodies will only be minimal. This exemption seems to pose a considerable problem for any 'adequacy' finding. The OPC's proposed changes would have no effect on the problems discussed above except they might make it easier to determine that a business is not an exempt small business.

---

[61] See, e.g., Hon. Daryl Williams AM QC MP, Attorney-General, Second Reading Speech to the Privacy Amendment (Private Sector) Bill 2000, *House of Representatives Hansard,* 12.4.2000, p. 15752.

Political parties and practices

'Political acts and practices' (acts done by Parliamentarians or Councillors in connection with elections, referenda or participation in 'another aspect of the political process') are exempted from the Act by s7C. Further, a registered political party (a political party registered under Part XI of the *Commonwealth Electoral Act 1918* (Cth)), is not an 'organisation' (s6C) and is therefore not bound by the provisions of the *Privacy Act*. The political acts and practices exemption was excluded from the terms of reference of the Privacy Commissioner's review of the private sector provisions.

There is no justification for political parties to be wholly exempt. Most individuals, if they were aware of the increasingly sophisticated database operations of political parties, would see it them as one of the clearest examples of personal information processing needing the protection of the privacy principles. There can be no justification for political acts and practices to be wholly exempt. There seems no good reason why principles of notification, data quality and security, and access and correction cannot apply to personal information used in political acts and practices.If compliance with any of the principles causes difficulties that interfere with the legitimate and desirable operation of representative democracy, then a specific exception may be justified.

To the extent that there is an implied constitutional right to freedom of political expression and communication it is difficult to see why this extends to forcing information onto an individual who has expressed a clear preference not to receive it. There are many alternative means for politicians to communicate with electors. However, the constitutional right should define the ambit of any exemption.

> *5–7 Should registered political parties be exempt from the operation of the privacy principles in the Privacy Act?*
>
> ***Submission 5-7: Registered political parties should only be exempt to the extent required by the Constitution.***
>
> *5–8 Should political acts and practices be exempt from the operation of the Privacy Act? If so, does the current exemption under s 7C of the Privacy Act strike an appropriate balance between the protection of personal information and the implied freedom of political communication?*
>
> ***Submission 5-8: Political acts and practices should only be exempt to the extent required by the Constitution.***

However objectionable these exemptions may be from a domestic perspective, they are probably not a practical issue in terms of consistency with international standards. The exceptions in the EU Directive for non-consensual processing of such data are far more limited than s 7C. They do not, for example, exclude the principles of access or security. However, the difference is probably of miniscule consequence to Europeans: Australian political parties are likely to have extremely limited interest in the data about Europeans which get transferred to Australia.

Information concerning a person's 'political opinions' and 'trade union membership' are included in the definition of 'sensitive information' in the *Privacy Act 1988* (s 6)(as is 'membership of a political association'). They are also regarded as 'special categories of data' in the EU Directive (Art. 8), so there is no difference between Australian and European standards on this point.

Employees

Employers are exempted from observing the Act with respect to processing of 'employee records' when the processing is (a) 'directly related' to (b) a 'current or former employment relationship' between the employer and the employee concerned (s 7B(3)). Criteria (a) and (b) obviously restrict

significantly the breadth of the exemption. For example, they would seem to rule out the application of the exemption in the case of prospective employment relationships. Thus, processing by an organisation of data relating to an applicant for a job with the organisation would probably not be covered by the exemption.[62] The term 'employee record' is defined in s. 6(1) as '…a record of personal information relating to the employment of the employee'. The definition then provides as 'examples' of such information 'health information about the employee and personal information about all or any of' a long list of examples. Designated as 'examples' only, these categories of information do not constitute an exhaustive list of what is meant by 'employee records'. At the same time, a logical implication is that not *all* personal information relating to an employee is to be regarded as an 'employee record' under the Act.

The government's proffered rationale is that such protection is more properly a matter for workplace relations legislation.[63] The Federal Attorney-General's Department and Federal Department of Employment and Workplace Relations issued a Discussion Paper on privacy of employee records for public comment in February 2004,[64] but no progress seems to have been made since then. The exemption was excluded from the terms of reference for the OPC's review of the private sector provisions of the *Privacy Act.*

There is no comprehensive protection for employee records under other areas of law. Although there is a wealth of rules – both statutory and in common law – regulating the relations between employers and employees for the benefit of the latter, these still fall far short of providing employee records with the protection that such records would otherwise gain were they to be embraced by the *Privacy Act 1988*.[65]

> *5–9 Should the employee records exemption remain? If so: (a) what should be the scope of the exemption; and (b) should it be located in the Privacy Act, workplace relations legislation or elsewhere?*

The Senate Committee recommended that 'the privacy of employee records be protected under the *Privacy Act 1988*' (Bolkus Report, 2005, recommendation 13 p. 158), and that the ALRC 'should examine the precise mechanisms under the *Privacy Act* to best protect employee records' (Bolkus Report, 2005, recommendation 14, [7.38])[66] The OPC and ALRC have also expressed the view that employee records should be brought under the scope of the *Privacy Act 1988*.[67]

There is no justification for the private sector employee records exemption, and it represents one of the major gaps and weaknesses in the Privacy Act. Experience in other jurisdictions (including the IPP regime applying to Commonwealth agencies) shows that employees are one of the main categories of user of privacy rights. This is unsurprising given that the implications of non-compliance can be very far-reaching and serious in an employment context.

---

[62] See also OPC, *Coverage of and Exemptions from the Private Sector Provisions*, Information Sheet 12-2001. The validity of this interpretation has not yet been tested in the Courts.

[63] Second Reading Speech, *supra* n 61, p. 15752.

[64] *Employee Records Privacy. A discussion paper on information privacy and employee records*. (February 2004).

[65] See further, e.g., Otlowski, 2001.

[66] Note too Australian Law Reform Commission, *Essentially Yours: the Protection of Human Genetic Information in Australia*, Report No. 96 (2003), vol. 2, especially Part H and Recommendations 30–1, 34–2. The ALRC Report recommends that, in general, employers should refrain from collecting or using genetic information in relation to job applicants or employees. At the same time, the ALRC Report acknowledges there may be rare circumstances in which such action is needed to safeguard workers' health and safety or the health and safety of third parties, and that such action should be allowed if it complies with stringent privacy, anti-discrimination and occupational health and safety controls.

[67] See, e.g., submissions from these two bodies to the Senate Committee, cited in Bolkus Report (2005) at pp. 75–78.

Submission 5-9: There should be no general exemption for employee records. Some uses of employment records in particular contexts may justify exemptions from or modifications to particular IPPs/NPPs.

International standards are a factor to be given some weight in concluding that this exemption is not in Australia's interests. The Article 29 Working Party found this exemption to be of particular concern given that human resource data are often traded across borders and often contain sensitive information. The Working Party was also concerned that the exemption 'allows information about previous employees to be collected and disclosed to a third party (for example, a future employer) without the employee being informed.' The Australian Government contends that the latter concern rests on a misconception of the exemption, and that '[t]he prospective employer would have to comply with the collection principle, and notify the individual of the collection' (Ford, 2003, p. 145). This contention is correct if, as is probably the case, the exemption does not apply to employer collection of information on prospective employees. The Australian government has also contended that few employment-related data are transferred from Europe (Ford, 2003, p. 145). The validity and relevance of this contention are at the very least questionable. Although we have not seen solid empirical data on the quantity and nature of information flows from Europe to Australia, there can be little doubt that personal data *are* being transferred along this channel and that at least some of these relate to current or past employment matters and are, in addition, sensitive.

Media organisations

Journalists are expressly exempted from having to reveal their confidential sources (s66(1A)), so that is not what is at issue here. The exemption for media organisations is far too broad. Journalism is not defined and the definition of media organisation effectively allows anyone to claim the exemption by setting up a 'publishing' enterprise. The condition requiring a public commitment to privacy standards can be satisfied by the organisation itself, with no independent assessment.

At least some of the current media privacy standards are substantively weak and/or lack strong enforcement mechanisms. For example, in relation to the print media, the Australian Press Council (APC) – a self-regulatory body representing all major commercially available newspapers and magazines in Australia – has developed a set of Privacy Standards so that its members may take advantage of the exemption.[68] The Standards do not contain an equivalent of NPPs 5 (openness) or 9 (transborder data flow) and are more lax in several respects than some of the other NPPs.[69] The APC lacks enforcement powers other than publication of findings of non-compliance.

In relation to broadcast media, the OPC's 2005 private sector review report notes weaknesses in the powers of the Australian Broadcasting Authority (ABA – now Australian Communications and Media Authority) with respect to enforcing the privacy provisions of broadcasting codes of practice:

> 'The ABA submission … states that it lacks appropriate sanctions (what it calls middle range sanctions) that would allow it to actively enforce the privacy provisions in broadcasting codes of practice. When a breach occurs, the ABA is limited to informing the media organisation and extracting commitments from broadcasters about code training and disseminating the ABA's breach findings amongst staff. The ABA … also states it has found a pattern of repeat offending privacy related breaches in commercial television (though no pattern existed in radio)' (OPC, 2005, p. 196).

---

[68] Available at <http://www.presscouncil.org.au/pcsite/complaints/priv_stand.html>.

[69] Compare, e.g., Standard 4 ('A media organisation should take reasonable steps to ensure that the personal information it holds is protected from misuse, loss, or unauthorised access') with NPP 4.1 (requiring protection for personal information from 'misuse and loss and from unauthorised access, modification or disclosure'). See further Mellor (2003); Waters (2002). A slightly dated overview of the various Australian media codes of conduct (and practice thereafter) which are relevant for privacy is provided in Lindsay (2002).

The 2005 private sector review report by the OPC recommends that the *Privacy Act* be amended to require media organisations and the Australian Broadcasting Authority (now the Australian Communications and Media Authority) to consult with the Privacy Commissioner when developing standards under s. 7B(4). A definition of 'in the course of journalism' and a tighter definition of 'media organisation' are also recommended (OPC, 2005, recommendations 58-59 p. 199).

> *5–10 Should acts and practices of media organisations in the course of journalism be exempt from the operation of the Privacy Act? If so: (a) what should be the scope of the exemption; and (b) does s 7B(4) of the Privacy Act strike an appropriate balance between the free flow of information to the public and the protection of personal information?*
>
> ***Submission 5-10: This exemption should be reviewed. While there are serious issues about the balance between privacy rights and freedom of expression, and about the legitimate public interest role of the media, these issues should be addressed with selective exceptions to some of the principles, if justified, rather than by a blanket exemption.***

International standards are not a major factor in determining policy here. Article 9 of the EU Directive also provides for a similar exemption – requiring derogation from the main body of provisions in the Directive (i.e., those in Chapters III, IV and VI) insofar as the processing of personal data 'is carried out solely for journalistic purposes or the purpose of artistic or literary expression' and the derogation is 'necessary to reconcile the right to privacy with the rules governing freedom of expression'.[70] These provisions are also, on their face, somewhat nebulous with key terms (such as 'journalistic purposes') left undefined. Their potential breadth is illustrated in recent case law applying the notion of 'journalism' to cover website publishing of certain personal information by a person who was not a professional journalist.[71] Nevertheless, the exemption for media organisations in the *Privacy Act* arguably goes further than Art. 9 of the EU Directive given that application of the exemption does not turn on a dynamic assessment of the 'necessity' of reconciling privacy interests with freedom of expression. This should be a point of concern for the Commission, even though it was not raised by the Article 29 Working Party in Opinion 3/2001. At the same time, it should be remembered that some national transpositions of the EU Directive also fail to provide for such a dynamic 'necessity' assessment,[72] as does, for example, Canadian legislation.[73] Case law of the ECJ does not deal directly with the validity of a static approach. The changes proposed by the Privacy Commissioner in 2005, if implemented, would bring the Australian exemption closer to the EU Directive.

> *5–11 Should the terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' be defined in the Privacy Act? If so, how should they be defined? Are there other terms that would be more appropriate?*
>
> ***Submission 5-11: See our answer to Q 5-10 above. If there are to be selective exceptions for public interest media activity, the relevant terms will need to be much more carefully and closely defined. While difficult, it must be possible to distinguish between genuine news and current affairs journalism and the infotainment, entertainment and advertising which makes up the bulk of media content.***

---

[70] See too Recitals 17 and 37 in the preamble to the Directive.

[71] See judgment of 12.6.2001 by the Swedish Supreme Court (case B-293-00). The judgment is summarised and analysed in Bygrave, 2002b.

[72] See eg s 7 of Norway's *Personal Data Act 2000* (*lov om behandling av personopplysninger av 14 april 2000 nr 31*).

[73] See Canada's *Personal Information Protection and Electronic Documents Act 2000*, ss 4(2)(c), 7(1)(c).

5–12 If the media exemption is retained, how should journalistic acts and practices be regulated?

Submission 5-12: See our answers to Qs 5-10 & 5-11 – we do not believe the media exemption should remain in its current form

Related bodies corporate

5–13 Do any issues arise concerning related bodies corporate, changes in partnership and overseas acts required by foreign law in Part III Division 1 of the Privacy Act? If so, how should they be dealt with?

The 'related bodies corporate' exemption in s.13B is very broad and can result in uses of information being allowed which are contrary to the reasonable expectations of individuals. Many corporate relationships are obscure and customers of one trading enterprise are often unaware of other ownership or control relationships. The law should require businesses to legitimise transfers of information to related bodies corporate by informing individuals. There seems no reason to have a special exemption – businesses should be able to meet one of the tests in the exceptions to NPP2.

A specific issue taken up by the House of Representatives Committee in its inquiry into the 2000 private sector amendments was the application of this exemption to direct marketing. While the Committee's general conclusion on the exemption was that it is not as dangerous as it looks, they noted that NPP 2.3 means that although the related corporations provision allows information to be disclosed by corporation A to related corporation B, it is the primary purpose of collection of corporation A that determines what use corporation B can make of the information according to the 'reasonable expectations' test. This is generally true, but not (as was pointed out to the Committee) in relation to the direct marketing exception in NPP 2.3(c), which is why corporate groups are so keen on this provision. In our example, B can send direct marketing to A's customers (with an opt-out of course) without worrying about why A collected the information. [74]

Other exemptions

5–14 Are there any other entities or types of activities that should be exempt from the operation of the Privacy Act? If so, what are those entities or types of activities, and what should be the scope of the exemption?

