Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs

# Privacy Amendment (Private Sector) Bill 2000

Graham Greenleaf
Professor of Law, University of New South Wales
15 May 2000

**Contents of submission**

# 1. Introduction

## 1.1. Structure of submission

I have read the submission proposed by the Australian Privacy Charter Council and I wish to endorse that submission. I have not covered many of the matters in that submission but have concentrated on a few aspects of the Bill.

References to sections ('s5B') are to sections of the *Privacy Act 1988*, as proposed to be amended by this Bill. References to clauses ('cl 3') are to clauses of the Bill

I have attached brief biographical details indicating my qualifications and experience in relation to privacy matters.

## 1.2. Overall assessment of the Bill

In its current form, the *Privacy Amendment (Private Sector) Bill 2000* is essentially 'business protection legislation', and not primarily to protect the privacy of consumers and citizens.

At the most general level, the formal structure of the Bill is supportable, including its co-regulatory structure. The principal deficiencies of the Bill are its numerous exception and exclusions, and the omission of a number of basic protective mechanisms that prevent effective enforcement of such consumer rights as do exist. As noted by the Charter Council, the Bill also contains many well-drafted provisions.

Before this Bill deserves any support from a consumer perspective, it requires many major improvements. With such major improvements, the structure of the Bill is capable of providing a useful (though still inadequate) form of privacy protection. Well-controlled and enforceable co-regulatory schemes can provide a useful advance in the world-wide development of privacy laws - but this Bill lacks both the necessary public interest controls and fair enforcement mechanisms.

As the Bill stands, I do not support its enactment. Due to its numerous weaknesses, it will legitimate previously questionable privacy-invasive business practices more than it will protect privacy. Large areas of privacy-invasive business (and political) practices will be completely exempt from the Bill. Protection to individual privacy will be piecemeal, and will leave consumers unprotected against many of the worst privacy invasions (which will now have an aura of legitimacy of 'complying with the Privacy Act'). Such rights as the Bill provides will be inadequately enforced and enforced in a way which is biased toward business.

This Bill is capable of amendment so it could at least bring Australia up to the standards of privacy protection now commonplace in Europe, New Zealand, Hong Kong and elsewhere. Such legislation will not be sufficient to provide sufficient privacy protection in the 21st century, but would at least bring Australia up to last century's standards.

In this submission I have detailed some major deficiencies of the Bill, and suggest how some of them can by remedied by simple amendments. Many other deficiencies, and suggestions for improvement, are covered in submissions by the Privacy Charter Council. These constructive suggestions for improvement of the Bill

should not be misinterpreted as support for a Bill which is fundamentally anti-consumer. It will take major surgery for this Bill to be of substantial value to consumers.

### 1.3. Biased purposes (cl 3)

The new objects clause of the Act (s3) indicates a pro-business bias which may affect the interpretation of the Act by the Commissioner, Code bodies and Courts. The objects only refer to individual 'interests' in protecting their privacy, but refers to 'the *right* of business to achieve its objectives efficiently'.

*Recommendation:* Two changes would make the objects more evenly balanced, without bias toward either business or consumers:

(i) a change to 'individuals rights in protecting their privacy'; and

(ii) a change to 'the right of business to achieve its legitimate objectives efficiently'.

## 2. Deficiencies in the enforcement procedures

Co-regulation involving a range of different industry Code authorities will not operate in a way which is fair and effective unless:

- The procedures are not biased against either businesses or consumers.
- The Code authorities have sufficient powers to properly investigate complaints.
- There is a process by which the potential differences in interpretation of the Act by different Code authorities can be overcome, with uniform and legally correct interpretations of the Act resulting and applied by all Code authorities and the Commissioner.

The proposed complaints procedures will not deliver any of these necessary outcomes, and are unfair and biased against complainants, for the reasons following.

### 2.1. The lack of an appeals structure is biased toward businesses

Businesses complained about will in effect have a right of appeal to the Federal Court on the merits of their case, whereas unsuccessful individual complainants will have no such right. This is unfair and biased.

As is currently the case under s55 of the Privacy Act, under the new ss55 and 55A, a determination of a complaint by a Code authority or by the Commissioner can only be enforced by proceedings in the Federal Court (or the new or Federal Magistrates Court), and the Court has to deal with the matter by way of a hearing *de novo* (anew) as to whether there has been conduct constituting an interference with privacy (s55A(5)).

As a result, all that a business has to do if it is aggrieved by the way in which a Code Complaints Body or the Privacy Commissioner has dealt with their complaint, is sit on its hands and not pay the compensation or take the other steps it has been ordered to take. The complainant must then take the matter to the Federal Court, and the business can have the matter heard in full again. In effect, it obtains a right of appeal to a Court.

The problem is that an unsuccessful complainant, whether the complaint is heard by a Code Complaints Body or by the Privacy Commissioner, has no such right of appeal - no right to have the matter heard *de novo* by any higher authority. They have no redress against a wrong interpretation of an Industry Code or the National Privacy Principles (or of other provisions of a Code or the Act), or of the wrong application of the law to the facts of the complainant's case. This is unfair and biases the whole enforcement structure of the Act against consumers.

A determination will now be prima facie evidence of the facts upon which the determination is based (s55A(6)). It will be possible, however, for those facts to be challenged. This does not address the fundamental problem of unsuccessful complainants having no right of appeal, but is an improvement since the successful complainant is at least not put to proof or those facts all over again.

### 2.2. Judicial review will not deliver justice, nor develop consistent privacy law

Nor does the proposal to make decisions of code complaint bodies subject to judicial review address the problem sufficiently. This will help ensure that code complaint bodies observe procedural fairness, but will do little ensure the development of consistent and legally correct interpretations of the National Privacy Principles or code provisions based on them to the wide range of factual situations which will arise in complaints. It will also fail to provide justice to complainants where a code complaints body has misinterpreted its own code, or applied the code to the facts of the complaint in a dubious fashion, or (as mentioned below) been frustrated in its investigation through lack of powers.

As a result of these continuing deficiencies of the proposals, there will be little likelihood of the development of a significant or consistent body of law concerning the meaning and application of the Principles. The Privacy Commissioner will not oversee the interpretation of codes by industry bodies in individual cases, being limited to some vague obligation to report on their general operation in his or her annual report. The Courts will only do so rarely, and only in cases where the code has been interpreted in favour of complaints and is therefore under attack by businesses.

### 2.3. Lack of powers to investigate

Industry complaint bodies will not have any statutory powers to investigate or obtain information, in contrast with the very strong powers held by the Privacy Commissioner. The Information Paper admitted:

> It is intended that privacy codes should require participants to co-operate with and provide requested information to code complaint bodies. However, this will not fully substitute for the Privacy Commissioner's statutory powers, particularly in relation to obtaining information from third parties.

This deficiency in investigative powers exacerbates greatly the complainant's lack of right of appeal. If investigations are frustrated, a complainant's case will remain unproven. Where an industry complaint body's investigation is frustrated by its lack of investigative powers (particularly where a third party not a party to the industry scheme has failed to cooperate), it is unlikely that it could be criticised in a process of judicial review, and the fact that it can make no enforceable determination denies the complainant the avenue of taking the matter to a tribunal where legal powers of

compulsion are available (the Federal Court). In contrast, in the rare event that a business could not provide evidence of its defence because some third party refused to provide evidence, the business can use the avenues of Federal Court process to obtain the evidence, once the complainant starts an enforcement action.

The ability of a Code authority to refer complaints to the Commissioner (s40(1B)) is useful, but is out of the control of the complainant and at the discretion of the Code authority, and is no substitute for a right of appeal against bad decisions based on inadequate investigations.