Individual persons who process personal data in a non-business capacity are currently exempt (Privacy Act s 7B(1)). This is reinforced in s. 16E which provides that the NPPs do not apply to processing by an individual carried out solely for the purposes of, or in connection with, his/her 'personal, family or household affairs'. Reading both provisions together, the exemption seems consistent with European standards and to correspond with Art. 3(2) second indent of the EU Directive (as construed by the European Court of Justice in the *Lindqvist* case).[75]

---

[74] The Committee's recommendations would have imposed some checks on this intra-corporate spamming, if adopted. They wanted the Privacy Commissioner to issue guidelines concerning compliance with NPP 1.3(d) as to what companies should tell consumers about potential disclosures to their related corporations (Recommendation 21). It is a good point that, once a company has a disclosure practice to related corporations, NPP 1.3(d) requires it to be revealed during collection, but this cannot deal with the post-collection decision to disclose to a related corporation. The Committee also recommended that where corporation A has received personal information from a related corporation B that was exempt from NPP 1 when it collected the information (e.g. B might be a small business, or the information might be exempt employee information), corporation B will have to comply with NPP 1 before it discloses the information to A. In doing so, it would presumably have to inform the person concerned that his or her information was being disclosed to A. These recommendations were rejected by the Government.

[75] Judgment of 6.11.2003 in Case C-101/01 *Bodil Lindqvist* [2003] ECR I-129711.

There has been considerable media attention recently about 'objectionable' practices by individuals such as voyeuristic photography and internet publication of unwelcome information by one individual about another. However, we suggest that these issues are best dealt with by other civil law measures, including a tort of privacy, and criminal laws where appropriate.

> ***Submission 5-14: The current exemption for 'personal, family or household affairs' should be retained.***

We do not see the need for any other total exemptions, and are not aware of any other entities or types of activities which need selective exceptions. Carefully designed selective exceptions should be able to accommodate any new or currently unrecognised compliance difficulties.

Powers of the Privacy Commissioner (Ch 6)

Overall effectiveness of the legislative scheme

> *6–1 Is the legislative structure pertaining to the Office of the Privacy Commissioner established under the Privacy Act appropriately meeting the needs of the community?*

We see no basis for considering that the 'Privacy Commissioner model' of privacy regulation is unsound. The lack of adequate enforcement of the Act can be remedied. As the title of this submission suggests 'after 20 years it's time to enforce the Privacy Act', but the inadequacies of the OPC's current practices have become more apparent since the Act was extended to the private sector generally.

Private sector compliance as a test of effectiveness - Submissions to the OPC review differed widely on their assessments of the level of compliance in relation to the private sector. The OPC summarises the view of most organisations and business groups as being that 'the overall level of compliance is good and the Office's approach is working well' (OPC, 2005, p. 131). In contrast, 'the perceived lack of enforcement mechanisms in the Privacy Act especially in relation to determination enforcement is a matter of strong concern amongst the advocacy and consumer groups' (OPC, 2005, p. 133). The OPC considers from its experience that 'many organisations have taken substantial steps to ensure that they comply' and that the number of complaints received by these organisations is low relative to the numbers of transactions they process (OPC, 2005, p. 146). It acknowledges, though, that these factors are not a basis for definitive conclusions – in part due to the existence of a variety of reasons for people's hesitancy about complaining (OPC, 2005, p. 147). The OPC also observes that levels of compliance appear to vary from sector to sector (OPC, 2005, p. 148). There is, furthermore, considerable sectoral variation in terms of complaint levels.[76]

Levels of satisfaction regarding complaint resolution - Given the key role of complaint investigation by the Privacy Commissioner in the *Privacy Act 1988*, a high level of satisfaction by both complainants and respondents would be some indication of a 'good level of compliance' (to use European terminology). As well as being an important part of compliance in themselves, complaint resolutions that are accepted by both sides can indicate a broader acceptance of the rules in the community. Appendix 14 of the private sector review report summarises the results of a survey in February/March 2005 of satisfaction levels of 100 complainants and 41 respondents. On every criterion of satisfaction measured (timeliness, impartiality, process information, communication of reasons, satisfaction with service and satisfaction with outcomes) complainants were far less satisfied than respondents. In some cases, the disparities in satisfaction were large: only 43% of complainants were satisfied with outcomes, but 86% of respondents were satisfied. In addition, 41% of complainants considered the service poor, and 56% did not think they had been dealt with fairly. These results do not create confidence that the complaints process is itself causing a greater level of compliance by demonstrating that the Act is being enforced. To the contrary, they raise fears that the complaints process may be demonstrating to respondents that they have little to fear from the OPC. An alternative, but implausible, explanation is that a very large percentage of complainants have unjustified complaints, and remain dissatisfied with outcome and service despite good communication of reasons and fair treatment.

We have argued previously (Greenleaf and Waters, 2004) that:

> The result of this 'softly softly' approach pursued by all the Commissioners to date is that many organisations regard privacy compliance as optional. Privacy Act obligations cannot be totally ignored, at

[76] Numbers of complaints relating to alleged breaches of NPPs have far outstripped numbers of complaints relating to alleged breaches of IPPs.

> least where this would be visible. Most larger organisations feel obliged to comply with the 'notice' requirements, although many privacy statements are inadequate. Privacy is also often thrown in as a further justification for increased security measures required for other reasons. Access to a person's own record is also now more likely to occur. But beyond these steps, few organisations have felt it necessary to seriously address issues of whether collection is necessary, proportionate and fair, whether uses and disclosures are in fact compliant with the relevant principles, or whether records are accurate and relevant.

We have seen nothing in the intervening years to justify any change of opinion.

Complaint outcomes as a measure of success - One indicator of the successful operation of a complaints-based system is whether individual complainants do get the remedies that the legislation provides in theory. In relation to the Commonwealth public sector, the unsatisfactory information that is available indicates that 'there is no substantial evidence that the Commissioner enforces the Act against Commonwealth agencies in any way that produces remedies for complainants' (Greenleaf 2006c):

> Of the approximately 200 public sector complaints in 2003-04, preliminary enquiries by the Commissioner found a breach in 16% of complaints and investigations found a possible breach of the IPPs in 38% of complaints. The nature of the complaints was as follows: agencies disclosing personal information (55%);data security (18%);failure to check the accuracy of personal information before use (17%); and collection of personal information (12%). It is consistent with complaint patterns in other jurisdictions that a majority of complaints should be about improper disclosures.
>
> One indicator of the successful operation of a complaints-based system is whether individual complainants do get the remedies that the legislation provides in theory. A complaint system that does not demonstrate that it delivers these remedies is suspect. In 62% of the cases investigated and 84% in which preliminary enquiries were made, no breach of privacy was found. (OPC, 2003-4). What then happened in the 38% of cases investigated where breaches were found ? Unfortunately, the OPC does not publish any systematic information about remedies granted,.so we are forced to generalise from the few complaint summaries published.
>
> In 2004, the Commissioner published 19 complaint summaries, of which only three related to public sector agencies. Two of these were simply illustrative examples of where the Commissioner declined to investigate because there was no breach ([2004] PrivCmrA 13), or because another law provided a more appropriate remedy ([2004] PrivCmrA 8)**.** In the one remaining case (*X v Commonwealth Agency* [2004] PrivCmrA 4) the Commissioner found on the balance of probabilities, the agency's employee did disclose to the complainant's ex-partner that the complainant was to receive money from a court settlement, allowing the complainant's ex-partner to obtain a court order restraining the complainant from accessing that money.— Because the complainant wished to be in a position to pursue action against the agency in the courts, OPC ceased its investigation of the complaint.
>
> 2004 is a typical year: there is no substantial evidence that the Commissioner enforces the Act against Commonwealth agencies in any way that produces remedies for complainants. Perhaps he or she does enforce it effectively – but there is little evidence of this. Breaches are found in 38% of cases – about 75 per year – but only one such breach is summarised by the Commissioner–. Outcomes in the other complaints are unknown. The Australian Commissioner's non-reporting makes the office unaccountable, and squanders the potential deterrent effect of the Act. Other Asia-Pacific Privacy Commissioners are also opaque in their enforcement practices (Greenleaf 2003), though perhaps not to this extent.

Concerning enforcement in the private sector, a conclusion in 2006 was that 'For the past four years since the private sector provisions have operated, we have scant evidence of effective enforcement.' (Greenleaf, 2006c):

> Only one enforceable order ('s52 determination') has been made against a private sector body (TICA determinations, 2005). Taking 2004-05 figures as a guide, of 1144 complaints closed during a year, most are closed without investigation (about 60%), and the rest after preliminary enquiries or investigation. These include about 15% of complaints where the Commissioner thinks 'the respondent has dealt adequately with the matter)'. In about 5% of cases this view is formed after the Commissioner investigates, reaches a provisional view that there is a breach of the Act, and then attempts to conciliate. No details of the outcomes of these conciliations are provided except that the resolutions include 'provision of access to records, correction of records, apologies, change to systems, [and] amounts of

> compensation ranging from less than $500 to $20,000' (OPC Annual Report 2004-05, 3.4.2.1-3). When we turn to the 22 complaint summaries published by the Commissioner in 2004-05 (OPC complaints 2004-05), chosen for their significance, none of them involve any financial compensation, let alone such a significant sum as $20,000. The summarised complaints are mainly variations on how complaints are dismissed, and none involve significant systemic changes. This is a very substantial failure of accountability: if the Commissioner's office, with an annual budget of A$5M, does anything to remedy individual complaints, they keep it to themselves.

This study does not take into account 2005-06 statistics, but we have no reason to think they lead to different conclusions.

> ***Submission: The OPC's own report gives reasons to conclude that there is significant community dissatisfaction with the way in which it carries out its responsibilities. The information available about complaint outcomes reinforces this. The Discussion Paper should examine this matter carefully, as there is no point having an Act containing sound privacy principles if they are not being effectively enforced for the benefit of the community.***
>
> ***Submission 6-1.1: The Office of the Privacy Commissioner should be retained. However, it should be made more transparently accountable for how it carries out its responsibilities.***

Commissioner's powers

> *6–5 Are the Privacy Commissioner's powers to oversee the Privacy Act appropriate and exercised effectively? For example, are the Commissioner's powers: (a) to furnish advice; (b) to research and monitor developments in data processing and computer technology; (c) to promote understanding of the IPPs and of the objects of the IPPs and the NPPs; (d) to undertake education programs to promote individual privacy protection; (e) relating to tax file numbers; (f) arising under other Acts, appropriate and exercised effectively?*

The Commissioner's Office has improved its practices in recent years in making information about its submissions etc more readily available to the public, particularly through its website and through email notifications to interested parties. However, all existing legislative impediments to greater transparency should be removed.

> ***Submission 6-5: The Commissioner's powers to report are unnecessarily circumscribed, in particular in those powers in s27 which only allow reports to be made to Ministers. The Commissioner should have an additional explicit power under s27 to report to the public, or make a special report to the Parliament, on any of the matters listed otherwise in s27, with as few exceptions as possible.***

Privacy impact assessments

> *6–6 Should the Privacy Act require a privacy impact assessment to be prepared for: (a) all proposed Commonwealth legislation; (b) other proposed projects or developments of agencies; or (c) other proposed projects or developments of organisations?*

Privacy Commissioners have been promoting Privacy Impact Assessment (PIA) as a tool for some time.[77] The federal government has endorsed this call at least in respect of Commonwealth

[77] Both the Commonwealth and Victorian Privacy Commissioners have issued Guides to PIA.

agencies.[78] If the technique of PIA is seen as only applicable to public sector agencies, it is probably best dealt with in another part of the Privacy Act. But if it is recognised as relevant to some major private sector projects as well (as are Environmental Impact Assessment and, increasingly, Social Impact Assessment) then it is could best promoted by means of an additional principle applying to all data users, with some defined criteria for when a project would need a PIA.

One model for such a principle would be the requirement placed on US federal government agencies in 2002, mandating an assessment of the privacy impact of any substantially revised or new Information Technology System.[79] There is also an obligation on Canadian federal agencies to conduct PIAs (Greenleaf 2002).

> ***Submission 6-6: The Discussion Paper should canvass the merits of an additional principle requiring Privacy Impact Assessments for significant projects or developments of organisations in both the public sector and the private sector.***

Personal information digest

The Personal Information Digests (both Commonwealth and ACT) have not been used as effectively as they could be. They should provide a valuable research tool, for academic inquiry, Parliamentary scrutiny and investigative journalism.

> *6–8 Is the Personal Information Digest published in a useful manner? If not, how might it be improved? Is the record itself useful?*

The Digest is currently less useful than it could be because, although it is published on the Internet,[80] it is only available as compressed ('zipped') files. It would cost little to greatly increase its utility by making it available in a free-text searchable form, and browsable at least by name of agency. Other publishers, including those who are interested in 'watching the watchers', should be able to re-publish the content of the Digest with different form of search facilities added, so as to make it easier to track the extent of use and interconnection of personal information.

> ***Submission 6-8: The Digest should be retained and improved, and should be published on the Internet in as flexible a searchable form is possible, and with re-publication of the information by others allowed.***

The Digest would be much more useful if the Commissioner could fashion it as an instrument to disclose more information to the interested public, and to the Commissioner's own office, about those information systems which are considered to pose more potential threat to people's privacy interests, rather than there being a 'one size fits all' approach which tends to obscure which are the most sensitive and significant personal information systems.

> ***Submission 6-8.1: The Commissioner should be able to vary the amount of information required to be submitted by an agency, or to excuse an agency from submitting any information. Such a requirement should be subject to Parliamentary review by way of a disallowable instrument.***

Used carefully, such a requirement could also be imposed on privacy sector organisations, although

> ***Submission 6-8.2: The Digest requirements should not be extended to the private sector generally, but the Commissioner should be able to require a private sector***

---

[78] Attorney-General Philip Ruddock, speaking at the launch of the Privacy Commissioners revised Guide to PIA in August 2006.

[79] By the E-Government Act 2002.

[80] See <http://www.privacy.gov.au/government/digest/>.

> ***organisation, or a class of private sector organisations, to submit information similar to that which is submitted by agencies, and publish it in the Digest. Such a requirement should be subject to Parliamentary review by way of a disallowable instrument.***

Location of Commissioner's functions

> *6–11 Should all the Privacy Commissioner's functions be consolidated in the Privacy Act?*

If the Commissioner's functions and powers are scattered through different pieces of legislation it is inevitable that they will be expressed in different forms even where the intent is the same. This will lead to both inconsistent interpretations of what should be a similar function /power and 'reform lag' where a power or function is improved by amendment in one Act but not in another. However, it is equally important that, wherever the Commissioner has a function, that the Commissioner's role be apparent from other legislation concerning that subject matter. It is highly desirable that as many as possibly of the Commissioner's functions be located in the Privacy Act, but only if the other legislation to which the function relates contains an explicit cross-reference to the Commissioner's role and the Privacy Act function.