All of these remedial processes are biased against complaints in favour of businesses, and should not be. These weaknesses bring the *bona fides* of the proposed legislation as genuine co-regulation into question.

### 2.4. The need for consistent and accessible privacy law

The Australian Consumers Association, in its submission, refers to the danger of 'privacy silos', inconsistent versions of privacy law emerging in different industries with Codes. This is my concern as well, but I differ from ACA in that I do not think that appeals to the Privacy Commissioner (who is not a lawyer) is a complete answer. I have no objection to appeals to the Privacy Commissioner as an intermediate stage - a first tier administrative review. This would assist in providing greater consistency of interpretation, and the Commissioner's investigative powers would assist in better resolution of some complaints.

However, the Privacy Act needs the benefit of occasional interpretation by the Courts on serious issues, and the Privacy Commissioner's decisions should also be subject to appeal where the issue is important enough. A right of appeal is unlikely to lead to a flood of cases.

## 3. Publication of Code decisions - avoiding secret justice

### 3.1. Formal determinations

New s18BB(3)(d) requires determinations (ie decisions on complaints) by Code authorities to be 'the same' as the Commissioner makes under s52, but it is not clear that this would require Code authorities to follow the Commissioner's practice of publishing such determinations. It does not even specifically require determinations to be in writing. These matters should be explicit in the terms of a Code.

It is of vital importance that the way in which Code authorities handle complaints, and particularly how they decide the most important complaints - those that go to a full formal determination. This information needs to be available to potential complainants, to their advisers, and to those generally interested in the way in which the law is being interpreted by Code bodies.

If there is not full access to determinations, then there is no transparency of the Code process and no guarantee of its integrity.

Recommendations

(i) s18BB should require Code authorities to make written determinations specifying the reasons for the determination, and to provide a public register of such determinations, and copies of determinations to anyone who asks for one.

(ii) s18BB should require determinations by Code authorities to be provided to the Privacy Commissioner when made, and for the Commissioner to publish them. Complainants should be anonymised where necessary.

### 3.2. Informal mediation

Most complaints will not be settled by formal determinations, but by informal mediation by the Code authority. However, even when complaints are settled by mediation, they are settled on the basis of an interpretation of the law (ie of the Code and of other aspects of the Act). For the same reasons as set out above, it is very important that this process has some transparency that will aid others to understand how the law is being interpreted. New s18BB(k) is unclear as to whether anything more than statistical recording of these complaints by Code authorities is necessary, and this is insufficient.

Recommendations

(i) s18BB(k) should require Code authorities to keep a brief summary of each complaint resolved without a determination, sufficient to identify the nature of the complaint, the Code provisions applied in resolving it, the nature of the settlement, and any issues of law which were raised in the complaint. Where necessary, both complainant and respondent may be anonymised.

(ii) The Code authority should provide a copy of these summaries to the Commissioner at least annually, for publication by the Commissioner. Publication via Internet, and a copy available on request from the Commissioner's office, will be sufficient.

## 4. Unjustified exemptions

I have only been able to deal with some of the Act's unjustified exemptions in this submission.

### 4.1. Flaws in the 'small' business exemption

Other submissions will explain how the demographics of Australian businesses mean that the $3M turnover definition of a 'small' business means most Australian businesses will have virtually no obligations to protect their customer's (or anyone else's) privacy.

I will concentrate on how the exemption will be abused to provide exemptions to big businesses, and how it will also operate unfairly to prejudice the interests of small businesses that wish to protect privacy, and will put at risk the privacy-protective efforts of industry associations.

#### How big businesses can rort the 'small' business exemption

The so-called 'small business exemption' contains a major loophole which will allow a company or individual to run a large business (say of annual turnover $10M) which is based around major use of customer personal information, but for that large business to have unrestricted swapping and use of that personal information within all units of the business, and still to escape completely from the operation of the Act. Big businesses can use this loophole to escape from their obligations to protect privacy.

This potential for the rorting of the Act takes several steps to explain:

- A 'small business operator' (not a 'small business') is the entity exempted from the operation of the Act, because 'organisation' does not include a 'small business operator' (s6C). Since only 'organisations' (in the private sector) are obliged to comply with the Act, small business operators ('SBOs') are therefore exempt from complying with the Act.

- The definition of a 'small business operator' says a SBO 'carries on one or more small businesses' (s6D(3)(a)). A SBO could therefore carry on a number of businesses, let's call them 'YourInfo (Marketing)', 'YourInfo (Sales)' and 'YourInfo (Collections)'.

- The exemption as a 'small business operator' is lost if any of the businesses of a SBO 'discloses personal information ... to anyone else for a benefit, service or advantage' (s6D(4)(c)). The loophole is that disclosure of personal information between any of the businesses run by the SBO is not disclosure 'to anyone else', it is just disclosure to the same SBO (the fact it is between different businesses is irrelevant). Similarly, the collection of information from the other business does not cause the exemption to be lost because it is not collection 'from anyone else' (s6D(4)(d)).

- The different businesses run by the SBO can use the personal information received from the other businesses for any purpose they like, because only disclosure, not use, can cause loss of the exemption.

- This is so even if the use is completely unrelated to the purpose of collection, and if the information used is inaccurate, irrelevant, incomplete etc. The individuals concerned have no rights of access or correction.

This means that any businesses run by the same operator, no matter how large and how privacy invasive in their use of information (provided it does not involve disclosures or collections for consideration), can completely avoid the operation of the Act by the expedient of splitting any of the constituent businesses into sub-businesses before they reach the $3M threshold (s6D(4)(a)). Just have lots of 'small' privacy invading businesses, and your total business operation can be as big as you like, and still remain a privacy-free zone.

**How to increase the sale value of a small business by privacy-invasion**

The SBO rort is made even worse by the way in which it increases the sale value of small businesses that hold potentially valuable personal information, by encouraging the use of this information for interferences with privacy which would otherwise be illegal.

This argument also takes a couple of steps:

- Many small businesses will hold personal information (often about their customers) which could be misused for purposes for which it was not provided by combining it with other personal information held by other businesses. However, the small business cannot do this, because it would involve disclosure of the information to someone else, which would cause loss of SBO status for both the disclosing business (s6D(4)(c)) and the collecting business (s6D(4)(d)).

- At face value, the value of the small business will therefore not include any component based on the commercially valuable disclosure and use of this personal information, because such disclosure is illegal.
- However, any SBO who buys the small business in question that has the valuable personal information (as opposed to buying the information) can immediately share all of this personal information with its other small businesses. The combining of the information held by all the businesses is now within the privacy-free zone.
- Because of the so-called small business exemption, the sale value of a business that holds personal information can therefore be higher than its value as a stand-alone business, because what would be an illegal invasion of privacy by a stand-alone business (even a small business), becomes perfectly legal when one 'small' business buys another.

This Act therefore increases the takeover value of small businesses with privacy-invasive potential. The Act should not operate to distort market mechanisms in this way.

**The 'small' business exemption will hurt small businesses and industry associations**

This exemption will also harm the small-ish business that wishes to obtain a reputation for protecting the privacy of its customers. There is no provision for an organisation which comes within the definition of 'small business operator' to 'opt in' to be bound by the Act.

A business that wishes to protect privacy therefore cannot even say that it complies with the Privacy Act without being in danger of false and misleading conduct through implying it is bound by the Act.

Many businesses with a turnover of less than $3M are involved in international e-commerce via the Internet. Successful Internet businesses are not necessarily big businesses. They may make extensive use of personal information, particularly concerning their customers, without buying or selling personal information. It is likely that Australian 'small' businesses will be excluded from any finding of 'adequacy' by the European Union, and will therefore be excluded from receiving any personal information from EU countries. Similar exclusions are likely under laws of regional jurisdictions which have data export prohibitions, such as Hong Kong. More details are provided below.