> ***Submission 6-11: It is highly desirable that all of the Commissioner's functions be located in the Privacy Act, but only if any other legislation to which the function relates contains an explicit cross-reference to the Commissioner's role and the Privacy Act function.***

Complaint resolution powers

> *6–12 Are the procedures under the Privacy Act for making and pursuing a complaint, including a representative complaint, appropriate? Are the Privacy Commissioner's powers to make preliminary inquiries and investigate complaints appropriate and effective?*
>
> *6–13 Is the obligation of the Privacy Commissioner to investigate a complaint about an act or practice that may interfere with the privacy of an individual appropriate, and is it administered effectively?*
>
> *6–14 Is the power of the Privacy Commissioner to investigate an act or practice that may interfere with the privacy of an individual appropriate, and is it used effectively?*
>
> ***Submissions 6-12, 6–13, 6-14: The Commissioner's powers in relation to complaint investigation are generally adequate, the problem lies elsewhere.***
>
> *6–15 Are the Privacy Commissioner's powers relating to the conduct of investigations appropriate and exercised effectively? For example, are the Commissioner's powers regarding [(a) – (g)] appropriate and exercised effectively? .... (g) reports ,*

There are particular problems with the lack of transparency of the complaints process. These are detailed below under 'Other issues – Inadequacy of the Commissioner's reporting practices'.

> ***Submission 6-15: The Commissioner's powers are not exercised appropriately or effectively in relation to reporting on complaint outcomes (see below).***

6–16 Are the Privacy Commissioner's powers under the Privacy Act to make determinations appropriate and administered effectively?

A right to obtain a determination It is clear from *X v Commonwealth Agency* [2004] PrivCmrA 4, and from comments on the OPC website that complaints will be dismissed under s41(2)(a) if the Commissioner is satisfied that the respondent has dealt adequately with the complaint, even if the complainant does not agree (Greenleaf 2004a). In that case the Commissioner could have proceeded to make a determination under s52 finding a breach and determining a remedy, even if the complainant did not agree it was adequate. If compensation was ordered the complainant could appeal against the amount to the AAT if he considered it inadequate. If other remedies, or none at all, were determined to be necessary then the complainant would still have the satisfaction that the respondent's breach of the NPPs was acknowledged publicly by the Commissioner. Even if the complaint was dismissed by a s52 determination, the complainant would have a more detailed decision on which to found a action for judicial review. For all of the above reasons, a dissatisfied complainant should be able to insist that a complaint be dealt with by a s52 Determination (as argued in Greenleaf 2004).

It does not seem from the Act that a complainant has any such right, and it does not seem to be practice of the Commissioner to offer complainants such an option, as shown by the above complaint and by subsequent events. The Commissioner's review of the Act (OPC 2005, Recommendations 37 and 42) concluded that the Commissioner 'expected' to make more determinations under s52, but made no commitment to do so at the request of dissatisfied complainants. The Commissioner's subsequent statement on this (OPC 2006) says nothing at all about given complainants any right to request a determination, or even that they will be told they can request one. It does say that parties to complaints will be given some unspecified information about s52 determinations.

It is now the best part of two years since the Commissioner concluded that she 'expected' to make more s52 determinations, and she has not yet issued one since then. IN fact, the current Commissioner has never made any s52 determinations. The previous Commissioner made 6, but four of those were on the same matter. The first Commissioner made two back in 1993, but then there was a decade's wait until the next on in 2003. A reasonable observer could only conclude that Australian Privacy Commissioners are pathologically adverse to using the only power that the Act gives them to determine complaints.

The well-known theory of 'responsive regulation', which appears to have been endorsed by the previous Privacy Commissioner (Crompton, 2005), posits a pyramid or hierarchy of enforcement options, credible use of the whole pyramid of options, and various types of transparency and feedback mechanisms. Ayres and Braithwaite have summarized some key aspects of their theory of responsive regulation as follows (Ayres and Braithwaite, 1992):

> Chapter 2 seeks to solve the policy problem that regulatory styles which are cooperative on the one hand or punitive on the other "may operate at cross-purposes because the strategies fit uneasily with each other as a result of conflicting imperatives." … it is contended that the achievement of regulatory objectives is more likely when agencies display both a hierarchy of sanctions and a hierarchy of regulatory strategies of varying degrees of interventionism. The regulatory design requirement we describe is for agencies to display two enforcement pyramids with a range of interventions of every-increasing intrusiveness (matched by ever-decreasing frequency of use). Regulators will do best by indicating a willingness to escalate intervention up those pyramids or to deregulate down the pyramids in response to the industry's performance in securing regulatory objectives.
>
> Finally, it is argued that the greater the heights of tough enforcement to which the agency can escalate (at the apex of its enforcement pyramid), the more effective the agency will be at securing compliance and the less likely that it will have to resort to tough enforcement. Regulatory agencies will be able to speak more softly when they are perceived as carrying big sticks.

Theorists such as Braithwaite and Christine Parker also stress that responsive regulation contains a 'storytelling orientation' where stories about the implementation each level of the enforcement pyramid - both successes and failures – are made known to the various classes of stakeholders in the regulatory system (including those who are regulated, the intended beneficiaries of this, and those responsible for assessing its effectiveness). Braithwaite says that one test of responsive regulation is how good a system is in 'bubbling up' stories of its successes and failures, provided these stories have credibility as being representative, and that this applies to privacy regulation [81].

Using these criteria, the OPC is a failure at implementing responsive regulation. The apex of its pyramid of enforcement, s52 determinations, has lost credibility because the OPC simply does not use it. Nor does the OPC publish any compelling 'stories' to demonstrate that it does not need to use it, such as large compensation settlements achieved *in terrorem* of a larger s52 award. Nor does it allow complainants to require a s52 determination, so the lack of them is no credible assurance that they are not needed. As will be discussed later, their reporting mechanisms lack any objective credibility.

> **Submission *6–16*: *The Commissioner's powers to make determinations are not administered in the best interests of complainants. The Act requires clarification that a complainant or respondent should be able to require that the Commissioner deal with a complaint by way of a s52 determination rather than under s41. This is also necessary if the proposed right of appeal against s52 Determinations (see below) are to be meaningful, as the right of appeal could then be avoided by dismissing a complaint under s41.***

Own-motion investigations - The OPC may also conduct an 'own-motion investigation' – i.e., investigate a matter without having received a complaint (s. 40(2)). This discretionary power will typically be exercised when there is evidence of a serious privacy breach with significant implications for the public interest.[82] The OPC lacks power to enforce an 'own-motion investigation' conducted under s. 40(2). The 2005 private sector review report notes that the OPC has experienced some problems in dealing with uncooperative respondents and that its lack of formal enforcement powers here may not be in line with the powers of similar regulators (OPC, 2005, p. 155). It recommends that it be granted additional powers to enforce own motion investigations (OPC, 2005, recommendation 44, p. 163). The Commissioner has started in 2005 to publish summaries of some own motion investigations, but we don't know how selective this is. This power also falls short as responsive regulation because its exercise is largely unknown.

> ***Submission 6-16.1: The Commissioner should be given power to make and enforce determinations as a result of an 'own motion' investigation. Such own motion investigations should be the subject of public notice by the Commissioner, and procedures developed for appropriate intervention by other interested parties (such as NGOs in the relevant area). The Commissioner should be able to make a special report to Parliament of the results of an own motion investigation.***

---

[81] John Braithwaite discussed theories of responsive regulation and privacy regulation in an address to the Seminar held by the APEC Privacy Sub-Group of the ECSG, Canberra, January 2007, but the application of his remarks is ours.

[82] See further OPC (2005), Appendix 10.

Enforcing determinations

6–17 Are the Privacy Act provisions for enforcing determinations adequate and administered effectively?

Lack of appeal rights The principal deficiency in the Act in relation to determinations is the lack of any right of appeal by complainants who are dissatisfied with the Commissioner's determination of a complaint (assuming they can obtain a determination in the first place). In our submissions to the Government and to Parliament on the Bill leading to the private sector provisions we stressed (as did other commentators) that the lack of any right of appeal against s52 determinations (to the Federal Court, Federal Magistrates Court, or at least to the AAT), was extremely unfair to complainants. The arguments that were ignored in the drafting of the private sector legislation were picked up in the OPC's Issues Paper (prior to OPC 2005), which noted that of the reasons for this unfairness is that 'Respondents have the possibility of having a case heard afresh by refusing to comply with a determination and waiting for the Commissioner to seek to have the case enforced in court. However, this strategy is not available to an aggrieved complainant.' As we reiterated in our submission to the OPC (Greenleaf 2005), a respondent to an unfavourable complaint determination made under s. 52 can effectively obtain full judicial review (i.e., review of the merits) of the determination by simply refusing to abide by it, given that court enforcement of the determination may only occur on the basis of a Federal Court hearing *de novo* of whether the respondent has breached the complainant's privacy (s. 55A(5)). The Act does not afford complainants with a similar review possibility and for this reason the procedure can be seen as biased in favour of respondents.

Judicial review of the Commissioner's decisions (either a s. 52 determination or a decision to cease investigation of a complaint under s. 41(1)) may always be sought by either complainant or respondent pursuant to the *Administrative Decisions (Judicial Review) Act 1977* (Cth), but such review will not address the merits of the Commissioner's policy choice except insofar as an error of law is involved.[83] The OPC website stated in 2005, seemingly misleadingly, 'If the Federal Privacy Commissioner closes your file and you disagree with that decision, you can appeal to the Federal Court or the Federal Magistrates Court.' In fact a complainant cannot appeal against such a s41 decision in the sense of seeking a merits review of the decision, but can only seek judicial review which the Issues Paper acknowledges is 'limited to reviewing the legality of the decision.'

Quite apart from the inherent bias toward respondents in the Act as it stands, it is unfair, unnecessary, and counter-productive to responsive regulation that there should be no appeal from determinations by the Privacy Commissioner. Some of the many reasons are:

- The OPC's errors in interpreting the principles and applying the Act remain hidden from the scrutiny that Courts would provide through the appeals process.
- The Courts have not had, for 20 years, the opportunity to interpret the *Privacy Act* and tell us what it means as a matter of law. We all imagine we know what it means – including the OPC – but an Act of the Privacy Act's complexity which has no judicial decisions to guide our understanding of it is in truth rather limited. It's still *terra incognito* in many respects (see Greenleaf 2000).

---

[83] See also *Mario Riediger v Privacy Commissioner* [1998] FCA 1742 (23.9.1998), unreported, *per* Einfeld J (dismissing application for judicial review under *Administrative Decisions (Judicial Review) Act 1977* (Cth) of OFPC decision under s. 41(1) of *Privacy Act* not to investigate complaint): 'the Federal Court's jurisdiction in these matters is limited to the review of any error of law made by the Commissioner in the course of his decision …[…] [A]n application of this kind must reveal … an error related to the making of the decision itself, for example, a denial of natural justice, manifest unreasonableness, the taking into account of irrelevant considerations, and so forth … [T]he Court simply cannot revisit the merits of the … complaints …' (para. 8).

- The OPC has at some points had inadequate resources to properly carry out its complaint investigation function, and under such circumstances it is even more important than usual that there is a possibility of review of decisions of fact involved in a complaint and not only errors of law and procedure.

This is anything but 'responsive regulation'. No feedback comes from the judicial system. It is more like frozen regulation. This is probably the principal deficiency of the complaints regime of the *Privacy Act 1988*. The OPC has recommended that the government consider amending the Act to give both complainants and respondents a right to have the merits of complaint decisions reviewed (OPC, *2005,* Recommendation 40). Not surprisingly, we agree.

> **Submission 6-17:** ***Both complainant and respondent should have a right of appeal against any s52 determination, in the form of a merits review. Whether this is to the Federal Court, Federal Magistrates Court, or the AAT, is of less importance.***

In terms of international standards, the EU Directive requires that decisions of supervisory authorities 'may be appealed against through the courts' (Art. 28(3)). The Article 29 Working Party does not single this out as a necessary part of an adequate enforcement mechanism, but it is clearly a valuable component given that it receives separate mention in the Directive.

> **Submission 6-17.1:** ***The lack of merits review of s41 decisions can best be addressed by providing complainants with the rights to insist on a s52 Determination, once there is a right of appeal against s52 Determinations.***

Injunctions

> *6–19 Are the Privacy Act provisions for obtaining injunctions adequate and effective?*

In theory, the power to seek an injunction to prevent privacy-invasive practices from continuing is the 'twin peak' of the Commissioner's pyramid of enforcement options. The Commissioner has never sought to obtain an injunction (or even threatened to, as far as is known), and so has in effect surrendered the potential effectiveness of this power as a tool for responsive regulation. The corollary of this is that few organisations would ever be aware that there was a possibility that the Commissioner could seek an injunction against their practices.

The Commissioner's ability to seek an injunction is potentially a particularly valuable aspect of the Privacy Act as regulation, because it carries with it the requirement that the Commissioner must also seek an interpretation of the Act by the Federal Court, rather than applying what the Commissioner's Office imagines is the law. Given that there are no useful decisions on the *Privacy Act* after 20 years – except one where one commercial parties used the injunction provision against another (Greenleaf 2004b) – the opportunity for the Commissioner to seek judicial guidance on difficult aspects of the Act would be a rare and valuable opportunity, but it is one the Commissioner has never taken up.

The ability for complainants to seek an injunction as an alternative to the long wait to have complaint considered by the Commissioner is inherently valuable. Alternative avenues of enforcement are generally a good thing, in our view, and it would be desirable for complainants, in cases that are serious enough, to have an effective means of bypassing the Commissioner and going directly to the judicial system for remedies. Likewise, the ability for NGOs to seek injunctions, because of the lack of a standing requirement in s98, is a theoretically valuable means by which contesting interpretations of principles could be resolved. However, unless complainants or NGOs have the resources to risk costs being awarded against them when they seek an injunction, and possibly damages if they seek an interim injunction, they cannot utilise these opportunities. Twenty years experience shows that none have even tried to do so.

> ***Submission 6-19: The s98 injunction provisions are valuable in theory, but ineffective in practice. The Discussion Paper should consider means by which the use of s98 by the Commissioner, by NGOs and by complainants can be made more effective.***

Compliance model and remedies

> *6–21 Is the current compliance model used in the Privacy Act appropriate and effective to achieve the Act's purposes? If not, is that because of its content, its administration, or some other reason?*

A sound compliance model is crippled by both structural flaws and inadequate enforcement.

> ***Submission 6-21: The current compliance model used in the Privacy Act is appropriate in its essential features, but it has major deficiencies including lack of appeal rights and lack of a right in complainants to demand determinations (see submissions above), as well as a lack of transparency (see submissions to follow). At present it is not effective to achieve the Act's purposes.***

The 'palm tree justice' flavour of the administration of the *Privacy Act* has been contributed to by a succession of Commissioners who are not lawyers, and who do not seem to take the Act seriously enough as legal regulation and a rights-based regime, but rather see it primarily as a platform to exhort better business and government practices. This is a subjective view from an outside perspective, and would no doubt be rejected by many people associated with the OPC.

> ***Submission 6-21.1: The compliance model is also ineffective because of its administration, which is unduly adverse to transparency, enforcement of the Act, and clarification of the Act by the Courts.***
>
> *6–22 Does the range of remedies available to enforce rights and obligations created by the Privacy Act require expansion? For example, should the available remedies include any or all of the following for particular breaches of the Act: (a) administrative penalties; (b) enforceable undertakings or other coercive orders; (c) remedies in the nature of damages; (d) infringement notices; (e) civil penalties; (f) criminal sanctions?*

When making a determination under s. 52, the OPC is not able to apply systemic remedies; i.e., remedies that attempt to prevent future problems related to general patterns of behaviour or processes (beyond those directly related to the specific complaint giving rise to the determination). In other words, the OPC is unable to prescribe *generally* how a respondent should act. The problematic aspect of this shortcoming is noted by the OPC in relation to its Determination No. 2 of 2004 (on tenancy databases). In its 2005 private sector review report, the OPC notes the problems it has in prescribing systematic changes in s. 52 determinations, (OPC, 2005, pp. 157-159) and recommends that the Commissioner be given additional 'power to require a respondent to take steps to prevent future harm arising from systemic issues' (OPC, 2005, recommendation 44, pp. 163).

> ***Submission 6-22: The Commissioner's powers in the Act should be clarified so that it is clear that the Commissioner can prescribe* generally *how a respondent should act.***

Transparency and feedback – Inadequacy of the Commissioner's reporting practices

The following submissions are primarily drawn from Greenleaf 2004, updated for subsequent developments.

Lack of a complaints procedure manual There is no published manual of the procedures used, and policies adopted, by the OPC in its investigation and resolution of complaints. Potential complainants, respondents and organizations representing them, are left to infer these procedures

and policies from piecemeal and scattered complaint summaries which are infrequently issued by the OPC. The OPC issued ten Case Notes in mid-2004 which at first glance appeared to be a disappointing catalog of the ways in which the Commissioner could refuse to investigate complaints under s41. However, it is vital that these matters be documented, as it is by this means that the majority of complaints investigated by the Commissioner are dealt with. To take one of these as an example, *O v Credit Provider* [2004] PrivCmrA 5, the case note revealed important details of how complaints can be declined because a respondent is considered not to have had an adequate opportunity to deal with the complaint because the complainant had not raised a specific issue (compensation) with the respondent. There was potential for a considerable deal of unfairness to complainants in this practice, which required further clarification by the OPC. We said at the time (Greenleaf 2004c):

> 'Although the complainant had complained directly to the respondent, the Commissioner refused to investigate, under s41(2)(b), because the complainant had not raised the specific issue of compensation with the respondent.
>
> If this meant that a complainant lost his or her 'place in the queue' after waiting (say) six months to have their complaint dealt with by the Commissioner, because they had not raised every specific issue with the respondent even though they had raised the substance of the complaint with the respondent, it would be very unfair and would deter justified complainants.
>
> The Commissioner's Office has informed PLPR that it has a number of procedures to avoid this problem. First, it has what is in effect a triage system where complaints are assesses when first received, and if a complainant has not first complained to the respondent, the complaint is (usually) declined until this occurs. However, wherever investigation is declined but the complainant later returns to the Commissioner's Office having complained to the respondent (or for other reasons), the complainant's 'place in the queue' is dated from his or her initial approach to the Commissioner.
>
> Second, although the Commissioner's Office does expect the complainant to make a reasonable effort at raising their key issues with the respondent (and will refuse to investigate if this has not occurred, as here), .if some lesser aspect of the issue had not been raised with the respondent, the Office would give the respondent the opportunity to consider the issue in the course of the investigation (thus satisfying s40(1A)) rather than requiring the complainant to go back to the respondent directly.'

It should not be necessary for such important practices to be revealed in a piecemeal fashion (Greenleaf 2004). The need for a published Procedures Manual has been raised with the OPC on various occasions by privacy advocates, but nothing has happened.

Submission 6-22.1: The OPC should publish online a comprehensive manual of its complaint resolution policies and procedures, and keep it up-to-date.

Complaint outcomes – reporting In late 2002 the OPC commenced publishing brief summaries of some significant mediated complaints, for the first time since 1989. In four years, 72 have been published (11 in 2003;19 in 2004; 18 in 2005 and 22 in 2006 – though none since August), plus a few Determinations as mentioned. While this is significant increase on previous practice, it is still less than two per month.

Prior to most of the improvements in the OPC reporting practices, Greenleaf carried out a study 'Reforming reporting of privacy cases: A proposal for improving accountability of Asia-Pacific Privacy Commissioners' (Greenleaf, 2003), which summarized the importance of reporting complaint outcomes as follows:

> "If details of these complaint resolutions by Privacy Commissioners are not made effectively available to the interested public, the consequences are generally adverse. Some adverse consequences are as follows:
>
> - Potential complainants or respondents (or their professional advisers) have very little information about how the Act is interpreted by the Commissioner, and little idea what arguments they need to raise. It is irrelevant for this purpose that the Commissioner's decisions do not constitute legal precedents binding on himself or others.

- They know little about the remedies which have been granted in the past, and so have little guide as to whether a complaint is worth pursuing, or what might be a sensible stance to take in settlement negotiations. There is always a 'going rate' for any type of injury.
- Business, in particular, lacks certainty about how to comply with the law.
- If remedies granted for breaches remain unknown, it is easy to conclude the law is not enforced.
- Privacy remains a Cinderella area of legal practice, as it does not have what practitioners perceive as the most important indicia of 'real' law – decisions (cf. Bygrave, 2000).
- Scholars are hampered in the development of a privacy jurisprudence, as they have no basis for a critical analysis of how the Commissioner is interpreting the Act. To the extent that such decisions are available, they are used for such analysis[84].
- The press, consumer organisations and privacy advocates are impeded in keeping watch on the adequacy or fairness of Privacy Commissioners' decisions and remedies.
- The deficiencies of the laws being administered by Commissioners do not receive convincing illustrations which could be used by those pressing for law reform.
- Non-publication allows Privacy Commissioners to 'bury their mistakes', so that any misinterpretations of the law, and any failures to insist that government agencies and business interests provide adequate remedies in individual cases, are less likely to come to light.
- Even if a Privacy Commissioner is succeeding in resolving all complaints fairly and legally, the deterrent effect of publishing examples of what constitutes breaches (and the remedies that may follow) is lost. In this sense, valuable educative resources are squandered.
- Even if justice is being done, it is not being seen to be done.
- Privacy Commissioners are increasingly considering cooperating in the resolution of complaints with cross-border elements. To do so they will need to better understand each other's complaint resolution practices.
- Non-publication is inconsistent with full accountability for public funds. The principal statutory obligation of most Privacy Commissioners' Offices is complaint investigation and resolution, but the effectiveness and justice of a Commissioner's work cannot be fully assessed without individual case examples.

Of course, there are countervailing factors. Publication of complaint resolutions is only one aspect of the transparency and educational role of a Privacy Commissioner. Different views can be taken of where Privacy Commissioners, who often have inadequate resources, should place their priorities. Some Commissioners with a very effective record in other forms of public communication are very poor at reporting complaints, but we should not over-emphasise this since it is much easier and less contentious to publish 'feel good' information exhorting compliance with an Act than it is to identify those who fail to comply.

The need for complaint reporting is also sometimes difficult to reconcile with the desire to mediate a settlement between the parties, but this can usually be dealt with by anonymisation. Where it cannot, it should be a matter of case-by-case assessment, not a general reason for non-publication. ..."

We submit that these factors remain vital in explaining why the level and detail of reporting by the OPC, while a commendable improvement, is still not sufficient to play the role that reporting of examples can and should play in the overall administration of the *Privacy Act*. In particular, we have little idea of what criteria are used to select the tiny number of complaints of which details are reported, and no objective means of measuring whether these are a true reflection of OFPC practices. The OPC website only says 'Most cases chosen for inclusion in case notes involve new interpretation of the Act or associated legislation, illustrate systemic issues, or illustrate the application of the law to a particular industry.' This does not indicate that all cases meeting such criteria are published. Part III of Greenleaf (2003) recommended changes to Commissioners' reporting practices. Many of those recommendations are still relevant to the OPC's reporting

[84] See for example Beardwood, 2002; Evans, 2003.

practices, though some have already been dealt with by OPC practices. We submit the recommendations that remain relevant below. Supporting argument and examples are in the study.

> ***Submission 6-22.2: The OPC should be required to reform its procedures for reporting privacy complaints along the following lines: (i) adhering to publicly-stated criteria of seriousness of which complaints are reported; (ii) confirmation in each Annual Report that these criteria for reporting have been adhered to; (ii) naming complainants who elect to be named; (iv) naming private sector respondents where the interests of other potential complainants or the public interest justifies this; and (v) naming all public sector respondents except where this would cause serious harm to the interests of the complainant or another person; and (vii) providing sufficient detail in complaint summaries for them to useful to interested parties.***

We make the following submission of detailed recommendations to support 6.22.2 above, based on Greenleaf (2003):

> *Criteria of seriousness* A set of publicly stated criteria of seriousness on the basis on which a Commissioner's Office decides that a summary of the complaint resolution should be published. The following seven criteria of seriousness are recommended for consideration.
>
> - If a complaint involves the exercise of enforcement powers by a Commissioner,(where a Commissioner has such powers) then this is a strong indicator that it is significant, unless it is merely repetitive of many other complaints. If the numbers are small, all such complaints should be reported to avoid any need for selection.
> - Although a complaint is dismissed because it does not involve a breach of IPPs or an Act (or for another reason), it is still significant if its dismissal involved a new interpretation of the law (or its application in a significant new context). It may also be significant in demonstrating that certain practices of public bodies and companies do not breach privacy laws (which may or may not be controversial).
> - Although a complaint is settled to the satisfaction of the parties, it is still significant if it involves a new interpretation of the law (or its application in a significant new context). Mediation may involve conditions being imposed on what can be reported, and requirements of anonymity, but is not in itself a reason for non-reporting.
> - If a case involves a different example or a remedy, or the provision of a remedy on a scale which is new, it is significant even if no new interpretation of the facts is involved.
> - Even if a complaint involves no new interpretation of law, or no new/greater remedy, repeated examples of very important types of complaints are worthwhile. However, separate but similar complaints should not be bundled together, as this confuses the facts of cases and impedes consistent citation mechanisms.
> - Findings that are contested by one of the parties to the complaint are usually worth reporting, as they may indicate both significant areas of disagreement within the community (and so law reform might be desirable), or areas where the Commissioners' interpretation of the law could be questioned.
>
> The criteria of 'seriousness' will change over time, with illustrative complaints being more valuable in the early years of administration of new legislation, even if no significant interpretations or remedies are involved (eg first application in an industry).
>
> *Adherence to criteria* There should be confirmation in each Annual Report that the criteria for reporting adopted by the OPC have been adhered to. Statistics on the ratio of published summaries to resolved complaints should also be published.
>
> *Naming complainants* Complainants should be able to elect to be named in reports, except where this is inconsistent with a mediated settlement.
>
> *Naming private sector respondents* In relation to private sector respondents, the OPC does not identify respondents in reported cases. The detailed study suggests four criteria which favour identification and five criteria against identification of private sector respondents (it recommends general identification of public sector respondents). These factors may justify a default position of non-identification, provided it is coupled with a readiness in Commissioners to identify where the interests of the complainant, others who may have been harmed by the conduct, or the public interest, justify identification, and subject to any

> strong reasons which would make identification unfair in the particular case. This is of course subject to the requirements of the Act.
>
> *Level of detail* Commissioners need to ensure that their complaint summaries contain sufficient detail for interested parties to obtain a full understanding of the legal issues involved and the essential steps in the Commissioner's reasoning leading to their resolution. In relation to remedies, sufficient of the factual circumstances are needed for the adequacy of the remedy to be understood in relation to the seriousness of effect on the complainant, and to allow comparison with potentially comparable complaints (subject to the privacy interests of the complainant).
>
> *'One stop' reporting* Privacy Commissioners should report on their own websites at least minimal details of appeals and judicial review of their own decisions, and of other Court and Tribunal decisions concerning the Acts they administer.

Complaint outcomes – statistics At present, despite the breadth of the remedies (including monetary compensation) provided in s52, it is impossible to accurately answer the question 'do complainants get remedies under the Privacy Act?', except for the occasional remedy revealed haphazardly in a reported complaints. The discussion in the previous section refers to summaries of individual complaints, but it is equally important that interested observers should be able to obtain a clear idea of the OPC's overall performance in handling complaints. In the Commissioner's Annual Reports and web site graphs statistics have only been systematically provided to indicate the number of cases received, and the numbers disposed of each year, but with little or no indication of the outcomes to complainants and respondents of the process. In some reports there has been an indication of the percentage of complainants whose complaints were upheld.

Two types of statistics are needed:

(i) *Statistics of which provisions are used to dispose of complaints* (particularly the various sub-categories of s41): This information is provided for the first time in the 2003-04 Annual Report. This is a major improvement on previous practices.