Where a business is in an industry which has a Code under the Act, it cannot even participate fully in the industry Code, because any complaints against it will not be able to be dealt with by use of procedures under the Act (including enforcement of determinations, referrals to the Commissioner, administrative review etc).

Similarly, any industry associations which have as members any businesses within the definition of 'small business operator' and have an industry Codes will be at risk of false and misleading conduct unless all information and publicity about the Code stresses that the legally significant aspects of the Code only apply to those of their members with turnover of less than $3M (and how will the public know who they are?).

This exemption therefore harms those small-ish businesses, and industry associations, that wish to protect privacy by refusing them the reputational and trade benefits that compliance with the Act provides.

**Appropriate measures to safeguard small business interests**

It should be possible to develop a flexible means of providing appropriate allowance for the interests of small businesses using other provisions in the Act without creating a dangerous 'privacy free zone'.

Recommendation

The small business exemption should be deleted from the Bill.

The Privacy Commissioner should be required, before the Bill comes into force, to make a Public Interest Determination concerning small businesses, for the purpose of modifying the NPPs to the extent necessary to ensure that a simplified and less onerous set of privacy obligations applies to those small businesses where lesser obligations are proportionate and appropriate to the lesser risk to privacy of their business operations. Such a Determination should be reviewed periodically by the Commissioner as the need arises.

The Commissioner should be required to take the modifications to the NPPs into account in the development of all industry Codes, to ensure that such Codes have appropriate provisions for small businesses.

Such a requirement on the Commissioner would ensure that appropriate allowance is made for small businesses, based on the Commissioner's expertise in the NPPs and how they will be administered, while at the same time preserving the benefits of privacy protection both for businesses and consumers.

### 4.2. A better political parties 'exemption'

The only legitimate interest that politicians and political parties have in being 'exempted' in any way from an obligation to respect people's privacy is that there is some potential for the Privacy Act to be mis-used by one political party against another during the electoral process, with possible interference in the democratic process resulting.

The blanket exemption in the Bill is completely unnecessary to address that problem. All that is needed is to remove the Privacy Commissioner, and the Act, from the heat of the electoral process.

Recommendation

The current exemption for political parties (new s7C) should be deleted.

Where a complaint under the Act is made against a political party (or an associated body), the following procedure should apply:

- Once writs have been issued for any election in which that political party has candidates, the Privacy Commissioner shall immediately cease to investigate any such complaint.
- Once the poll is declared for all seats in which the political party has candidates, the Privacy Commissioner will resume investigation of any such complaint.

### 4.3. The employment exemption

Others will deal with this exemption at more length, but I wish to add a number of further reasons why the exemption is unjustified:

- Public sector employment information are already covered by the Privacy Act (and this has not caused problems), so the exemption of private sector employees is discriminatory.
- The workplace relations legislation does not cover many of the privacy protections provided by the NPPs.
- If such an exemption is included, it is unlikely that Australian employers will be able to obtain employment information from European employers.

## 5. Will the Privacy Act be 'adequate' for EU purposes?

One of the objectives of the Bill (cl 3) is to meet 'international concerns ... relating to privacy', which it is clear from the Explanatory Memorandum principally includes meeting the requirements of the European Union's privacy Directive so that Australia can receive a Declaration of 'adequacy' of its laws by the Committee of Ministers of Member States (the 'A31 Committee').

### 5.1. Uncertainty about the meaning of 'adequacy'

At the time of writing, exactly what the EU will require for a Declaration of adequacy has to be regarded as unknown. The first 'benchmark' is likely to be a Declaration concerning the 'Safe Harbor' proposals put forward by the US government. The EU Commission has proposed to the A31 Committee a draft Declaration that accepts a modified 'Safe Harbor' proposal as 'adequate'. However, the previous draft was vehemently opposed by the Working Party of National Data Protection Commissioners (the 'A29 Committee'), and the A31 Committee will take into account the views of the A29 Committee on the new draft (when available) and of the European Parliament. The result is unlikely to be known until near the end of this year, and it is possible that the A31 Committee might require further negotiation of modifications of the Safe Harbor proposals with the US.