> **Submission 6-22.3:** ***Publication of statistics of which provisions are used to dispose of complaint should be continued, and expanded to provide additional details. For example, it would be simple but informative to list the laws relied upon under s41(e).***

(ii) *Statistics of remedies afforded to successful complaints* (by agreement, in the case of mediated complaints), including details of the amounts of compensation paid to complainants. The 2003-04 Annual Report only states that "These steps included apologising to the complainant; changing procedures; giving access to the information sought; amending records, training staff; and compensating the complainant for loss or damage suffered as a result of the interference with their privacy."

> **Submission 6-22.4:** ***The OPC should publish, at least annually, statistics of the remedies obtained where complaints are settled with some remedy being provided to the complainant, including statistics of the numbers of cases in which compensation was paid and the amounts of compensation paid.***

The AAT decision in *Rummery and Federal Privacy Commissioner* [2004] AATA 1221 (22 November 2004) illustrates why more transparency concerning the OPC practices in regard to payment of compensation are needed, both by way of reporting of complaint summaries, and by remedy statistics. This is the only appeal as yet under s61 against the amount of compensation awarded by the Commissioner under a s52 determination, partly because the Commissioner has only twice made such determinations awarding compensation in the history of the Act, for $1,000 and $2,500. A three member AAT Panel awarded an eight-fold increase in the compensation awarded by the Commissioner, from $1,000 to $8,000. Is this misjudgment by the OFPC typical of its handling of complaints involving claims for compensation? This is a rhetorical question because we have no way of knowing how often the OPC obtains compensation for complainants, or in what

amounts. We assume that OPC would now adopt the criteria for compensation set out in *Rummery*[85], but have no way of knowing.

> ***Submission 6-22.5:*** **Rummery** ***should be considered as a warning that all aspects of the Commissioner's practices concerning the awarding or negotiating of compensation may need review. In particular those practices need to be more transparent so as to be susceptible to external comment, criticism and comparison with awards in comparable jurisdictions (as the AAT attempted to undertake in*** **Rummery*).***

[85] Also mentioned, but without need to apply it, by the NSW Administrative Decisions Tribunal in *NW v New South Wales Fire Brigades (No 2)* [2006] NSWADT 61

Transborder Data Protection (Ch 13)

Export of private sector information – NPP 9

> *13–1 Does NPP 9 provide adequate and appropriate protection for personal information transferred from Australia to a foreign country?*

NPP 9 prohibits 'transfers' of personal information by an organisation to someone (other than the organisation itself) in a foreign country unless one of six conditions (a) - (e) is satisfied. If one of the conditions is satisfied, then the Australian organisation which transferred the data does not have any liability under the Act for any privacy breaches which may occur subsequently. It is therefore important, from the individual's point of view, to ensure that the conditions do not allow transfers which create unjustified privacy risks (see Greenleaf, 2001a, para 2.10).

The six conditions will generally be sufficient to allow any legitimate transfer overseas of personal information. However, the conditions are undesirably weak and may allow transfers which will harm the interests of the data subjects concerned.

Condition (a) allows foreign transfers where the exporting data user 'reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles'. Instead of any objective and expert determination by a government or Privacy Commissioner of which overseas countries have 'adequate' laws (the 'white list' approach), the condition is satisfied by the mere 'reasonable belief' of the Australian organisation disclosing the information. The 'reasonable belief' need only be that the overseas arrangement 'effectively upholds' privacy principles, not that there are enforcement mechanisms substantially similar to those in the Australian Act. While similar to the role of Art 25 of the Directive, which allows transfers to foreign countries with 'adequate' laws, this provision is much weaker.

Conditions (b) - (e) are largely un-contentious (and similar to those in Art 26(1) of the Directive). Condition (f), however, merely requires that the exporting data user 'has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles'. This probably does not even require that the individual should have some recourse against anyone in the event that the 'reasonable steps' turn out to be inadequate. There will be no recourse against the data exporter if the 'reasonable steps' turn out to fail. This is much weaker than the Directive.

The subjective and imprecise nature of condition (a), and the weak and imprecise nature of exception (f), means that there is real danger that personal information will be exported from Australia under conditions which give little protection to privacy, but expose an exporting data user to little risk.

> ***Submission 13-1: NPP 9 does not provide adequate and appropriate protection for personal information transferred from Australia to a foreign country. Conditions (a) and (f) both need to be strengthened. In particular, data exporters should remain liable for breaches of standards by data importers under most circumstances.***

Comparison with international standards - Europe

By comparison with European standards, the Directive by Article 25 requires restrictions on transfers of personal data to jurisdictions which do not provide an adequate level of protection, except in situations allowed by Article 26. The Article 29 Working Party seems to consider as a necessary criterion for adequacy of a third country's law that 'further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient

(i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1).'

A critical assessment of the adequacy of NPP 9 (Waters 2001) noted that it differs in some significant respects from the terms of Articles 25 & 26.

- Under [NPP 9], consent for transfer does not have to be 'unambiguous' [exception 9b)], and organizations are allowed to make an assumption about the likelihood of consent where it is impracticable to obtain it [exception (e)].
- Organisations are allowed to make their own assessment of whether there is 'adequate protection' in the destination country [exception (a)].
- The exception where 'the organization has taken reasonable steps to ensure that the information …will not be held, used or disclosed inconsistently with the NPPs', [exception (f)] is much weaker than the nearest equivalent in Article 26(2) in that it addresses only standards and not safeguards and the exercise of rights.
- There is no equivalent in NPP 9 to the public interest, legal claims, or vital interests derogations in Article 26, although it is assumed that the government intends to provide for these in some other way – otherwise, a range of important cross border transfers – including for law enforcement or major emergencies – would be prohibited.

In addition, Waters noted, NPP 9 does not provide any protection where personal information is transferred either to a State or Territory government which is not subject to a privacy law or to one of the large number of private sector organizations which will be exempt from the proposed Commonwealth regime. So, NPP 9 appears to fall short of Articles 25 & 26 in a number of key respects.

The Article 29 Working Party was also critical of NPP 9 in its Opinion 3/2001. One ground of criticism was the lack of guidance on which other countries offer protections substantially similar to the NPPs. The Privacy Commissioner shows reluctance to become involved in giving such guidance, both for reasons of resources and because of relationships with other countries (OPC, 2005, pp. 77-79). The Commissioner intends, nevertheless, to publish an information sheet to help exporters of data 'more easily assess whether a privacy regime is substantially similar' and 'o outline the issues that should be addressed as part of a contractual agreement' (OPC, 2005, recommendation 18, p. 80). Another ground was that exception 9(f) has no requirement that any remedies be available to data subjects (as in the third criticism above). The Australian Government has not to our knowledge addressed these criticisms.

The Article 29 Working Party was also critical of the fact that the extra-territorial operation of the Act (s. 5B) did not apply to 'non-Australians' and that this meant that NPP 9 would not extend to protect non-Australians. The Australian Government subsequently amended s. 5B to provide that the requirement of Australian citizenship or residence (see s. 5B(1)(a)) does not apply to NPP 9 (s. 5B(1A)). What this means is that if an Australian business transfers personal data to its own subsidiary overseas, or to a business otherwise bound by s. 5A, then that recipient of the transferred data will be bound to observe NPP 9 in any subsequent transfers from the second jurisdiction, regardless of the data subject's identity or nationality. This amendment may have been well-intentioned, but its narrow scope in only applying to NPP 9 means that most of the extra-territorial extension of the Act does not apply to non-Australians. However, extra-territorial operation of other principles does not seem to be a requirement for adequacy under Art. 25 of the data protection Directive.

However, in considering these differences, it should also be borne in mind that NPP 9 (in both the Commonwealth and Victoria) is one of the very few such data export provisions yet *in force* in any country outside Europe.[86] Some jurisdictions (e.g., NSW, Hong Kong) have enacted such provisions but not yet brought them into force. Australian's data export restrictions may give insufficient protection to Australians, as argued above, but that does not necessarily mean they will lead to a finding of 'inadequacy' of Australian law.

> ***Submission 13-1.1: Any revision of NPP 9 should also seek to ensure that it is as consistent as possible with European standards for data exports.***

> *13–5 Is adequacy of the Privacy Act under the European Union Data Protection Directive: (a) necessary for the effective conduct of business with European Union members; and*

In light of the discussion above, it is obviously difficult to give any definite answer to this question.

> ***Submission 13-5: Whether adequacy is 'necessary' remains to be seen, as the European Union has as yet not indicated by its actions what effect lack of adequacy will have on trading relationships with other countries. However, if adequacy of Australia's privacy laws can be achieved without detriment to Australia's interests, then it is desirable to achieve it in the interests of Australian businesses.***

> *13–5 (2nd part) (b) desirable for the effective protection of personal information transferred into and out of Australia?*

> ***Submission 13-5.1: This depends on whether Australia's current privacy laws are assessed as adequate, which is not yet known. If the answer is 'no', then adequacy is desirable for the effective protection of information transferred into Australia, as it would mean that Australia would provide a somewhat higher level of protection than it does now. Even if the answer is 'yes', it does provide an assurance that our laws are providing sufficient protection to incoming data according to international standards.***

> *13–5 (3rd part) If so, what measures are necessary to ensure the adequacy of Australia's privacy regime under the European Union Data Protection Directive?*

> ***Submission 13-5.2: This cannot be stated with certainty. Which factors (if any) the European Commission considers demonstrate a lack of adequacy will not be clear until it makes a decision. These would be unlikely to be the same as the criticisms made by the Article 29 Working Party, only some of which are justified. Potentially significant differences between the Act and the factors going toward 'adequacy' are indicated elsewhere in this submission.***

Comparison with international standards - APEC Privacy Framework

> *13–6 Does the APEC Privacy Framework provide an appropriate model for the protection of personal information transferred between countries?*

The APEC Privacy Framework does not at present provide an appropriate model for protecting data exports. The final (September 2005) version of Part (IV) B of the Framework says nothing directly about personal data exports – either in terms of limitation rules or requirements to allow them. As a result, the APEC Framework does *not* do any of the following: (i) Forbid data exports to countries

[86] Restrictions on transborder data flow are also in force in Argentina (*Personal Data Protection Act 2000* s. 12) and Canada (*Personal Information Protection and Electronic Documents Act 2000*, Schedule 1, clause 4.1.3), though the provisions of the Canadian legislation do not deal *expressly* with such data flow.

without APEC-compliant laws (contrast the EU Directive); (ii) Explicitly allow restrictions on data exports to countries without APEC-compliant laws (contrast the OECD Guidelines and the Council of Europe Convention); (iii) Require data exports to be allowed to countries that have APEC-compliant laws (or equivalent protections) (contrast any other international privacy agreement) (see Greenleaf 2006, 2006a).

The APEC principle IX(b) provides that where information is transferred to a third party (domestically or internationally) this requires either the consent of the data subject (an addition proposed by Japan) or that the discloser exercise due diligence and take reasonable steps to ensure that the recipient protects the information consistently with the APEC Principles. This sub-principle was proposed by the USA. This is a soft substitute for a Data Export Limitation principle, and may leave the data subject without a remedy against any party where the exporter has exercised due diligence but the importer has nevertheless breached an IPP. Contrary to the statement by Crompton and Ford cited in the Issues Paper [13.78], the APEC Framework does not hold the data exporter 'accountable' in any meaningful sense, because the Framework does not have any requirement of legal enforcement. There is no guarantee of any legal remedy against the exporter, and none against the importer if it is in a jurisdiction without applicable privacy laws (Greenleaf 2006b). This shares all the weaknesses of NPP 9, and adds some of its own.

Even if one ignores the enforcement problem, the only standard of privacy protection that is required is 'the recipient protects the information consistently with the APEC Principles'. The problem is that the APEC Principles are very weak: the principles are 'at best an approximation of what was regarded as acceptable information privacy principles twenty years ago when the OECD Guidelines were developed' (Greenleaf 2006b); the enforcement measures can best be summarized as 'anything goes', allowing 'anything ranging from complete self-regulation unsupported by legislation, through to legislation-based national privacy agencies' (Greenleaf 2006b); and the whole edifice is 'the weakest international privacy standard yet developed' (Greenleaf 2006).

APEC's Privacy Sub-group of the E-Commerce Steering Group is now attempting to develop some mechanism for a trial of binding corporate rules as a means of data transfer between some APEC economies, but it would seem likely to be many years (if ever) before this makes a serious contribution to both privacy protection and free flow of personal information in the region.

> ***Submission 13–6: The APEC Framework is the weakest international privacy standard yet developed, and does not provide an appropriate model for the protection of personal information transferred between countries.***

Comparison with international standards – Asia-Pacific Privacy Charter

> *13–6 (2nd part): Are other standards, such as the Asia-Pacific Charter, a more appropriate model?*

Principle 12 of the draft Asia-Pacific Privacy Charter provides:

> 'An organisation must not transfer personal information to a place outside the jurisdiction in which it is located unless there is in force in that jurisdiction a law embodying principles substantially similar to these Principles, or with the consent of the person concerned, or the organisation has taken all reasonable steps to ensure that the personal information will be dealt with in accordance with these Principles in that place and continues to be liable for any breaches of these Principles.'

Given that the draft Charter presents a high standard of privacy principles, the requirement of 'a law embodying principles substantially similar to these Principles' in the data exporting jurisdiction does require a more appropriate standard of protection. Where data exports occur to jurisdictions without such legislative protection, the continuing liability of the data exporter for breaches by the importer is what is needed to protect the data subject. The data exporter is in the best position to

obtain a contractual indemnity from the data importer (the party breaching the principles), so this is generally fair. However, it may need modification to reduce the liability for the data exporter under some circumstances where strong legislative privacy protections apply in the jurisdiction of the data importer, if these provide sufficient protection for the Australian data subject.

> ***Submission 13–6.1: Principle 12 of the draft Asia-Pacific Privacy Charter does provide a more appropriate model for protecting privacy where data exports occur. It may need modification to reduce the liability for the data exporter under some circumstances where strong legislative privacy protections apply in the jurisdiction of the data importer.***

Comparison with international standards – Council of Europe Convention

Another international standard which should be given serious consideration as an appropriate model for the protection of personal information transferred between countries is the Council of Europe's privacy Convention (Council of Europe 1981). In their 2005 Montreux Declaration the world's privacy and data protection Commissioners appealed 'to the Council of Europe to invite, in accordance with article 23 of the Convention … non-member-states of the Council of Europe which already have a [sic] data protection legislation to accede to this Convention and its additional Protocol.' It is worth noting that the EU – or, more accurately, European Communities (EC) – has long signalled a wish to accede to the Convention. Amendments to the Convention were adopted in 1999 in order to permit accession by the EC but are not yet in force.[87]

Since 2001 a similar approach has seen the Council of Europe Cybercrime Convention become an international instrument of widespread adoption outside Europe. It is a way of sidestepping the cumbersome process of developing a new UN convention on privacy, by starting with an instrument already adopted by the region with the most concentrated distribution of privacy laws. This approach deserves serious consideration by Australia, New Zealand, Japan, South Korea and other Asia-Pacific countries with privacy legislation approximating OECD and Council of Europe standards, as it could provide a reasonable basis (a common reasonably high privacy standard) for a guarantee of free flow of personal information between parties to the treaty, both as between Asia-Pacific countries and as between those countries and European countries. As other countries outside Europe or the Asia-Pacific adopt serious privacy legislation, as South Africa soon may, joint membership of this Convention would also guarantee data transfers between these countries and Australia. Such invitation and accession would also be likely to carry with it the benefits of a finding of 'adequacy' under the EU Directive, given that the 2001 Additional Protocol (Council of Europe 2001) to the Convention has added a data export restriction and a requirement of an independent data protection authority to bring it more into line with the EU privacy Directive.

Given that the APEC Privacy Framework has not attempted to provide such a general legislation-based mechanism for free flow of personal information within the Asia-Pacific, perhaps globalizing this European instrument is now the realistic way open to do so. It would also be a much quicker solution than waiting for some new global enforceable treaty to emerge from the UN or elsewhere.

> ***Submission 13–6.2: Accession to the Council of Europe's privacy Convention could give Australia a mechanism for ensuring a reasonable level of privacy protection (assuming some improvements to NPP 9), coupled with guarantees of free flow of personal information between Australia and Europe and possibly other non-***

---

[87] See Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to accede. The amendments will enter into force on the thirtieth day after approval by all of the Convention Parties (Art. 21(6) of the Convention). As of 1.12.2006, 26 Parties had registered their approval.

European countries as well. The Discussion Paper should explore how effective this would be.

Export of public sector information

The IPPs governing the Australian federal public sector do not include *any* data export restrictions. Waters (2001) notes a possible argument that the security principle (IPP 4) might require a data 'exporter' to take reasonable steps to ensure that personal information was not misused in the hands of a recipient. However, that position is untested, and an explicit requirement would be better. Since the IPPs pre-date the Directive by seven years, and the NPPs now include a data export restriction, this omission seems to be something of an historical anomaly. The position is different for some State and Territory public sector laws, where the Victorian provision is now in force but the NSW provision is not.

Submission 13-1.2: A data export principle similar to a revised and improved NPP 9 should also apply to the Commonwealth public sector. It should also apply to transfers within Australia.

Other aspects of data exports

13–1 (2nd part) Does the relationship between NPP 2 (disclosure of personal information) and NPP 9 (international transfer of personal information) need to be clarified?

Any transfer to a third party overseas also involves a 'disclosure' of personal information, and NPP 2 limiting disclosures for secondary uses must also be complied with.

13–2 Should the Privacy Act be amended to clarify that NPP 9 applies when personal information is transferred outside Australia to a related body corporate?

Where a transfer is to the same organisation overseas, NPP 9 does not apply, and there is no need to consider whether any of the six enabling conditions apply. The s5B extra-territorial operation of the Act then comes into play, and Australian privacy law will usually apply, not (only) the law of the foreign country. While the law should be amended to state that NPP 9 does apply to transfers to related corporations, consideration should also be given to making s5B apply to them. Companies should not be able to structure their operations to avoid Australian privacy laws, and related corporations can be argued to have a close enough connection with Australia to justify extra-territorial operation of our law.

In addition, whether a transfer is to the same organisation or a related corporation, this recipient organisation can then transfer the data to an organisation in the overseas county (provided the transfer complies with NPP 2) which is neither bound by any privacy laws nor has any practices which comply with Australian privacy practices. This is a loophole that should be closed, but this needs to be done by imposing obligations on organisations to take additional care when they disclose personal information to such recipients.

Submission 13–2 The Privacy Act should be amended to provide or confirm that NPP 9 applies when personal information is transferred outside Australia to a related body corporate. The Discussion Paper should consider the application of s5B to related bodies corporate as well.

> *13–3 What role, if any, should the Office of the Privacy Commissioner play in identifying countries that have equivalent Privacy Act protection for personal information?*

It is important that businesses be able to operate with some clarity in exporting data, at least in those cases where it is clear that another country does have similar privacy laws to ours. However, there will be many cases where it is difficult to make such a decision in the absence of a complaint that requires decision, and many cases where it is clear there is no such protection but for political reasons a Commissioner will not want to pronounce negatively on other country's laws. It is also better for the Commissioner not to have a power of delegated legislation here, but only to be able to make guidelines. The best compromise Commissioner therefore seems to be to empower, but not require, the Commissioner to operate a 'whitelist' of countries he or she consider has equivalent laws. The effect of this list would be as a factor going toward an exporter's good faith belief.

> ***Submission 13–3: The Commissioner should have power to maintain a 'whitelist' of countries whose legislation provides equivalent protection, both in terms of principles and enforcement.***

Notification of exports

> *13–4 Should organisations be required to inform individuals that their personal information is to be transferred outside Australia? If so, what form should such notification take?*

A requirement to notify would be one of the most effective protections against inappropriate transfers. It should extend to notification of which jurisdiction data is to be transferred, and the identity of the recipient in that jurisdiction.. It will assist individuals to exercise informed choice and/or bring pressure to bear for improvements in legislative protection, at least in Australian jurisdictions without adequate laws.

> ***Submission 13-4: Yes, a requirement to notify would be one of the most effective protections against inappropriate transfers. There should be a requirement to inform individuals that their personal information is to be transferred to any jurisdiction without equivalent privacy protection (including some State jurisdictions within Australia). If the organisation has an intention to transfer at the time of collection, it should give notice at that point. If it later decides to export the data, it should give notice at that time.***
>
> ***Submission 13-4.1: There should also be a requirement to inform individuals to which jurisdiction(s) their personal information is to be transferred, and the identity of the recipient in that jurisdiction.***

References

APEC Framework Part B - *APEC Privacy Framework International Implementation ("Part B") Final* – Version VII ECSG Plenary Meeting Gyeongju, Korea, 8-9 September 2005.

Ayres, I. and Braithwaite, J. 1992 [Summary of] *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992), located at <http://islandia.law.yale.edu/ayres/respons.htm>.

Beardwood, J. 2002, 'Tea leaves and goat entrails: A review of the Privacy Commissioner's significant findings under new Canadian privacy legislation', *Computer und Recht International* (CRI), Issue 06/2002.

Berthold, M. and Wacks, R. 1997, *Data Privacy Law in Hong Kong,* 1st ed. (Asia: Sweet & Maxwell, 1997).

Bolkus Report, 2005 Senate Legal and Constitutional References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988* (June 2005).

Bygrave, L. 1990, 'The Privacy Act 1988: A Study in the Protection of Privacy and the Protection of Political Power', 19 *Federal Law Review* 128.

Bygrave, L. 2002a, *Data Protection Law: Approaching Its Rationale, Logic and Limits* ###The Hague / London / New York: Kluwer Law International, 2002).

Bygrave, L. 2002b, 'Balancing data protection and freedom of expression in the context of website publishing – recent Swedish case law', 18(1) *Computer Law and Security Report* 56.

Council of Europe 1981, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* (Convention No 108).

Council of Europe 2001, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasbourg, 8.XI.2001.

Crompton, M. 2005, 'Are comparisons possible? A framework for assessing the performance of data protection supervisors', *Jusletter* 3rd October 2005, available at <http://www.privacyconference2005.org/fileadmin/PDF/crompton.pdf>

Data Protection Working Party 2001, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, at <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2001/wp40en.pdf>

European Union 1995, *Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (O.J. L 281, 23.11.1995, p. 31).

Evans, K. 2003, 'The NZ Privacy Commissioner's case notes – an analysis', 9 *Privacy Law and Policy Reporter* 191.

Ford, P. 2003, 'Implementing the EC Directive on Data Protection – an outside perspective", 9 *Privacy Law & Policy Reporter* 141.

Greenleaf, G, 2006, 'Asia-Pacific Developments in Information Privacy Law and its Interpretation' UNSW Law Research Paper No. 2007-5 at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952578>

Greenleaf, G. 2006a, 'APEC Privacy Framework completed: No threat to privacy standards' [2006] *Privacy Law and Policy Reporter* 5 at http://www.austlii.edu.au/au/journals/PLPR/2006/5.html

Greenleaf, G. 2006b, 'APEC's Privacy Framework sets a new low standard for the Asia-Pacific' in M. Richardson and A. Kenyon (eds.), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge: Cambridge University Press, 2006).

Greenleaf, G. 2006c, 'Australia – Privacy at 30 something' Draft chapter for J. Rule and G. Greenleaf (Eds.), *Privacy At Forty: Seven National Histories* (unpublished 2006).

Greenleaf, G . 2005, 'Implementation of APEC's Privacy Framework', in Datuk Haji Abdul Raman Saad Personal (ed.), *Data Protection in the New Millenium* (Malaysia: LexisNexis, 2005).

Greenleaf , G. 2004, *Submission to the Federal Privacy Commissioner*, *Review of the private sector provisions of the Privacy Act 1988 (Cth)*, 20 December 2004, available at <www.privacy.gov.au/act/review/revsub47.doc> accessed 31 January 2007.

Greenleaf, G. 2004a, 'Casenote - *X v Commonwealth Agency [2004] PrivCmrA 4'* (2004) 11 *Privacy Law and Policy Reporter* 16.

Greenleaf, G. 2004b 'Australian privacy law grows up' (2004) 11(1) *Privacy Law and Policy Reporter* 1.

Greenleaf, G. 2004c 'Casenote - *O v Credit Provider [2004] PrivCmrA 5*' (2004) 11(2) *Privacy Law and Policy Reporter* 40.

Greenleaf, G. 2003, "Reforming reporting of privacy cases: A proposal for improving accountability of Asia-Pacific Privacy Commissioners", accepted for publication in Paul Roth (ed.), *Privacy Law and Policy in New Zealand*, (Wellington, NZ: Butterworths LexisNexis, 2004) copy available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=512782> accessed 31 January 2007.

Greenleaf, G. 2002 'Canada makes privacy impact assessments compulsory' 8(10) *Privacy Law and Policy Reporter* 190.

Greenleaf, G. 2001, "Key concepts undermining the NPPs - A Second Opinion," 8(1) *Privacy Law and Policy Reporter* 1.

Greenleaf, G. 2001a, "Private sector privacy: Problems of interpretation", *CyberLRes* 3 available at <http://www.austlii.edu.au/au/other/CyberLRes/2001/3/> accessed 31 January 2007.

Greenleaf, G. 2000 'Reps Committee protects the privacy- free zone' (2000) 7 *Privacy Law and Policy Reporter* 1.

Greenleaf, G. 1996, "Stopping surveillance: Beyond 'efficiency' and the OECD" 3 *Privacy Law and Policy Reporter* 148 available at <http://www2.austlii.edu.au/itlaw/articles/efficiency.html> accessed 31 January 2007.

Greenleaf, G. and Waters, N. 2003, 'Editorial - Is privacy now just a low business risk' 11(2) *Privacy Law and Policy Reporter* 30.

Greenleaf, G. and Waters, N. 2003, *The Asia-Pacific Privacy Charter Working Draft 1.0*, 3 September 2003 - [2003] *PrivLRes* 1, available at <http://www.worldlii.org/int/other/PrivLRes/2003/1.html> accessed 5 February 2007.

Gunning, P. 2001, 'Central Features of Australia's Private Sector Privacy Law' 7(10) *Privacy Law and Policy Reporter* 189 available at <http://beta.austlii.edu.au/au/journals/PLPR/2001/16.html> accessed 31 January 2007.

Lindsay, D. 2002, "Freedom of Expression, Privacy and the Media in Australia" in M. Colvin (ed.), *Developing Key Privacy Rights* (Oxford / Portland, Oregon: Hart Publishing, 2002).

Mellor, K. 2003, 'Australian Press Council Privacy Standards: do they measure up?' 10(2) *Privacy Law & Policy Reporter* 24 available at <http://kirra.austlii.edu.au/au/journals/PLPR/2003/24.html> accessed 31 January 2007.

Montreux Declaration 2005, 'The protection of personal data and privacy in a globalised world: a universal right respecting diversities', Declaration of the 27th International Conference of privacy and Data Protection Commissioners, Montreux, Switzerland, September 2005.

OECD 1981, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1981).

Office of the Privacy Commissioner ('OPC') 2006 'Commissioner's use of s.52 Determination Power' 1(1) *Privacy Matters* 2, Spring 2006.

Office of the Privacy Commissioner ('OPC') March 2005, *Getting in on the Act: Review of the Private Sector provisions of the Privacy Act 1988*, available at <http://www.privacy.gov.au/ACT/review/revreport.pdf> accessed 5 February 2007.

Office of the Privacy Commissioner ('OPC'), November 1996, *Plain English Guidelines to the Information Privacy Principles* available at <http://www.privacy.gov.au/publications/ipp8_11.pdf> accessed 21 July 2005.

Otlowski, M. 2001, 'Employment Sector By-passed by the Privacy Amendments, 14 *Australian Journal of Labour Law* 169.

Perrin, S. Black, H. Flaherty, D. Rankin, T.M. 2001, *The Personal Information Protection and Electronic Documents Act – An Annotated Guide* (Toronto: Irwin Law, 2001).

Roth, P. 2000, 'Casenote: *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 (NZ Court of Appeal)' 7(7) *Privacy Law and Policy Reporter* 134 available at < http://beta.austlii.edu.au/au/journals/PLPR/2000/59.html> accessed 31 January 2007.

Shaw, M. 2005, 'Privacy laws may be tightened', *The Age*, 16.8.2005, available at <http://www.theage.com.au/news/national/privacy-laws-may-be-tightened/2005/08/15/1123958006150.html> accessed 16 August 2005.

Wacks, R. 2000, 'How Videos: Is the Surveillance of Domestic Helpers Lawful', 7(5) *Privacy Law and Policy Reporter* 100 available at <http://beta.austlii.edu.au/au/journals/PLPR/2000/49.html> accessed 31 January 2007.