A realistic assessment of the likely 'adequacy' of the Australian Bill must therefore await the outcome of the A31 Committee's deliberations on the Safe Harbor proposal, and this is unlikely to be possible during the Parliamentary passage of this Bill. The safest course, given the importance of satisfaction of the EU standard, is to address deficiencies in the Bill which are likely to cause problems with an EU finding of 'adequacy'.

### 5.2. Problems with the Bill's 'adequacy'

Even with as weak a benchmark as the current Safe Harbour proposal, there are a number of aspects of the 2000 Bill which are likely to limit the scope of any EU finding of adequacy for Australia, and will therefore constitute problems for all or some sectors of Australian businesses:

- **Lack of extra-territorial protection for EU citizens** - Section 5B only extends the protection of the Act concerning extra-territorial practices of Australian businesses to benefit Australians, and therefore cannot be used to protect citizens of EU countries. NPP 9 dealing with transborder data flows

does not operate to prevent the transfer of the information by an Australian business to its own branch operating overseas, because this is only a transfer to itself (and s5B would normally apply to extend the protection of the Australian Act). There is therefore a loophole in the Bill whereby an Australian company could import personal information on EU citizens, but could then export it outside Australia to a country with no privacy law but without the Australian Act applying.

- **Lack of correction rights for EU citizens** - The existing approach in s41(4) which prevents anyone other than Australian citizens and permanent residents from exercising correction rights (IPP 7) is extended to the private sector (NPP 6 and equivalent provisions in Codes). As with the previous example, this provision prevents against EU citizens obtaining the same benefits as Australians from our privacy law, and is contrary to the EU objective in the notion of 'adequacy' that their citizens should be protected by (adequate) local laws wherever their information is used, in the same way that the privacy of local citizens is protected.

  New Zealand's Privacy Commissioner recently proposed that the *NZ Privacy Act 1993* be amended to ensure that non-citizens have all rights under the Act, in order to ensure adequacy under EU law and that of other jurisdictions such as Hong Kong. The Australian Bill is failing to do this.

- **Generally available publications** - The broad exemption in the Act for information in a "generally available publication"[1], irrespective of whether the information came to be included in the publication in breach of the Act, may cause problems, as the A29 Committee noted a similar deficiency in the Safe Harbor principles.

- **'Small' businesses** - There is no equivalent in the EU Directive for an exemption for 'small' businesses (or in the Safe Harbor proposals). At best, this is likely to result in an A31 Declaration that expressly excludes exempt Australian 'small' businesses from its coverage. However, the resulting difficulties involved in an EU business knowing whether any Australian business was covered by the Act could lead to the type of procedural complexities that legislation was supposed to avoid. There is no provision for 'small' businesses that wish to be bound by privacy law so as to be able to import personal information from Europe to opt in to being covered by the Act. They would have to resort to some artificial device such as buying or selling personal information so as to lose their exempt status under the Act. But how would the EU exporter be satisfied of this?

- **Employment information** - There is no equivalent general exemption in the EU Directive, and this is likely to lead to any A31 Declaration excluding any transfer of employment-related information. The A29 Committee wanted such an exclusion of employment information made explicit in the Safe Harbor

---

1 "generally available publication" 'means a magazine, book, newspaper or other publication that is or will be generally available to members of the public (however published)' - s6, as amended by the Bill, Schedule 1, Item 14).

proposal because the US Commerce Department did not have jurisdiction over such information. If there is such an exclusion, a European company would not be able to export employee data to a branch of its own company in Australia because the Australian company cannot 'opt in' to be covered by the Act in relation to its employment information.