Waters, N. 2002, 'Can the media and privacy ever get on?' 8(8) *Privacy Law & Policy Reporter* 149 available at < http://beta.austlii.edu.au/au/journals/PLPR/2002/1.html> accessed 31 January 2007

Waters, N. and Greenleaf, G. 2006, *Interpreting the Security Principle*, v.4, Interpreting Privacy Principles Project, Cyberspace Law and Policy Centre, University of New South Wales, available at <http://www.cyberlawcentre.org/ipp/> accessed 5 February 2007.

Waters, N. and Greenleaf, G. 2006a, *Interpreting Retention and Disposal Principles*, v.1, Interpreting Privacy Principles Project, Cyberspace Law and Policy Centre, University of New South Wales, avaialable at <http://www.cyberlawcentre.org/ipp/> accessed 5 February 2007.

Waters, N. and Greenleaf, G. 2005, 'IPPs examined: The correction principle', *Privacy Law and Policy Reporter* 5, available at <http://www.austlii.edu.au/au/journals/PLPR/2005/5.html> accessed 5 February 2007.

Index of submissions made

Each submission is identified by the ALRC question to which it relates, with sub-numbering where more than one submission is made to a question.

Overview of privacy and the Act (Chs. 1-3)

Action for breach of privacy

Submission 1-2: A statutory privacy tort is desirable because of the inadequacy of other tortious and equitable remedies. A useful guide to the potential elements of such a tort are the provisions recommended by the Hong Kong Law Reform Commission.

Submission 1.2.1: The preferable location for such statutory privacy torts, insofar as they apply to the private sector, is the Privacy Act. Such legislation should preserve the right of States or Territories to enact higher standards of privacy protection. At the same time, national consistency by agreement should be sought.

National consistency

Submission 2-1: National consistency is a valuable objective, but should not be pursued to the detriment of the level of protection. Agreement on model or uniform laws to be implemented in all jurisdictions would be the best way forward, at least in regard to the various public sectors.

Structure of the Privacy Act 1988 (Cth)

Submission 3-1: The Act should be simplified by providing one 'core' set of principles applying to both the private sector and the (Commonwealth) public sector. To the extent that there needs to be special sub-sectoral rules, they should be be legislative exception to the 'core' set of principles.

Submission 3-2: 'Information Privacy Act' (as in Victoria) would be a better name, given the current scope of the Act. However, if the scope of the Act is broadened to make it more comprehensive (eg include privacy torts), then 'Privacy Act' is appropriate.

Submission 3-2.1: The Discussion Paper should consider whether a more comprehensive legislative code is desirable to cover all aspects of privacy, including bodily and territorial privacy and surveillance as well as information privacy.

Privacy principles - Threshold issues (Ch 4)

Specificity of principles

Submission 4-36: The starting point is that it is desirable to adopt principles (i) which are consistent, at least within Australia, and (ii) which represent best practice in terms of promoting internationally accepted privacy standards.

Uniform principles

Submission 4-34: There should be a single set of principles to apply to both Commonwealth agencies and private sector businesses (and ideally to all State and Territory public sector agencies and to all other organisations including those currently exempt from any of the existing laws). We submit that there are no particular principles that should apply only to either the public or private sector, but that there are exceptions which will be more or less relevant to different sectors. As argued above, there is no single existing model which should be preferred as all have been shown to have weaknesses – a new set of common principles should be derived from analysis of the various precedents. In some cases the resulting principles will be very close to the existing NPPs or IPPs, thereby minimising any adjustment of compliance requirements.

International consistency

Submission 4-34.1: Wherever possible and consistent with Australian interests, Australian privacy principles should be consistent with the main international privacy standards, of which the three most

important instances for Australian interests are the European Union's privacy Directive, the OECD's privacy Guidelines and the APEC Privacy Framework.

Reasons for reform of information privacy principles

Submission 4–34.2: There are three reasons, apart from the important objective of consistency, why the information privacy principles in Australian Privacy Laws may need to be revised: (i) where a principle as currently legislated clearly falls short 'on its face' of meeting community expectations; (ii) where the practice of government agencies or businesses in complying with the principle have exposed shortcomings; and (iii) where courts or tribunals have 'read down' the meaning of a principle (often

in conjunction with interpretation of core concepts) so that it does not in law have the anticipated effect.

Collection principles

Methods of receiving information

Solicited information

Collection directly from data subject

Submission 4-3.1: Commonwealth agencies should have an obligation to collect wherever possible directly from the data subject, as is currently the case with NSW, Victorian and NT government agencies, and private sector organizations.

Submission 4-3.2: The wording of a 'direct collection' principle should be based on NPP 1.4 but should omit 'only' which does not readily accommodate situations where some information can be obtained directly with supplementary information justifiably obtained from a third party.

Unsolicited information

Submission 4-4: The law should make it clear that collection principles apply, to the maximum practicable extent, to unsolicited information.

Observations / surveillance of the data subject

Submission 4-4.1: The law should make it clear that the collection principles apply to the maximum practical extent to information obtained from observation or surveillance.

Submission 4-4.2: Further consideration needs to be given to the policy issues concerning a requirement of notice when information is collected by observation, and the law needs to be clarified on this point.

Information extracted

Submission 4-4.3: The law should make it clear that the collection principles apply to the maximum practical extent to information extracted from other records.

Submission 4-4.4: Further consideration needs to be given to the policy issues concerning a requirement of notice when information is collected by observation, and the law needs to be clarified on this point.

Information generated as a result of transactions with an individual

Submission 4-5: All collection obligations should apply to all forms of collection, irrespective of the source from or means by which the data is collected. However, different requirements of notice may apply depending on how the data is collected, with the default position being that notice is required unless an exemption is provided.

Lawful purpose(s)

Purpose justification

Submission 4-5.1: Consideration should be given to whether Australian law should adopt any form of 'purpose justification' test, along Canadian, European or other appropriate lines.

Excessive collection

Submission 4-5.2: The collection obligations should expressly link the amount of personal data that may be collected to the purpose of collection, and limit it to what is necessary for that purpose.

Anonymity

Submission 4-29: The anonymity principle should be retained but redrafted to include the concept of pseudonymity as an alternative where appropriate. The principle

should also clarify that it applies at the stage when an information system is being designed, not only 'after the event' when a person wishes to enter a transaction with a data user.

Submission 4-29.1: The anonymity principle should impose an obligation on organisations to give an individual the option of remaining anonymous or pseudonymous (as appropriate) when entering into transactions. The touchstone remains 'minimum collection necessary for the purpose of the transaction'.

Submission 4-29.2: The anonymity principle should impose an obligation on organisations to facilitate, where practicable and lawful, anonymous or pseudonymous transactions between individuals and third parties.

Submission 4-30: The anonymity/pseudonymity principle should also apply to the public sector.

Relationship between disclosure and collection

Submission 4-5.3: Australian law should clarify the relationships between collection and disclosure of personal information, and in particular the limitations that the purposes of collection of a first organisation play in limiting the uses of a second organisation to which the information is disclosed.

Obligations of confidence – role in limiting use and disclosure

Submission 4-5.4: The Discussion Paper should consider the role that the law of breach of confidence plays in determining the circumstances under which the use or disclosure of personal is limited, and in particular whether the principles in Johns v ASC and similar cases needs to be supported by statutory provisions .

Fair collection principles

Submission 4-5.7: The Discussion Paper should give more attention to issues concerning fair collection, which are of considerable practical importance.

Notification requirements in collection principles

Notification when collecting

Required notice of collection

Relationship with openness principles

Submission 4–1: The Discussion Paper should canvass the possibility of a combined 'awareness' principle, covering both notification requirements at the time of collection and more general information provision.

Application of awareness/notification principles

When is notice not required?

Submission 4-2: Consideration should be given to changing the 'notice' principle from one of 'ensuring awareness' to 'specifically notifying', with a conditional exception where the data user could establish that at least the typical data subject had been made aware by other means.

Submission 4-2.1: Strong justification should be necessary where notice is not provided before or at the time of collection.

Submission 4-2.2: The Discussion Paper needs to canvass a more radical re-appraisal of the awareness and notification requirements in the context of new communications technologies.

Submission 4-3: The law should require all data users to identify the party or parties to the transaction, and to expressly require operative contact details to be given.

Submission 4-1: The Discussion Paper should consider whether, if notices use generic descriptors of recipients, there should be an additional obligation to answer specific enquiries about the identity of actual recipients.

Additional matters about which 'awareness' measures could be required

Submission 4-1.1: The law should require all data users to notify individuals of both internal and external dispute resolution options. Used appropriately, this can be assisted by layered privacy notices.

Layered or staged provision of notice

Submission 4-1.2: Concerning layered privacy notices, the Discussion Paper should canvass views about the minimum set of information which needs to provided at or before the time of collection to achieve the objective of the awareness principle, and the minimum standard of transparency of links to more detailed information.

Use and Disclosure principles

Single or separate principles?

Submission 4-6: There are competing arguments. This question deserves to remain open in the Discussion Paper.

Meaning of 'use'

Submission 4-6.1: The use principle should clarify whether accessing personal information, without further action being taken as a result of that access, is 'use' of personal information.

Meaning of 'disclosure'

Submission 4-6.2: Privacy laws should make it clear that even information already known to the recipient can still be 'disclosed'.

Limits on use and disclosure

(i) Meaning of 'purpose of collection'

Submission 4-7: The law should be clarified to expressly allow for the declaration of multiple specific purposes, where collection is necessary for each of these purposes (but see discussion of bundled consent).

(ii) Related purposes exceptions

Submission 4-8: The general adoption of 'directly related' in the related purposes test is appropriate.

(iii) Related purposes – 'reasonable expectations test'

Submission 4-9: The 'reasonable expectations' test is desirable as part of a test of related purposes.

(iv) Direct marketing 'opt out' exception

Submission 4-12: NPP 2 should be amended to contain a sub-principle dealing expressly with direct marketing, broadly defined, unequivocally giving individuals a

right to opt-out of receipt of further communications. No alternatives should be allowed. Such a principle needs to be designed to be consistent with other more specific legislation, which may however continue to apply a higher standard in relation to particular types or modes of communication.

Submission 4.12.1: Consideration should be given to providing a right to opt-out of direct marketing from government agencies – subject perhaps to limited exemptions for public health and safety campaigns or where government agencies had specific knowledge of individuals' eligibility.

Submission 4-12.2: Privacy law should require that data users take reasonable steps, on request, to advise an individual from where they acquired the individual's personal information.

(v) Consent exception

Submission 4–12.3: The Discussion Paper should consider the implications of the confusion caused by the lack of any distinction in the Privacy Act between uses or disclosures justified by consent and those justified by acknowledgment of notification.

Submisison 4-11: The law needs to be clarified concerning 'bundled consent' in order to prevent abuse of the practice.

(vi) Prior notice / mere awareness exception

Submission 4-11.1: The exception for mere awareness of disclosure practices without consent to them or acknowledgment of them should be removed.

(v) Exceptions for prevention of harm to the person or others

Submission 4-7: The ALRC should canvass the justification for the recent amendments concerning emergencies, which were given relatively little scrutiny in Parliament.

(vi) Exception where authorised under law

Submission 4-7.1: The Discussion Paper should consider whether, in light of international standards and examples from other jurisdictions, the 'authorised by law' exception could be made more specific.

Disclosure exceptions are not requirements to disclose, nor general justifications

Submission 4-7.2: There should be a clear statement in privacy laws that an exception to a use or disclosure principle is neither a requirement nor an authorization to use or disclose.

Data matching

Submission 4-7.3: The Discussion Paper should give consideration to the inclusion of a definition of 'data matching' and to empowering the Privacy Commissioner to regulate all data matching practices according to a set of statutory principles. Consideration should be given to whether such regulation should also apply to the private sector .

Trans-border data transfers

Submission 4-31: Yes, the same principles regulating data exports should apply to both public sector agencies and private sector organisations.

Data quality principles

Scope of principles

Submission 4-15: The data quality obligations should only be expressed at a general level in the principles, as is the case at present.

When data quality obligations apply

Submission 4-16: A data quality principle should refer expressly to a wide range of criteria of quality, including accurate, complete, up-to-date, and relevant. It should apply both at the time of collection and at the time of use and disclosure, but should otherwise not apply independently to the 'holding' of the data. Retaining the 'reasonable steps' qualifier in such a principle will ensure that the obligation is not unreasonably onerous.

International considerations

Data security principles

Submission 4-17: A security principle constructed from the security principles in the the draft Asia Pacific Privacy Charter and the APEC Privacy Framework should apply to all data users.

Contractors and outsourcing

Submission 4-17: The security principle should also require organisations to take reasonable steps to ensure that personal information they disclose to contractors is protected.

Comparison with European standards

Retention and disposal principles

Submission 4-18: Privacy law should address retention and disposal in an independent principle applying to all data users.

Submission 4-19: Privacy law should address retention and disposal in an independent principle applying to all data users.

Submission 4-19.1 A retention and disposal principle should require data users to destroy or permanently de-identify personal information when it is no longer needed either for the purpose of collection or for any other purpose required by law, or for any secondary purpose for which it has already legitimately been used. Secondary purposes for which personal information may be used or disclosed in future should not provide an alternative justification for retention.

Comparison with international standards

Openness and transparency principles

Submission 4-20 The Discussion Paper should canvass the possibility of a combined 'awareness' principle, covering both notification requirements at the time of collection and more general information provision, and with specific attention to the respective roles of proactive notice vs obligations to respond to enquiries.

Submission 4-20.1: The Digest provisions should remain. Even if the compilation and publication of a central Digest were to be discontinued, the obligation on agencies to

maintain individual records and make these available for public inspection. IPP 5.4(a)) should remain.

Submission 4-20.2: Privacy law should give the Commissioner the discretion to require organisations to publish further information about particular personal information handling projects. (See also Submission 6-8)

Access and correction principles

Access – relationship to FOIA

Submission 4-23 and 4-24: This needs to be answered in the context of a rationalisation of the Privacy and FOI Acts. We support generally the ALRC's 1995 recommendations in Report 77.

Intermediary access

Submission 4-23.1: Privacy principles should provide that, wherever possible, a data subject whose data is exempt from access by the data subject should be able to have

that data accessed by a mutually agreed third party intermediary who is able to ensure that the data subject's privacy rights have been observed. In default of agreement, the Privacy Commissioner should be empowered to be such an intermediary. NPP 6.3 is not a adequate implementation of such a principle.