- **Weak control over onward transfers** - As discussed later, two of the conditions under which personal information can be exported from Australia under NPP 9 are much weaker than anything found in the Directive. The A29 Committee has consistently identified controls over onward transfers as one of the key elements of 'adequacy', so this may also cause difficulties.

## 6. Other recommendations

It has not been possible in the time available for me to complete my submission on the following matter, but I indicate some of my concerns below.

### 6.1. Related corporations

The effect of new s13B is to allow related corporations to exchange information about individuals where this disclosure is unrelated to the primary purpose for which the information was collected, or where the individual would not reasonably expect this to happen (otherwise, s13B would be unnecessary).

Normally this exchange of information between related corporations will not matter so much, because the recipient corporation will still have to satisfy one of the conditions of NPP 2 before it can *use* the information (see NPP 2.3 which clarifies this). The use would have to be with the consent of the individual, or as authorised by law, or with similarly serious justification.

However, there is two exceptions to this:

- NPP 2.1(c) allows the information to be used for direct marketing purposes by the related corporation even though such use is contrary to the individual's reasonable expectations at the time of collection of the information, provided the individual is given the opportunity to opt out.

- Where information is used in a non-identified form, NPP2 may be irrelevant. The extent to which the related corporation may be able to use a de-identified form of the information, merged with other information it holds, to create profiles of Internet usage and to customise user interactions in a way that falls outside the Act's definition of 'personal information' is uncertain.

It is far preferable for the corporation which collected the information to obtain the consent of the individual to disclose it to the related corporation, as this will be within the consumer's expectations in dealing with a corporation with which it has had previous dealings, rather than a corporation which may be related but with which it has never dealt.

Recommendation

The exemption from parts of the NPPs for related bodies corporate in new s13B should be deleted as unnecessary.

Alternatively, s13B should state that it has no application to NPP 2.1(c) (direct marketing contrary to the individual's reasonable expectations at the time of collection).

### 6.2. Inadequate definition of 'personal information' for cyberspace

In a published article 'Privacy Principles - irrelevant to cyberspace?' (1996) 3 PLPR 114 (available at <http://www2.austlii.edu.au/itlaw/articles/IPPs.html>) I have identified deficiencies with the Privacy Act's definition of 'personal information' in relation to cyberspace transactions.

In the article I concluded:

> The approach of this definition misses the point to some extent. Information about, say, the interests, understanding or consumption habits of a particular person can be aggregated by an internet service provider (or providers), by use of e-mail or machine addresses, for purposes such as e-mailing customised direct marketing materials to that address, or to customise the appearance of a web page so as to appeal most to requests which come from a particular machine address. It makes no difference whether the ISP can `reasonably ascertain' the identity of the person who is associated with either the e-mail address or the http request, because the information about their consumption habits has been aggregated and used to market back to them, without them necessarily being aware of this or having consented to it. More serious consequences may also follow from such aggregation, such as decisions to limit access, or to deny some goods or services. If the definition of `personal information' excludes such activity, IPPs will be very weak in cyberspace.

Recommendation

The definition of 'personal information' in the Act should be amended to include wording such as 'any information which enables interactions with an individual on a personalised basis'.

### 6.3 Transborder data flows (NPP 9)

NPP 9 prohibits 'transfers' of personal information by an organisation to someone (other than the organisation) 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.

All of the publications by the A29 Committee of the EU have interpreted the 'adequacy' requirement of the Directive as requiring some such 'onward transfer' restriction, so this will be an aspect of the Bill that the EU looks at carefully.

Condition (a) plays the role of A25 of the Directive (which allows transfers to foreign countries with 'adequate' laws), but is weaker.

> (a) the organisation 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.

Conditions (b) - (e) are similar to those in A26(1) of the Directive and largely uncontentious.

Condition (f), however, is much weaker than anything found in the Directive:

> (f) the organisation 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 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.

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.

The EU may well regard these two aspects of NPP 9 as inadequate protection for EU citizens.

Recommendation

Conditions (a) and (f) should be tightened.