Access - Comparison with international standards

Notification of inaccuracies to third parties

Submission 4-25: The law should require data users to notify third parties, where practicable and at the express request of the individual concerned, that they have received inaccurate information and to pass on any corrected information.

Correction- dependence on access rights

Submission 4-25.1: Correction obligations should apply independently of rights of access – i.e. the right of individuals to seek correction should apply whether they have

obtained access through formal processes (such as under the Privacy or FOI Acts) or have become aware of the information by other means.

Correction – other improvements

Submission 4-25.2: The principle should make it clear that correction can take the form of amendment, deletion or addition, as appropriate in the circumstances. There are many situations where there is a legal requirement to keep a historical record of actual transactions, but this should not prevent the correction of 'operational' records, leaving the original incorrect information only in an archive.

Submission 4-25.3: The principle should specify that the obligation in relation to disputed information has to be performed in a way which ensures that any annotation is made available to any subsequent user of the disputed information.

Identifiers (NPP 7 and Ch 12)

Submission 4-26: Identifiers and data-matching are separate issues and should be dealt with in separate provisions. (See earlier re data-matching)

Submission 12-1: Tax file number principles should be dealt with consistently with unique multi-purpose identifiers - See submission 12-3 below.

Submission 12-3: The privacy principles in the Privacy Act, and methods for adjudication concerning breaches of them, should apply to any unique multi-purpose identifiers adopted in Australia. Any variations from the application of any of the principles should be defined by specific legislative provisions stating exceptions or variations, and not left to inference from the existence of a different set of principles. Such an approach will (i) ensure that variations are obvious; (ii) facilitate a consistent body of law emerging on both the core principles and the exceptions.

Additional Principles

Accountability

Prevention of harm

Submission 4-35: A separate 'prevention of harm' principle should not be adopted.

Consent or 'choice' principle

Submission 4-35.1: There should not be a separate principle concerning consent or choice.

Security breach notification

Submission 4-35.2: The Discussion Paper should canvass the role of a Security Breach Notification Principle, drawing on the US experience. We agree with the ALRC (paragraph 4.206) that the threshold criteria for triggering a notification requirement is critical. There should by now be enough experience of the US State laws to guide a sensible rule.

No disadvantage principle

Submission 4-35.3: Privacy law should include an additional no-disadvantage principle to ensure that data users do not use pricing or other sanctions to deter individuals from exercising their privacy rights. Such a principle would need to designed carefully to avoid becoming a constraint on innovation.

Automated decision-making principles

Submission 4-35.4: Consideration be given to an automated decision-making principle which requires human intervention before any adverse action is taken in relation to any individual based solely on automated processes.

Privacy impact assessments principles

Submission 4-35.5: The Discussion Paper should canvass the merits of an additional principle requiring Privacy Impact Assessments for significant projects

Exemptions from the Privacy Act (Ch 5)

Policy concerning exemptions – avoid 'privacy-free zones'

Submission 5-1: Exemptions should as far as possible be limited to, and where possible located within, the principle(s) to which they are applicable. Organisations should not be given a blanket exemption from privacy principles, because at least some privacy principles are applicable to all organisations, even if their application needs to be modified. This approach (i) will help avoid a plain reading of a principle creating misleading expectations of coverage, and (ii) help avoid organisations being able to claim that they 'comply' with a principle, when in fact an exemption located elsewhere means the exact opposite outcome.

Exempt Commonwealth agencies

Submission 5-2: The agencies listed in Q5-2 should not be completely exempt. The extent of any justifiable exemptions to or modifications of specific IPPs should be stated in the Act.

Submission 5-3: No, the agencies listed in Q5-3 should not be so broadly exempt. The extent of any justifiable exemptions to or modifications of specific IPPs should be stated in the Act.

State and Territory authorities

Submission 5-4: State and Territory authorities should be exempt from the Privacy Act, except to the extent discussed in 5-5.

Submission 5-5: Any State or Territory authority that competes with private sector organisations should be subject to the Privacy Act unless they are subject to a State or Territory Act which includes a set of privacy principles of comparable scope and a means by which individuals may enforce them by law including by appeal to a Court.

Small business operators

Submission 5-6: The Small Business Operator exemption should be removed.

Submission 5-6.1: If special provisions for small businesses are needed, the definition of exempt Small Business Operator should only define who comes within a Code made by the Privacy Commissioner which can relax or remove bureaucratic aspects of the principles and the Act.

Political parties and practices

Submission 5-7: Registered political parties should only be exempt to the extent required by the Constitution.

Submission 5-8: Political acts and practices should only be exempt to the extent required by the Constitution.

Employees

Submission 5-9: There should be no general exemption for employee records. Some uses of employment records in particular contexts may justify exemptions from or modifications to particular IPPs/NPPs.

Media organisations

Submission 5-10: This exemption should be reviewed. While there are serious issues about the balance between privacy rights and freedom of expression, and about the legitimate public interest role of the media, these issues should be addressed with selective exceptions to some of the principles, if justified, rather than by a blanket exemption.

Submission 5-11: See our answer to Q 5-10 above. If there are to be selective exceptions for public interest media activity, the relevant terms will need to be much more carefully and closely defined. While difficult, it must be possible to distinguish between genuine news and current affairs journalism and the infotainment, entertainment and advertising which makes up the bulk of media content.

Submission 5-12: See our answers to Qs 5-10 & 5-11 – we do not believe the media exemption should remain in its current form

Related bodies corporate

Other exemptions

Submission 5-14: The current exemption for 'personal, family or household affairs' should be retained.

Powers of the Privacy Commissioner (Ch 6)

Overall effectiveness of the legislative scheme

Submission: The OPC's own report gives reasons to conclude that there is significant community dissatisfaction with the way in which it carries out its responsibilities. The information available about complaint outcomes reinforces this. The Discussion Paper should examine this matter carefully, as there is no point having an Act containing sound privacy principles if they are not being effectively enforced for the benefit of the community.

Submission 6-1.1: The Office of the Privacy Commissioner should be retained. However, it should be made more transparently accountable for how it carries out its responsibilities.

Commissioner's powers

Submission 6-5: The Commissioner's powers to report are unnecessarily circumscribed, in particular in those powers in s27 which only allow reports to be made to Ministers. The Commissioner should have an additional explicit power under s27 to report to the public, or make a special report to the Parliament, on any of the matters listed otherwise in s27, with as few exceptions as possible.

Privacy impact assessments

Submission 6-6: The Discussion Paper should canvass the merits of an additional principle requiring Privacy Impact Assessments for significant projects or developments of organisations in both the public sector and the private sector.

Personal information digest

Submission 6-8: The Digest should be retained and improved, and should be published on the Internet in as flexible a searchable form is possible, and with re-publication of the information by others allowed.

Submission 6-8.1: The Commissioner should be able to vary the amount of information required to be submitted by an agency, or to excuse an agency from submitting any information. Such a requirement should be subject to Parliamentary review by way of a disallowable instrument.

Submission 6-8.2: The Digest requirements should not be extended to the private sector generally, but the Commissioner should be able to require a private sector organisation, or a class of private sector organisations, to submit information similar to that which is submitted by agencies, and publish it in the Digest. Such a

requirement should be subject to Parliamentary review by way of a disallowable instrument.

Location of Commissioner's functions

Submission 6-11: It is highly desirable that all of the Commissioner's functions be located in the Privacy Act, but only if any other legislation to which the function relates contains an explicit cross-reference to the Commissioner's role and the Privacy Act function.

Complaint resolution powers

Submissions 6-12, 6–13, 6-14: The Commissioner's powers in relation to complaint investigation are generally adequate, the problem lies elsewhere.

Submission 6-15: The Commissioner's powers are not exercised appropriately or effectively in relation to reporting on complaint outcomes (see below).

Submission 6–16: The Commissioner's powers to make determinations are not administered in the best interests of complainants. The Act requires clarification that a complainant or respondent should be able to require that the Commissioner deal with a complaint by way of a s52 determination rather than under s41. This is also necessary if the proposed right of appeal against s52 Determinations (see below) are to be meaningful, as the right of appeal could then be avoided by dismissing a complaint under s41.

Submission 6-16.1: The Commissioner should be given power to make and enforce determinations as a result of an 'own motion' investigation. Such own motion investigations should be the subject of public notice by the Commissioner, and procedures developed for appropriate intervention by other interested parties (such as NGOs in the relevant area). The Commissioner should be able to make a special report to Parliament of the results of an own motion investigation.

Enforcing determinations

Submission 6-17: Both complainant and respondent should have a right of appeal against any s52 determination, in the form of a merits review. Whether this is to the Federal Court, Federal Magistrates Court, or the AAT, is of less importance.

Submission 6-17.1: The lack of merits review of s41 decisions can best be addressed by providing complainants with the rights to insist on a s52 Determination, once there is a right of appeal against s52 Determinations.

Injunctions

Submission 6-19: The s98 injunction provisions are valuable in theory, but ineffective in practice. The Discussion Paper should consider means by which the use of s98 by the Commissioner, by NGOs and by complainants can be made more effective.

Compliance model and remedies

Submission 6-21: The current compliance model used in the Privacy Act is appropriate in its essential features, but it has major deficiencies including lack of appeal rights and lack of a right in complainants to demand determinations (see submissions above), as well as a lack of transparency (see submissions to follow). At present it is not effective to achieve the Act's purposes.

Submission 6-21.1: The compliance model is also ineffective because of its administration, which is unduly adverse to transparency, enforcement of the Act, and clarification of the Act by the Courts.

Submission 6-22: The Commissioner's powers in the Act should be clarified so that it is clear that the Commissioner can prescribe generally how a respondent should act.

Transparency and feedback – Inadequacy of the Commissioner's reporting practices

Submission 6-22.1: The OPC should publish online a comprehensive manual of its complaint resolution policies and procedures, and keep it up-to-date.

Submission 6-22.2: The OPC should be required to reform its procedures for reporting privacy complaints along the following lines: (i) adhering to publicly-stated criteria of seriousness of which complaints are

reported; (ii) confirmation in each Annual Report that these criteria for reporting have been adhered to; (ii) naming complainants who elect to be named; (iv) naming private sector respondents where the interests of other potential complainants or the public interest justifies this; and

(v) naming all public sector respondents except where this would cause serious harm to the interests of the complainant or another person; and (vii) providing sufficient detail in complaint summaries for them to useful to interested parties.

Submission 6-22.3: Publication of statistics of which provisions are used to dispose of complaint should be continued, and expanded to provide additional details. For example, it would be simple but informative to list the laws relied upon under s41(e).

Submission 6-22.4: The OPC should publish, at least annually, statistics of the remedies obtained where complaints are settled with some remedy being provided to the complainant, including statistics of the numbers of cases in which compensation was paid and the amounts of compensation paid.

Submission 6-22.5: Rummery should be considered as a warning that all aspects of the Commissioner's practices concerning the awarding or negotiating of

compensation may need review. In particular those practices need to be more transparent so as to be susceptible to external comment, criticism and comparison with awards in comparable jurisdictions (as the AAT attempted to undertake in Rummery).

Transborder Data Protection (Ch 13)

Export of private sector information – NPP 9

Submission 13-1: NPP 9 does not provide adequate and appropriate protection for personal information transferred from Australia to a foreign country. Conditions (a) and (f) both need to be strengthened. In particular, data exporters should remain liable for breaches of standards by data importers under most circumstances.

Comparison with international standards - Europe

Submission 13-1.1: Any revision of NPP 9 should also seek to ensure that it is as consistent as possible with European standards for data exports.

Submission 13-5: Whether adequacy is 'necessary' remains to be seen, as the European Union has as yet not indicated by its actions what effect lack of adequacy will have on trading relationships with other countries. However, if adequacy of Australia's privacy laws can be achieved without detriment to Australia's interests, then it is desirable to achieve it in the interests of Australian businesses.

Submission 13-5.1: This depends on whether Australia's current privacy laws are assessed as adequate, which is not yet known. If the answer is 'no', then adequacy is desirable for the effective protection of information transferred into Australia, as it would mean that Australia would provide a somewhat higher level of protection than it does now. Even if the answer is 'yes', it does provide an assurance that our laws are providing sufficient protection to incoming data according to international standards.

Submission 13-5.2: This cannot be stated with certainty. Which factors (if any) the European Commission considers demonstrate a lack of adequacy will not be clear until it makes a decision. These would be unlikely to be the same as the criticisms made by the Article 29 Working Party, only some of which are justified. Potentially significant differences between the Act and the factors going toward 'adequacy' are indicated elsewhere in this submission.

Comparison with international standards - APEC Privacy Framework

Submission 13–6: The APEC Framework is the weakest international privacy standard yet developed, and does not provide an appropriate model for the protection of personal information transferred between countries.

Comparison with international standards – Asia-Pacific Privacy Charter

Submission 13–6.1: Principle 12 of the draft Asia-Pacific Privacy Charter does provide a more appropriate model for protecting privacy where data exports occur. It may need modification to reduce the

liability for the data exporter under some circumstances where strong legislative privacy protections apply in the jurisdiction of the data importer.

Comparison with international standards – Council of Europe Convention

Submission 13–6.2: Accession to the Council of Europe's privacy Convention could give Australia a mechanism for ensuring a reasonable level of privacy protection (assuming some improvements to NPP 9), coupled with guarantees of free flow of personal information between Australia and Europe and possibly other non-European countries as well. The Discussion Paper should explore how effective this would be.

Export of public sector information

Submission 13-1.2: A data export principle similar to a revised and improved NPP 9 should also apply to the Commonwealth public sector. It should also apply to transfers within Australia.

Other aspects of data exports

Submission 13–2 The Privacy Act should be amended to provide or confirm that NPP 9 applies when personal information is transferred outside Australia to a related body corporate. The Discussion Paper should consider the application of s5B to related bodies corporate as well.

Submission 13–3: The Commissioner should have power to maintain a 'whitelist' of countries whose legislation provides equivalent protection, both in terms of principles and enforcement.

Notification of exports

Submission 13-4: Yes, a requirement to notify would be one of the most effective protections against inappropriate transfers. There should be a requirement to inform individuals that their personal information is to be transferred to any jurisdiction without equivalent privacy protection (including some State jurisdictions within Australia). If the organisation has an intention to transfer at the time of collection, it should give notice at that point. If it later decides to export the data, it should give notice at that time.

Submission 13-4.1: There should also be a requirement to inform individuals to which jurisdiction(s) their personal information is to be transferred, and the identity of the recipient in that jurisdiction.

References

Index of submissions made